نشریه ۵۳–۸۰۰ سازمان ملی استاندارد و فناوری آمریکا

بازبینی شماره ۴

کنترل‌های امنیتی و حریم خصوصی برای سازمان‌ها و سیستم‌های اطلاعاتی فدرال

می‌توانید این نشریه را به صورت رایگان از آدرس زیر دریافت نمایید:

http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

مجوز استفاده از این نشریه

سازمان ملی استاندارد و فناوری آمریکا[1] این نشریه را در راستای پیشبرد مسئولیت‌هایی که تحت قانون کنترل امنیت اطلاعات فدرال[2] به عهده گرفته، منتشر نموده است. این سازمان مسئول تدوین استانداردها و دستورالعمل‌هایی در حوزه‌ی امنیت اطلاعات است که از جمله‌ی این موارد می‌توان به مشخص کردن حداقل الزامات امنیتی برای سیستم‌های اطلاعاتی فدرال اشاره نمود. البته استانداردها و دستورالعمل‌های این سازمان نباید بر روی سیستم‌های امنیتی ملی به کار گرفته شوند، مگر با تأیید مقاماتی که قدرت و اختیار سیاست‌گذاری برای این سیستم‌ها دارند. لازم به ذکر است که این نشریه با الزامات امنیتی بخش 8b(3) بخشنامه‌ی A-130 اداره‌ی مدیریت و بودجه‌ی آمریکا[3] که به ایمن‌سازی سیستم‌های اطلاعاتی می‌پردازد، همخوانی دارد. اطلاعات تکمیلی در این زمینه نیز در پیوست سوم این بخشنامه آورده شده است.

هیچ یک از مطالب این نوشتار با استانداردها و دستورالعمل‌هایی که وزیر بازرگانی آمریکا برای سازمان‌های دولتی الزام‌آور کرده است، مخالفت نمی‌کنند یا در صدد ایجاد تغییر در اختیارات فعلی وزیر بازرگانی، مدیر OMB یا هر مقام فدرال دیگری نیستند، پس چنین برداشتی از مطالب این نشریه کاملاً نادرست است. سازمان‌های غیردولتی نیز می‌توانند این نشریه را به طور کاملاً اختیاری و بدون پرداخت هزینه مورد استفاده قرار دهند.

ممکن است در این نشریه از نهادهای تجاری، ایده‌ها یا تجهیزات خاصی نام برده شده باشد تا یک مفهوم یا روشی تجربی به طور کامل شرح داده شود. به هیچ وجه هدف سازمان NIST ارائه‌ی پیشنهاد یا توصیه‌ی خاصی در مورد این نهادها، ایده‌ها یا تجهیزات نبوده است. حتی اشاره به اسامی آن‌ها نباید سبب شود که تصور کنید آن‌ها لزوماً بهترین موارد موجود هستند.

ممکن است در این نشریه به منابعی ارجاع داده شده باشد که هم‌اکنون سازمان NIST در حال نگارش آن‌ها باشد. این امکان نیز وجود دارد که سازمان‌های فدرال، اطلاعات این نشریه اعم از مفاهیم و روش‌ها را پیش از تکمیل نگارش منابع به کار بگیرند، بنابراین تا زمان اتمام تدوین هر یک از منابع، الزامات، دستورالعمل‌ها و

[1] National Institute of Standards and Technology (NIST)
[2] Federal Information Security Management Act (FISMA)
[3] Office of Management and Budget (OMB)

روش‌های فعلی قابل استفاده هستند. سازمان‌های فدرال می‌توانند روند نگارش نشریه‌های جدید سازمان NIST را از نزدیک دنبال کنند. ما از سازمان‌ها دعوت می‌کنیم که در بازه‌ی زمانی اختصاص داده شده به نظرسنجی عمومی، تمام نسخه‌های پیش‌نویس را بازبینی کنند و به سازمان NIST بازخورد دهند. تمام نشریه‌های بخش امنیت کامپیوتر سازمان NIST به جز موارد ذکر شده در بالا در آدرس http://csrc.nist.gov/publications موجود و قابل دسترسی هستند.

گزارش‌هایی از فناوری سیستم‌های کامپیوتری

آزمایشگاه IT سازمان ملی استاندارد و فناوری آمریکا[4] با ارائه‌ی توصیه‌هایی فنی برای زیرساخت استانداردها و سنجش ملی، رفاه عمومی و همچنین اقتصاد دولت را بهبود می‌بخشد. این آزمایشگاه با ارائه‌ی تست‌ها، روش‌های تست، داده‌های مرجع، پیاده‌سازی‌های شاهد مثال و تجزیه و تحلیل‌های فنی، به روند توسعه و استفاده‌ی پربازده از IT در جامعه سرعت می‌بخشد. تدوین استانداردها و دستورالعمل‌های فنی، راهبری و مدیریتی برای حفظ امنیت و حریم خصوصی اطلاعاتی که در سیستم‌های اطلاعاتی فدرال قرار دارند، از جمله مسئولیت‌های ITL است. نشریات سری ۸۰۰ سازمان NIST نیز در واقع گزارش‌هایی از تحقیقات، دستورالعمل‌ها و تلاش‌های ITL در زمینه‌ی امنیت سیستم‌های اطلاعاتی هستند و همکاری‌های این آزمایشگاه با سازمان‌های علمی، دولتی و صنعتی را گزارش می‌کنند.

چکیده

این نشریه فهرستی از کنترل‌های امنیتی و حریم خصوصی برای سیستم‌های اطلاعاتی فدرال و سازمان‌ها و همچنین فرایندی برای انتخاب آن‌ها ارائه می‌کند. کنترل‌های امنیتی و حریم خصوصی عملیات‌ها و دارایی‌های سازمانی، افراد، سایر سازمان‌ها و کشور را از تهدیدات مختلفی مثل حملات سایبری، بلایای طبیعی، شکست‌های ساختاری و خطاهای انسانی مصون می‌دارند. آن‌ها قابل سفارشی کردن هستند و به عنوان بخشی از فرایند کنترل امنیت اطلاعات و مخاطرات حریم خصوصی، در سطح سازمان پیاده‌سازی می‌شوند. این کنترل‌ها

[4] Information Technology Laboratory (ITL)

همچنین از الزامات امنیتی متعددی که برگرفته از قوانین، خط‌مشی‌ها، دستورات، مقررات، احکام اجرایی، استانداردها و نیازهای کسب‌وکار هستند، پیروی می‌کنند. نشریه‌ی ۵۳-۸۰۰ علاوه بر موارد فوق، توضیح می‌دهد که چطور می‌توان مجموعه‌ای از کنترل‌ها یا پوشش‌هایی تخصصی برای کارکردها، فناوری‌ها و محیط‌های عملیاتی خاص ایجاد کرد. در نهایت باید گفت که این کنترل‌ها قابلیت‌ها و سازکارهایی ارائه می‌دهند که از نظر امنیتی فوق‌العاده قوی هستند و می‌توان تا حد بسیار بالایی به عملکرد آها اطمینان داشت. همین امر سبب می‌شود محصولات IT و سیستم‌های اطلاعاتی که از آن‌ها و با بهره‌گیری از اصول مهندسی امنیت ساخته می‌شوند تا حد قابل توجهی مورد اعتماد باشند.

FIPS 200 و SP 800-53

پیاده‌سازی استانداردها و دستورالعمل‌های امنیت اطلاعات

استاندارد FIPS 200 استانداردی فدرال است که حداقل الزامات امنیتی برای اطلاعات و سیستم‌های اطلاعاتی فدرال را مشخص می‌کند. همه‌ی سازمان‌ها ملزم هستند این استاندارد که توسط سازمان NIST و در پاسخ به قانون FISMA ایجاد شده است را رعایت کنند. بدین منظور، سازمان‌ها ابتدا بر اساس استاندارد FIPS 199[۵] رده‌ی امنیتی سیستم اطلاعاتی خود را تعیین می‌کنند، سپس طبق استاندارد FIPS 200، سطح تأثیر سیستم اطلاعاتی را به دست می‌آورند و در نهایت، مجموعه‌ای متناسب از کنترل‌های امنیتی مبنا از میان کنترل‌های نشریه ۵۳-۸۰۰ انتخاب و بر روی سیستم خود اعمال می‌کنند. طبق راهنمایی که در نشریه ۵۳-۸۰۰ آورده شده است، دست سازمان‌ها در اعمال کنترل‌های امنیتی مبنا باز گذاشته شده است و آن‌ها ملزم به پیاده‌سازی کنترل‌های خاصی نیستند، یعنی سازمان‌ها می‌توانند کنترل‌هایی را اعمال کنند که با محیط عملیات و نیازهای کسب‌وکار آن‌ها مرتبط‌تر است.

با استفاده از استاندارد FIPS 200 در کنار نشریه ۵۳-۸۰۰، اطمینان حاصل می‌شود که کنترل‌های امنیتی مناسبی بر روی همه‌ی اطلاعات فدرال و سیستم‌های اطلاعاتی اعمال می‌شوند. با ارزیابی مخاطرات در سطح سازمان نیز می‌توان انتخاب اولیه کنترل‌های امنیتی را اعتبارسنجی کرد و فهمید که آیا نیاز به پیاده‌سازی کنترل‌های بیشتری برای حفاظت از عملیات‌های سازمانی، دارایی‌های سازمان، افراد، سایر سازمان‌ها یا کشور

[۵] نشریه FIPS 199 استانداردهای رده‌بندی امنیتی اطلاعات و سیستم‌های اطلاعاتی فدرال را تعیین می‌کند.

هست یا خیر. مجموعه کنترل‌های امنیتی که پس از انجام این مراحل حاصل می‌شوند، سطح مناسبی از امنیت را برای سازمان ایجاد خواهند کرد.

ایجاد بنیان‌های مشترک برای تأمین امنیت اطلاعات

همکاری میان نهادهای بخش خصوصی و عمومی

سازمان NIST برای ایجاد و توسعه‌ی استانداردها و دستورالعمل‌های مشخص‌شده در قانون FISMA، با سایر سازمان‌های فدرال و بخش خصوصی رایزنی و مشورت می‌کند. این کار سبب می‌شود تا امنیت اطلاعات بهبود پیدا کند، از دوباره‌کاری‌های پرهزینه و غیرضروری جلوگیری شود و اطمینان حاصل شود که نشریات این سازمان مکمل خوبی برای استانداردها و دستورالعمل‌هایی هستند که جهت حفاظت از سیستم‌های اطلاعاتی ملی به کار گرفته می‌شوند. علاوه بر انجام بررسی‌های عمومی، سازمان NIST با رئیس دفتر اطلاعات ملی آمریکا[۶]، وزارت دفاع (DoD) و کمیته‌ی سیاست‌گذاری بر سیستم‌های امنیتی ملی (CNSS)[۷] همکاری می‌کند تا یک چارچوب امنیتی واحد برای دولت راه‌اندازی کند. یک چارچوب مشترک برای امنیت اطلاعات، راه‌هایی مقرون‌به‌صرفه را برای مدیریت مخاطرات پیش روی سرمایه‌ها و عملیات سازمان، افراد، سایر سازمان‌ها، و کشور، در اختیار بخش‌های غیرنظامی، دفاعی و امنیتی دولت و پیمانکاران آن قرار می‌دهد. این چارچوب یکپارچه، مبنای مستحکمی را برای اتخاذ تصمیمات دوطرفه و مشترک، و اشتراک‌گذاری اطلاعات به صورت ساده‌تر ارائه می‌کند. NIST همچنین با مؤسسات دولتی و خصوصی دیگری نیز همکاری می‌کند تا روابطی را بین استانداردهای امنیتی و راهنمایی‌های NIST و سازمان بین‌المللی استانداردسازی و کمیسیون بین‌المللی الکتروتکنیک (ISO/IEC)، برقرار نماید.

الزامات امنیتی

از دیدگاه انواع تشکل‌ها با منافع متفاوت

[6] Director of National Intelligence (ODNI)
[7] Committee on National Security Systems (CNSS)

اصطلاح «الزام امنیتی» به شکل‌های مختلفی، توسط انواع جوامع و گروه‌ها مورد استفاده قرار می‌گیرد، بنابراین نیاز است توضیحات بیشتری ارائه شود تا منظور از این اصطلاح در موارد استفاده‌های متفاوت روشن شود. الزامات امنیتی می‌توانند در سطح بالایی از تجرید مطرح شوند، مثلاً در قوانین، احکام اجرایی، دستورات، خط‌مشی‌ها، استانداردها، مأموریت‌ها و فرایندهای کسب‌وکار. مثلاً قانون FISMA و نشریه FIPS 200 الزامات امنیتی را در چنین سطحی بیان می‌کنند.

کارکنان، الزامات امنیتی را به هدف پیمانکاری تهیه می‌کنند. این الزامات به گونه‌ای هستند که حفاظت لازم را از مأموریت‌ها و فرایندهای کسب‌وکار سازمان فراهم می‌آورند. مهندسان امنیت، مهندسان سیستم، و ترکیب‌کنندگان سیستم، الزامات طراحی امنیتی را برای سیستم‌های اطلاعاتی تهیه می‌کنند، معماری امنیتی و الزامات امنیتی را تعیین می‌کنند، و سپس توابع امنیتی لازم را در سخت‌افزار، نرم‌افزار و ثابت‌افزار اجرا می‌کنند.

الزامات امنیتی در انواع کنترل‌های امنیتی غیرفنی که نیز منعکس می‌شوند. مهم است که برای هر مورد استفاده از اصطلاح الزام امنیتی برای جوامع مربوطه تعریف شود که آن‌ها بتوانند مقصود خود را به‌روشنی با یکدیگر در میان بگذارند. لازم است تعیین شود که الزامات امنیتی قرار است در چه شرایطی مورد استفاده قرار گیرند، به گونه‌ای که افراد مربوطه بتوانند اهداف خود را به خوبی محقق سازند.

ممکن است سازمان‌ها، قابلیت‌های امنیتی لازم برای حفاظت از مأموریت‌ها و فرایندهای کسب‌وکار خود تعریف کنند. قابلیت‌های امنیتی معمولا مجموعه‌ای از ابزارهای حفاظتی (یعنی کنترل‌های امنیتی) هستند که از مجموعه‌های اختصاصی کنترل‌های امنیتی برگرفته شده‌اند، تا کارکردهای مورد نیاز را فراهم آورند.

بی‌طرفی خط‌مشی و فناوری

ویژگی‌های کنترل‌های امنیتی

کنترل‌های امنیتی موجود در فهرست با تعدادی استثنا، به گونه‌ای طراحی شده‌اند که طرفدار خط‌مشی یا فناوری خاصی نباشند. یعنی تمرکز کنترل‌های امنیتی و ارتقاهای کنترل بر روی اقدامات حفاظتی و تدافعی پایه مورد نیاز برای محافظت از اطلاعات در طول پردازش، انتقال و زمانی که در حافظه ذخیره شده‌اند، است. بنابراین، ارائه راهنمایی برای به‌کارگیری کنترل‌های امنیتی بر روی یک فناوری یا محیط عملیاتی خاص یا برای

یک قشر خاص و عملیات‌های کسب‌وکار و مأموریت‌های خاص، خارج از محدوده مطالب این نشریه است. استفاده‌های خاص مربوط به هر برنامه کاربردی، به کمک فرایندهای اختصاص تشریح‌شده در فصل ۳ و پوشش‌های مورد اشاره در پیوست خ، امکان‌پذیر خواهند بود. شایان ذکر است که بی‌طرف بودن کنترل‌های امنیتی نسبت به خطمشی‌ها و فناوری‌ها، به معنای ناآگاه بودن آن‌ها نسبت به خطمشی‌ها و فناوری‌های مذکور نیست. داشتن آگاهی کافی از خطمشی‌ها و فناوری‌ها، مسئله‌ای ضروری برای تولید کنترل‌های مناسب و مرتبط است.

در موارد معدودی که فناوری‌های خاصی در کنترل‌های امنیتی مورد اشاره قرار گرفته‌اند (مانند فناوری‌های همراه، PKI، بی‌سیم و VOIP)، به سازمان‌ها خاطرنشان می‌شود که اولویت بالاتری برای قابلیت امنیتی کنترل‌ها قائل شوند و مسائل مربوط به فناوری‌های خاص را در درجه دوم اهمیت قرار دهند. بسیاری از ابزارهای امنیتی مورد نیاز، از سایر کنترل‌های امنیتی موجود در مجموعه‌های اولیه به دست می‌آیند و برای توسعه پوشش‌ها و طرح‌های امنیتی با استفاده از فرایندهای اختصاصی، به کار گرفته می‌شوند. ممکن است کنترل‌های امنیتی موجود در خانواده‌های مختلف، همپوشانی‌هایی نیز با یکدیگر داشته باشند.

علاوه بر توسعه پوشش‌ها و طرح‌های امنیتی اختصاصی و شخصی‌سازی‌شده، شماره‌های ویژه NIST و گزارشات بین‌اداره‌ای، گاهی اوقات راهنمایی‌هایی را در خصوص کنترل‌های امنیتی برای فناوری‌های خاص و کاربردهای مختص بخش‌های مختلف (مانند شبکه‌های برق هوشمند، بخش بهداشت و درمان، سیستم‌های کنترل صنعتی، و کاربردهای همراه) نیز ارائه می‌کنند.

به‌کارگیری کنترل‌های امنیتی بی‌طرف، منافع زیر را به دنبال دارد:

- سازمان‌ها را ترغیب می‌کند تا صرف نظر از فناوری‌های اطلاعاتی مورد استفاده در سیستم‌های اطلاعاتی سازمان، بر قابلیت‌های امنیتی مورد نیاز برای موفقیت در مأموریت‌ها و فرایندهای خود، و همچنین بر حفاظت از اطلاعات، تمرکز کنند.
- سازمان‌ها را ترغیب می‌کند تا امکان استفاده از هر یک از کنترل‌های امنیتی در فناوری‌های خاص، محیط‌های عملیاتی، مأموریت‌ها، و انجمن‌های ذینفع را بررسی و تحلیل کنند.
- سازمان‌ها را ترغیب می‌کند تا خطمشی‌های امنیتی را به عنوان بخشی از فرایند اصلاح کنترل‌های امنیتی با پارامترهای متغیر، تعیین و تنظیم نمایند.

تعیین و تنظیم طرح‌های امنیتی با استفاده از پوشش‌ها و راهنمایی‌های اصلاحی، در کنار کنترل‌های امنیتی بی‌طرف، روش‌های مقرون‌به‌صرفه و مبتنی بر مخاطره‌ای را جهت تأمین امنیت اطلاعات، در اختیار سازمان‌ها قرار می‌دهند. روش‌های ارائه‌شده، بر اساس فناوری، بخش، و محیط عملیاتی، طراحی خواهند شد.

سعی و اهتمام در طراحی و پیاده‌سازی کنترل‌های امنیتی

کنترل مخاطراتی که کارکردهای مأموریتی و تجاری سازمان را تهدید می‌کنند

کنترل‌های امنیتی نشریه ۵۳-۸۰۰ سازمان NIST طوری طراحی شدند که پیروی از قوانین فدرال، احکام اجرایی، دستورا، خط‌مشی‌ها، مقررات، استانداردها و دستورالعمل‌ها را آسان کنند. منظور از پیروزی از موارد مذکور این نیست که از چک‌لیست خاصی تبعیت شود یا گزارشات متعددی برای FISMA تهیه شوند. در عوض، سازمان‌ها باید سعی و اهتمام لازم را در تأمین امنیت اطلاعات و مدیریت مخاطرات از خود نشان دهند. برای داشتن سعی و اهتمام لازم در زمینه امنین اطلاعات، سازمان‌ها باید تمام اطلاعات مورد نیاز را در برنامه‌های مدیریت مخاطرات مورد استفاده قرار دهند و به نحو مؤثری از راهنمایی‌های اصلاحی و انعطاف‌های موجود در اسناد NIST استفاده کنند تا کنترل‌های امنیتی مورد اشاره در طرح‌های امنیتی سازمان، متناسب با مأموریت‌ها و الزامات کسب‌وکار سازمان باشند. سازمان‌ها همچنین باید با استفاده از ابزارها و شیوه‌های مدیریت مخاطرات، ابزارهای حفاظتی مورد نیاز را تهیه، پیاده‌سازی و نگهداری نمایند، تا بتوانند با تهدیدات پیش روی سرمایه‌ها و عملیات سازمان، افراد، سایر سازمان‌ها، و کشور مقابله کنند. به کمک فرایندها، رویه‌ها و فناوری‌های مؤثر و مبتنی بر مخاطره، می‌توان اطمینان حاصل کرد که تمام سازمان‌ها و سیستم‌های اطلاعاتی فدرال، قابلیت‌های لازم برای پشتیبانی از مسئولیت‌ها، زیرساخت‌ها و کاربردهای فدرال را دارا هستند.

کنترل‌های حریم خصوصی

حفاظت از حریم خصوصی در اطلاعات فدرال

پیوست د، تحت عنوان فهرست کنترل‌های حریم خصوصی، بخشی است که به‌تازگی، با هدف رفع نیازهای حریم خصوصی سازمان‌های فدرال، به این نشریه اضافه شده است. این پیوست:

- مجموعه‌ای ساختاریافته از کنترل‌های حریم خصوصی، بر اساس بهترین اقدامات در اختیار سازمان‌ها قرار می‌دهد و آن‌ها را در تبعیت از از قوانین فدرال، احکام اجرایی، دستورا، خط‌مشی‌ها، مقررات، استانداردها، دستورالعمل‌ها، راهنمایی‌ها و اسناد سازمانی، یاری می‌کند.
- ارتباط و پیوندی میان کنترل‌های امنیتی و حریم خصوصی ایجاد می‌کند، تا بتوان الزامات مربوط به امنیت و حریم خصوصی را به نحو مقتضی رعایت نمود. برای رعایت صحیح، باید توجه داشت که در سازمان‌ها، برنامه‌ها و سیستم‌های اطلاعاتی فدرال، گاهی این الزامات با یکدیگر همپوشانی پیدا می‌کنند.
- امکان استفاده از چارچوب مدیریت مخاطرات NIST را در فرایند انتخاب، پیاده‌سازی، ارزیابی، و نگهداری کنترل‌های امنیتی مورد استفاده در سازمان‌ها، برنامه‌ها و سیستم‌های اطلاعاتی فدرال نشان می‌دهد.
- همکاری نزدیک‌تری را بین مسئولان حوزه امنیت و حریم خصوصی در دولت فدرال ایجا می‌کند، تا بتوان اهداف مقامات ارشد را در زمینه قوانین، خط‌مشی‌ها، مقررات، رهنمودها، استانداردها، و راهنمایی‌های مربوط به حریم خصوصی، جامه عمل پوشاند.

مشابهت زیادی بین ساختار کنترل‌های امنیتی پیوست د و کنترل‌های امنیتی پیوست‌های ج و چ وجود دارد. به عنوان مثال، کنترل AR-1 (برنامه حریم خصوصی و مدیریت) از سازمان‌ها می‌خواهد تا طرح‌های خریم خصوصی را تهیه کنند که هم در سطح برنامه و هم در سطح سازمان قابل اجرا باشند. این طرح‌ها را می‌توان در کنار طرح‌های امنیتی نیز اجرا کرد، تا سازمان‌ها موقعیت انتخاب مجموعه مناسب کنترل‌های حریم خصوصی را بر اساس محیط عملیاتی، مأموریت‌ها و فرایندهای کسب‌وکار به دست آورند. به‌کارگیری همان مفاهیم مورد استفاده در مدیریت مخاطرات امنیت اطلاعات، سازمان‌ها را یاری می‌کند تا کنترل‌های حریم خصوصی را به گونه‌ای مقرون‌به‌صرفه و مخاطره‌محور پیاده‌سازی نمایند و در عین حال، از حریم خصوصی افراد حفاظت و از الزامات پیروی کنند. کنترل‌های استاندارد حریم خصوصی، رویکرد منظم و ساختارمندی را برای رعایت الزامات فدرال فراهم می‌آورند.

نکته احتیاطی

پیاده‌سازی تغییرات بر اساس اصلاحات صورت‌گرفته در شماره ویژه 53-800

چهار تغییر عمده در این سند انجام شده‌اند: (۱) کنترل‌های امنیتی و کنترل‌های پیشرفته‌ای به پیوست‌های ج و چ و/ی مجموعه‌های اولیه با سطح تأثیر کم، متوسط و زیاد، اضافه شده یا از آن‌ها حذف شده‌اند؛ (۲) راهنمایی‌های تکمیلی، اصلاح شده‌اند؛ (۳) برخی از بخش‌های فصول اصلی یا پیوست‌ها، اصلاح شده‌اند؛ و (۴) ادبیات مورد استفاده در سند، رفع ابهام یا به‌روز شده است.

در هنگام تغییر مجموعه‌های اولیه اصلاحی کنترل‌های امنیتی در سطح سوم سلسله مراتب مدیریت مخاطرات (که در شماره ویژه 39-800 تشریح شده است) و به‌روزرسانی کنترل‌های امنیتی در تمام سطوح در سند اصلاح‌شده 53-800، سازمان‌ها باید از یک رویکرد سنجش‌شده و مبتنی بر مخاطرات استفاده کنند. مگر آن که به صورتی دیگر در خط‌مشی OMB آمده باشد، به سازمان‌ها توصیه می‌شود که فعالیت‌های زیر را برای اعمال تغییرات نسخه 53-800 انجام دهند:

- نخست این که سازمان‌ها باید بررسی کنند که پس از اعمال راهنمایی‌های اصلاحی ارائه‌شده در این سند، آیا کنترل‌های امنیتی یا کنترل‌های پیشرفته جدیدی وجود دارند که باید آن‌ها را به سیستم‌های اطلاعاتی یا محیط‌های کاری آن‌ها اعمال کرد یا خیر؛
- سپس، سازمان‌ها باید تغییرات اعمال‌شده در راهنمایی‌های تکمیلی، راهنمایی‌های موجود در فصول اصلی و پیوست‌ها، و ادبیات رفع ابهام و به‌روزشده را بررسی کنند تا دریابند که آیا تغییراتی هستند که باید آن‌ها را در سیستم‌های اطلاعاتی اعمال کرد یا خیر؛
- در نهایت، پس از این که سازمان‌ها کلیات تغییرات را تعیین کردند، این تغییرات تا حد امکان در فرایند پایش اعمال می‌شوند. پیاده‌سازی کنترل‌های امنیتی جدید و به‌روزشده برای مقابله با تهدیدات موجود، همواره بلاترین اولویت را دارا است. تغییراتی مانند تغییر در قالب‌ها یا تغییرات جزئی در ادبیات مورد استفاده در سند، معمولا پایین‌ترین اولویت را دارند، و بر اساس چرخه‌های مرور و بازبینی اعمال شده‌اند.

پیشگفتار

نشریه‌ای که در حال مطالعه آن هستید، بیشترین به‌روزرسانی با فهرست کنترل‌های امنیتی از زمان شروع آن از سال ۲۰۰۵ را دارد. این نشریه توسط NIST، وزارت دفاع، سازمان اطلاعات، و کمیته سیستم‌های امنیت ملی (به عنوان بخشی از کارگروه مشترک) توسعه یافته است. به‌روزرسانی حاضر، برای مقابله با تهدیداتی است که اخیرا مشاهده شده‌اند؛ تهدیداتی که هوشمندتر و سریع‌تر از گذشته هستند (تناوب حملات بیشتر شده است و مهاجمان حرفه‌ای‌تر شده‌اند و حملات خود را به هدفمندی بیشتری انجام می‌دهند). کنترل‌های امنیتی و کنترل‌های پیشرفته ارائه‌شده در این سند، حوزه‌های مختلفی را پوشش می‌دهند: کاربردهای همراه و رایانش ابری، امنیت برنامه‌های کاربردی، قابلیت اعتماد، تضمین، انعطاف سیستم‌های اطلاعاتی، تهدیدات داخلی، امنیت زنجیره تأمین، و استمرار حملات. علاوه بر این، شماره ویژه ۵۳-۸۰۰ هشت خانواده جدید از کنترل‌های حریم خصوصی را نیز در بر می‌گیرد.

نشریه ۵۳-۸۰۰ سازمان NIST با ارائه‌ی زیر و بم کنترل‌های امنیتی لازم برای قوی کردن سیستم‌های اطلاعاتی و محیط‌هایی که سیستم‌ها در آن کار می‌کنند، رویکرد بهتری برای امنیت اطلاعات و مدیریت مخاطرات در اختیار سازمان‌ها قرار می‌دهد. این راهبرد، شامل کنترل‌های امنیتی مختلفی برای «پایش پیوسته» است که اطلاعات بلادرنگی را به سازمان‌ها ارائه می‌کند. مقامات امنیتی ارشد سازمان‌ها می‌توانند با استفاده از این اطلاعات، تصمیمات مخاطره‌محور مناسبی را اتخاذ کنند که بر مأموریت‌ها و فرایندهای کسب‌وکار آن‌ها تأثیر می‌گذارد.

برای بهره‌گیری از مجموعه توسعه‌یافته‌ی کنترل‌های امنیتی و حریم خصوصی و همچنین ارائه‌ی انعطاف‌پذیری و چابکی بیشتر به سازمان‌ها، مفهوم پوشش‌ها در این نسخه معرفی شد. پوشش‌ها رویکردی ساختاریافته در اختیار سازمان‌ها قرار می‌دهند و از این طریق به آن‌ها کمک می‌کنند که مبناهای کنترل امنیتی را بسازند و برنامه‌های امنیتی مختص عملکردهای کسب‌وکار، محیطه‌های عملیات و فناوری‌ها ایجاد نمایند. این رویکرد اختصاصی از اهمیت بالایی برخوردار است، زیرا تعداد کنترل‌های امنیتی و کنترل‌های پیشرفته افزایش یافته است و سازمان‌ها می‌توانند بر اساس آن، راهبردهای مناسبی را در زمینه مدیریت مخاطرات توسعه دهند و با توجه به حیطه تحمل مخاطرات خود، نیازهای حفاظتی خویش را برطرف نمایند.

چندین ویژگی جدید نیز به این نسخه اضافه شده است تا استفاده‌ی آن برای سازمان‌ها را تسهیل نماید. این ویژگی‌ها عبارتند از:

- فروض مربوط به توسعه مجموعه اولیه کنترل‌های امنیتی
- راهنمایی‌های تکمیلی توسعه‌یافته، به‌روزشده و یکپارچه
- عبارت‌های انتخاب و اختصاص جدید برای کنترل‌های امنیتی و کنترل‌های حریم خصوصی
- نام‌های توصیفی برای کنترل‌های امنیتی پیشرفته و کنترل‌های حریم خصوصی پیشرفته
- جداول یکپارچه برای کنترل‌های امنیتی و کنترل‌های پیشرفته بر اساس خانواده مربوطه
- جداولی برای کنترل‌های امنیتی به منظور پشتیبانی از توسعه، ارزیابی و ضمانت عملکرد
- انطباق جداول با استاندارد امنیتی بین‌المللی ISO/IEC 15408 (معیارهای عمومی)

کنترل‌ها امنیتی و حریم خصوصی این نشریه به صورت بی‌طرف طراحی شده‌اند و همین امر سبب انعطاف‌پذیری آن‌ها حین پیاده‌سازی شده است. کنترل‌های مذکور به گونه‌ای طراحی شده‌اند که بتوان با استفاده از آن‌ها، قابلیت‌های مربوط به حریم خصوصی و امنیت اطلاعات را به خوبی در فرایندهای سازمانی (مانند معماری سازمان، مهندسی سیستم، چرخه عمر توسعه سیستم، و تأمین و تدارکات) تعبیه نمود. یکپارچه‌سازی موفقیت‌آمیز کنترل‌های امنیتی و کنترل‌های حریم خصوصی در فرایندهای سازمانی، سبب تکامل برنامه‌های امنیت و حریم خصوصی می‌شود. این امر همچنین باعث می‌شود که سازمان بتواند سرمایه‌گذاری‌های خود در زمینه امنیت و حریم خصوصی را، بر مأموریت‌ها و فرایندهای اصلی کسب‌وکار متمرکز نماید.

کارگروه مشترک

فصل اول

مقدمه

نیاز به حفاظت از اطلاعات و سیستم‌های اطلاعاتی

انتخاب و پیاده‌سازی *کنترل‌های امنیتی* برای سیستم‌های اطلاعاتی[۸] و سازمان‌ها، بسیار حائز اهمیت است. این امور نه تنها بر عملکرد[۹] و دارایی سازمان‌ها[۱۰] اثر می‌گذارند، بلکه می‌توانند رفاه فردی و عمومی را نیز تحت تأثیر قرار دهند. کنترل‌های امنیتی اقداماتی حفاظتی و تدافعی هستند که با اهداف زیر طراحی شده‌اند:

- حفاظت از محرمانگی، یکپارچگی و آماده به کار بودن اطلاعاتی که سازمان‌ها و سیستم‌های اطلاعاتی پردازش، ذخیره و ردوبدل می‌کنند.
- رعایت مجموعه‌ای از الزامات امنیتی[۱۱] مشخص و تعریف‌شده

پیش از آن که سازمان‌ها در صدد تأمین امنیت اطلاعات در سیستم‌های اطلاعاتی خود برآیند، باید به چند سوال مهم پاسخ دهند:

- با اعمال کدام کنترل‌ها الزامات امنیتی سازمان رعایت می‌شوند و به حد کافی از مخاطرات امنیتی کاسته می‌شود؟ مخاطرات امنیتی به دلیل استفاده از اطلاعات و سیستم‌های اطلاعاتی حین انجام ماموریت‌های سازمانی و امور مربوط به کسب‌وکار پدید می‌آیند.
- آیا پیش از این، کنترل‌های امنیتی پیاده‌سازی شده‌اند یا برنامه‌ای برای این کار در سازمان موجود است؟
- انتظار سازمان از کارایی و اثربخشی کنترل‌های امنیتی در چه سطحی است[۱۲]؟

---

[۸] هر سیستم اطلاعاتی مجموعه‌ای از *منابع* اطلاعاتی است که برای جمع‌آوری، پردازش، نگهداری، استفاده، به‌اشتراک‌گذاری، انتشار یا جابجایی اطلاعات ایجاد شده است. این سیستم‌ها شامل سیستم‌های تخصصی از قبیل سیستم‌های کنترل صنعتی و سیستم‌های سوئیچینگ تلفن نیز هستند.

[۹] در اینجا منظور از عملکرد، ماموریت‌ها، کارکردها و حتی اعتبار سازمان است.

[۱۰] کلمه‌ی سازمان به هر نهادی با هر سطح پیچیدگی، وسعت یا جایگاه در ساختار سازمانی اطلاق می‌شود.

[۱۱] الزامات امنیتی الزاماتی هستند که از نیازهای کسب‌وکار، قوانین، مقررات، احکام اجرایی، دستورات، سیاست‌ها و استانداردها استخراج می‌شوند و هدف آن‌ها حفظ محرمانگی، یکپارچگی و آماده به کار بودن اطلاعاتی است که سازمان‌ها و سیستم‌های اطلاعاتی پردازش، ذخیره و ردوبدل می‌کنند.

[۱۲] کنترل‌های امنیتی زمانی اثربخش خواهند بود که به درستی پیاده‌سازی شوند، طبق اهداف از پیش تعیین‌شده عمل کنند و خروجی مطلوبی ارائه دهند. البته همه‌ی این موارد باید ضمن رعایت الزامات و سیاست‌های امنیتی موجود در محیط عملیاتی سیستم اطلاعاتی صورت گیرند.

سازمانی که مخاطرات ناشی از اطلاعات و سیستم‌های اطلاعاتی خود را شناسایی می‌کند و در صورت لزوم تخفیف می‌دهد، با انجام فرایند مدیریت مخاطرات، می‌تواند پاسخ این سوال‌ها را بیابد[۱۳]. سند NIST Special Publication 800-39 دستورالعملی را برای مدیریت مخاطرات در سه لایه ارائه می‌دهد: سطح سازمانی، سطح ماموریت‌ها و فرایندهای کسب‌وکار و سطح سیستم اطلاعاتی. سازمان‌ها باید فرایند مشخصی برای مدیریت مخاطرت تعریف کنند و کنترل‌های امنیتی ذکر شده در این سند را به عنوان بخشی از آن فرایند مورد استفاده قرار دهند[۱۴].

بسیار مهم است که مقامات مسئول از مخاطرات امنیتی باخبر باشند و عواملی که می‌توانند تأثیر چشمگیری بر عملکرد و سرمایه‌های سازمان، افراد، دیگر سازمان‌ها و کشور داشته باشند را بشناسند[۱۵]. مسئولان همچنین باید از وضعیت فعلی برنامه‌های امنیتی سازمان خود مطلع باشند و از کنترل‌های امنیتی که هم اکنون اطلاعات و سازمان‌های اطلاعاتیِ آن‌ها را حفاظت می‌کند آگاهی داشته باشند. داشتن این اطلاعات آن‌ها را یاری می‌دهد تا با قضاوتی درست و سرمایه‌گذاری آگاهانه، مخاطرات را تا حد قابل قبولی کاهش دهند. هدف نهایی ایجاد محیطی است که با وجود مخاطرات ناشی از دسترسی غیرمجاز، استفاده، افشا، اختلال، دستکاری یا تخریب اطلاعات، امنیت کافی برای انجام ماموریت‌ها و فعالیت‌های روزمره‌ی سازمان فراهم کند.

۱–۱– هدف و کاربرد

هدف این نوشتار، ارائه دستورالعمل‌هایی در جهت انتخاب و تعیین کنترل‌های امنیتی برای سیستم‌های اطلاعاتی و سازمان‌هاست. این دستورالعمل‌ها سازمان‌های اجرایی دولت فدرال را در جهت رعایت الزامات ذکرشده در FIPS Publiction 200 یاری می‌دهند و به تمام مؤلفه‌های[۱۶] یک سیستم اطلاعاتی که اطلاعات فدرال را پردازش، ذخیره و منتقل می‌کند اعمال می‌شوند. در حقیقت، این دستورالعمل‌ها با انجام موارد زیر

---

[۱۳] مخاطرات امنیت اطلاعات، آن دسته از مخاطرات هستند که در اثر از دست رفتن محرمانگی، صحت و یکپارچگی، و در دسترس بودن اطلاعات یا سیستم‌های اطلاعاتی پدید می‌آیند. این مخاطرات، می‌توانند اثرات نامطلوبی بر سرمایه‌ها و عملیات سازمان، افراد، سایر سازمان‌ها و عموم مردم داشته باشند.

[۱۴] کنترل‌های مدیریت برنامه (پیوست چ)، مکمل کنترل‌های امنیتی سیستم‌های اطلاعاتی (پیوست ج) هستند. تمرکز این کنترل‌ها بر آن دسته از الزامات امنیت اطلاعات سازمان است که وابسته به یک سیستم اطلاعاتی خاص نیستند و در مدیریت برنامه‌های امنیت اطلاعات، نقشی کلیدی دارند.

[۱۵] این عوامل، مخاطرات مربوط به منابع اصلی و منابع زیرساختی که در دستور اجرایی شماره ۷ ریاست جمهوری در زمینه امنیت داخلی به آن‌ها اشاره شده است را نیز شامل می‌شود.

[۱۶] مؤلفه‌های سیستم‌های اطلاعاتی، مواردی از جمله چارچوب‌های اصلی، ایستگاه‌های کاری، سرورها (مانند پایگاه داده، ایمیل، احراز هویت، وب، پراکسی، فایل، و نام دامنه)، دستگاه‌های ورودی و خروجی (مانند اسکنرها، دستگاه‌های کپی و چاپگرها)، مؤلفه‌های شبکه (مانند فایروال‌ها، مسیریاب‌ها، گیت‌وی‌ها، سوئیچ‌های صدا و داده، کنترل‌گرها، نقاط دسترسی از راه دور، و حسگرها)، سیستم‌عامل‌ها، ماشین‌های مجازی، میان‌افزارها و برنامه‌های کاربردی را شامل می‌شوند.

دستیابی به سیستم‌های اطلاعاتی ایمن‌تر و فرایند مدیریت مخاطرات اثربخش‌تر درون دولت فدرال را ممکن می‌سازند:

- تسهیل انتخاب و تعیین کنترل‌های امنیتی برای سیستم‌های اطلاعاتی و سازمان‌ها
- ارائه‌ی یک فهرست ثابت و در عین حال انعطاف‌پذیر از کنترل‌های امنیتی. چنین فهرستی نه تنها نیازهایی که در حال حاضر برای حفاظت اطلاعات وجود دارند را برآورده می‌کند، بلکه نیازهایی که در آینده و بر اساس فناوری‌ها، الزامات و تهدیدات جدید پدید خواهند آمد را نیز رفع می‌کند.
- پیشنهادی در جهت اعمال کنترل‌های امنیتی برای آن دسته از سیستم‌های اطلاعاتی که طبق FIPS Publication 199 دسته‌بندی شدند. در FIPS Publication 199 استانداردهای دسته‌بندی امنیتی اطلاعات فدرال و سیستم‌های اطلاعاتی آورده شده است.
- ایجاد اصولی برای توسعه‌ی روش‌های ارزیابی کنترل‌های امنیتی و روندهایی برای تعیین میزان کارایی آن‌ها.
- بهبود روابط بین سازمان‌ها از طریق ایجاد یک زبان رایج برای تبادل نظر در خصوص مدیریت مخاطرات

علاوه بر کنترل‌های امنیتی ذکر شده در بالا، این نوشتار به موارد زیر نیز پرداخته است:

- ارائه‌ی مجموعه‌ای از کنترل‌های مدیریت برنامه امنیت اطلاعات که معمولاً در سطح سازمانی پیاده‌سازی می‌شود و در سیستم‌های اطلاعات سازمانی فردی کنترل نمی‌شود.
- ارائه‌ی مجموعه‌ای از کنترل‌های حریم خصوصی. این کنترل‌ها بر اساس استانداردهای بین‌المللی و بهترین اقداماتی تدوین شده‌اند که سازمان‌ها را در جهت رعایت الزامات برگرفته از قوانین فدرال، سیاست‌ها و استانداردها یاری می‌دهند.
- ایجاد پیوند و ارتباط بین کنترل‌های امنیتی و حریم خصوصی با هدف رعایت الزامات امنیتی و حریم خصوصی که ممکن است در مفهوم و پیاده‌سازی درون سیستم‌های اطلاعات فدرال، برنامه‌ها و سازمان‌ها هم‌پوشانی داشته باشند.

کنترل‌های استانداردشده‌ی حریم خصوصی روشی ساختاریافته‌تر و منظم‌تر برای رعایت الزامات حریم خصوصی ارائه می‌دهند و پیروی از این الزامات را به نمایش می‌گذارند. دخالت دادن همان مفاهیمی که در مدیریت مخاطرات مربوط به امنیت اطلاعات استفاده شد نیز به سازمان‌ها کمک می‌کند تا کنترل‌های حریم خصوصی را به شکلی مقرون‌به‌صرفه‌تر و مبتنی بر مخاطرات پیاده‌سازی کنند.

دستورالعمل‌ها و راهنمایی‌های آورده شده در این نگارش برای تمام سیستم‌های اطلاعاتی فدرال قابل استفاده هستند[۱۷] مگر آن‌هایی که به عنوان سیستم‌های امنیتی ملی و طبق بخش ۳۵۴۲ سند .U.S.C 44 طراحی شده‌اند[۱۸]. دستورالعمل‌ها از لحاظ فنی بسیار بسط داده شده‌اند تا دستورالعمل‌های مشابهی که برای سیستم‌های امنیتی ملی استفاده می‌شوند را تکمیل کنند. حتی ممکن است مقاماتی که سیاست‌هایی برای این سیستم‌ها تدوین می‌کنند دستورالعمل‌های این نوشتار را تأیید کنند و از آن‌ها برای سیستم‌های امنیت ملی نیز استفاده کنند[۱۹]. به تمام دولت‌های ایالتی، محلی و سازمان‌های بخش خصوصی توصیه می‌شود که از این دستورالعمل‌ها استفاده کنند.

۱–۲– مخاطبان این نگارش

مخاطبان این نگارش مختصصانی هستند که در زمینه امنیت اطلاعات و سیستم های امنیتی کار می‌کنند. به بیان دقیق تر این نوشتار گروه‌های مختلف زیر را مورد خطاب قرار می‌دهد:

- افرادی که مسئولیت مدیریت مخاطرات، نظارت و یا تأمین امنیت سیستم‌های اطلاعاتی را بر عهده دارند، مثل مقامات سازمان، مدیران اطلاعات، مدیران ارشد امنیت اطلاعات[۲۰]، مدیران سیستم‌های اطلاعاتی و مدیران امنیت اطلاعات.
- افرادی که مسئول توسعه سیستم‌های اطلاعاتی هستند؛ مثل مدیران برنامه، طراحان و توسعه‌دهندگان سیستم، مهندسین امنیت اطلاعات و کسانی که مسئولیت یکپارچه‌سازی سیستم را عهده‌دار هستند.
- کسانی که مسئولیت‌های عملیاتی و پیاده‌سازی امنیت اطلاعات را بر عهده دارند، مثل صاحبان کسب‌وکارها، دارندگان سیستم‌های اطلاعاتی، صاحبان اطلاعات، مدیران سیستم.
- افرادی که مسئول نظارت و ارزیابی امنیت اطلاعات هستند؛ از جمله: صاحبان سیستم‌های اطلاعاتی، کسانی که سیستم‌ها را ارزیابی می‌کنند.

---

[۱۷] یک سیستم اطلاعات فدرال، سیستمی است که توسط یک اداره اجرایی، پیمانکار یک اداره اجرایی، یا یک سازمان دیگر از سوی یک اداره اجرایی به کار گرفته می‌شود.

[۱۸] سیستم امنیت ملی، یک سیستم اطلاعاتی است که توسط یک اداره، پیمانکار یک اداره، یا یک سازمان دیگر از سوی یک اداره به کار گرفته می‌شود، به شکلی که عملکرد یا به‌کارگیری سیستم مذکور مربوط به فعالیت‌های اطلاعاتی یا رمزنگاری مربوط به امنیت ملی، دستورات و کنترل‌های نیروهای نظامی، و ابزارآلات مربوط به تسلیحات، یا بخشی ضروری از فرایندهای اطلاعاتی یا نظامی باشد؛ یا همواره بر اساس فرایندهای اطلاعاتی مبتنی بر معیارها و الزامات دستور اجرایی قانون کنگره، مورد حفاظت قرار گیرد.

[۱۹] **دستورالعمل** CNSS 1253 راهنمایی‌هایی را در خصوص پیاده**سازی** سیستم‌های امنیت ملی ارائه کرده است.

[۲۰] در سطح اداره، این پست به عنوان مدیر ارشد امنیت اطلاعات اداره شناخته می‌شود. همچنین ممکن است سازمان‌ها، این پست را مدیر ارشد امنیت اطلاعات یا مدیر مسئول امنیت اطلاعات بنامند.

- شرکت های تجاری که سیستم‌ها و محصولات IT تولید می‌کنند، فناوری‌های مرتبط با امنیت اطلاعات راه‌اندازی می‌نمایند یا خدمات امنیت اطلاعات ارائه می‌دهند.

۱–۳– ارتباط این نوشتار با سایر نوشتارهای حوزه کنترل امنیت

طی نگارش این متن، منابع گوناگونی مورد بررسی قرار گرفتند. هدف از انجام این کار نیز ایجاد مجموعه‌ای از کنترل‌های امنیتی بوده است که فنی و در عین حال به طور وسیعی قابل استفاده باشد. منابعی که مورد استفاده گرفتند شامل کنترل‌های امنیتی مختلفی بودند. از کنترل‌های حوزه‌ی مالی، دفاع، حسابرسی، سلامت و صنعت گرفته تا سازمان‌های اطلاعاتی. آن‌ها کنترل‌های تعریف شده توسط سازمان‌های ملی و بین‌المللی را نیز شامل می‌شدند. هدف این نوشتار ارائه‌ی مجموعه‌ای از کنترل‌های امنیتی است که بتواند الزامات امنیتی را تمام و کمال رعایت کند[۲۱]؛ الزاماتی که برای سازمان‌ها، فرایندهای کسب‌وکار و سیستم‌های اطلاعاتی و در راستای سایر استانداردهای امنیت اطلاعات وضع شده‌اند.

از فهرست کنترل‌های امنیتی این نوشتار می‌توان برای حفاظت از اطلاعات و سیستم‌های اطلاعاتی استفاده نمود. این فهرست می‌تواند در وضعیت‌های مختلف فنی، محیطی و عملیاتی اطلاعات و سیستم‌های اطلاعاتی را در برابر تهدیدات رایج و همچنین تهدیدات مداوم پیشرفته مصون دارد. به علاوه این کنترل‌ها می‌توانند به نشانه‌ی پیروی از انواع الزامات امنیتی دولتی، سازمانی یا نهادی مورد استفاده قرار بگیرند[۲۲]. سازمان‌ها موظفند تا کنترل‌های امنیتی مناسبی انتخاب کنند، آن‌ها را به درستی پیاده‌سازی نمایند و اثربخشی کنترل‌ها در رعایت الزامات امنیتی را به نمایش بگذارند.

۱–۴– مسئولیت‌های سازمانی

سازمان‌ها از FIPS Publication 199 استفاده می‌کنند تا اطلاعات و سیستم‌های اطلاعاتی خود را طبقه‌بندی کنند. طبقه‌بندی امنیتی فعالیتی است که کل سازمان را در بر می‌گیرد[۲۳] و با مشارکت پرسنل ارشد سازمان از قبیل مدیران IT، مدیران ارشد امنیت اطلاعات، دارندگان طلاعات، ذی‌نفعان و صاحبان سیستم‌های اطلاعاتی

---

[۲۱] الزامات امنیتی، الزاماتی هستند که از قوانین، دستورات، رهنمون‌ها، خطمشی‌ها، دستورالعمل‌ها، مقررات، استانداردها، راهنمایی‌ها، یا نیازهای سازمانی گرفته می‌شوند؛ تا با استفاده از آن‌ها از محرمانگی، صحت و یکپارچگی، و در دسترس بودن اطلاعات ذخیره‌ای، پردازشی و انتقالی، اطمینان حاصل شود.

[۲۲] **شماره** ویژه NIST 800-53A، راهنمایی‌هایی را در زمینه بررسی اثربخشی این کنترل‌های امنیتی ارائه کرده است.

[۲۳] به پانویس شماره **۷سند** FIPS 200 مراجعه کنید.

انجام می‌شود[۲۴]. اطلاعات در لایه های ۱ و ۲ طبقه‌بندی می‌شوند. مطابق FIPS Publication 200 سازمان‌ها از نتایج طبقه‌بندی امنیتی لایه‌های ۱ و ۲ استفاده می‌کنند تا سیستم‌های اطلاعاتی سازمانی را در لایه‌ی ۳ به عنوان سیستم‌های اطلاعاتی با سطح تأثیر کم، متوسط و زیاد طراحی کنند. گرچه فرایند انتخاب کنترل‌های امنیتی به طور کلی بر روی سیستم‌های اطلاعاتی لایه‌ی ۳ متمرکز است، اما این فرایند بر روی هر سه لایه‌ی فرایند مدیریت مخاطرات قابل اعمال است.

طبقه‌بندی امنیتی سند FIPS Publication 199 اطلاعات و عملیات و استفاده از سیستم‌های اطلاعاتی را با بدترین اثرات نامطلوبی که ممکن است بر روی عملیات‌های سازمانی و دارایی‌ها، افراد، سایر سازمان‌ها و کشور داشته باشد، مربوط می‌سازد[۲۵]. ارزیابی‌های مخاطرات سازمان که اطلاعات مربوط به تهدیدات خاص و رایج، اطلاعات مربوط به آسیب‌پذیری‌ها و احتمال بروز اثرات نامطلوب به خاطر این آسیب‌پذیری‌ها را دربرمی‌گیرد، در انتخاب نهایی کنترل‌های امنیتی بسیار مفید است[۲۶]. مجموعه نهایی و مورد توافق کنترل‌های امنیتی که مبتنی بر نیازهای خاص سازمان در زمینه مأموریت‌ها و فرایندهای کسب‌وکار است، به همراه دلایل مربوطه، در طرح امنیتی سیستم‌های اطلاعاتی مستندسازی شده است[۲۷]. استفاده از کنترل‌های امنیتی این نوشتار، امنیت بیشتری برای سیستم‌های اطلاعاتی فدرال را به همراه دارد. ضمن این که انعطاف‌پذیری و چابکی مورد نیاز سازمان‌ها برای مقابله با فضای تهدیدات که روزبه‌زور پیچیده‌تر می‌شود را نیز حفظ می‌کند.

دستیابی به امنیت اطلاعات که برای سازمان‌ها، فرایندهای کسب‌وکار و سیستم‌های اطلاعاتی در حد مطلوبی باشد، مسئولیتی چندوجهی است که نیازمند موارد زیر است:

- الزامات و مشخصات امنیتی که صریحاً مشخص شده باشند.
- محصولات فناوری که به خوبی بر اساس فرایندهای تولید نرم‌افزار، سخت‌افزار و ثابت‌افزار طراحی و ساخته شده باشند.

---

[۲۴] **سازمان**‌ها معمولا کنترل‌های مدیریتی، عملیاتی و مالی را روی سیستم‌های اطلاعاتی و ابزارهای امنیتی مربوطه اعمال می‌کنند. از جمله این ابزارها، می‌توان به قابلیت اجرا و الزام نمودن آن دسته از کنترل‌های امنیتی اشاره کرد که برای حفاظت از سرمایه‌ها و عملکرد سازمان، افراد، سایر سازمان‌ها، و کشور ضروری به شمار می‌آیند.

[۲۵] ملاحظات مربوط به تأثیر بالقوه این عوامل بر سایر **سازمان**‌ها در سطح ملی، از قانون USA PATRIOT و رهنمون‌های ریاست‌جمهوری در زمینه امنیت داخلی (HSPD) گرفته شده است.

[۲۶] بررسی مخاطرات را می‌توان بسته به نیازهای سازمان، به طرق مختلفی انجام داد. شماره ویژه NIST 800-137، راهنمایی‌هایی را در خصوص ارزیابی مخاطرات به عنوان بخشی از فرایند کلی مدیریت مخاطرات سازمان، ارائه می‌کند.

[۲۷] مقامات مربوطه یا نمایندگان آن‌ها، از طریق پذیرفتن طرح‌های امنیتی نهایی، موافقت می‌کنند که از کنترل‌های امنیتی انتخاب‌**شده درسازمان** (از جمله در مأموریت‌ها و فرایندهای کسب‌وکار آن) و همچنین در سیستم‌های اطلاعاتی آن، استفاده شود.

- فرایندها و اصول صحیح مهندسی امنیت و مهندسی سیستم‌ها، که برای ترکیب محصولات فناوری اطلاعات با سیستم‌های اطلاعاتی سازمان طراحی شده‌اند.
- اصول صحیح امنیتی که به خوبی مستندسازی شده و در الزامات آموزشی و فعالیت‌های روزانه کارکنان امنیتی در نظر گرفته شده‌اند.
- نظارت مداوم سازمان‌ها و سیستم‌های اطلاعاتی جهت تعیین اثربخشی کنترل‌های امنیتی به کار گرفته‌شده، تغییراتی که در سیستم‌های اطلاعاتی و محیط‌های عملیات رخ می‌دهند و پیروی از قوانین، مقررات، سیاست‌ها و استانداردها[۲۸]
- برنامه‌ریزی امنیت اطلاعات و مدیریت چرخه عمر توسعه سیستم[۲۹]

از دیدگاه مهندسی، تأمین امنیت اطلاعات تنها یکی از بیشمار قابلیت‌های عملیاتی مورد نیاز برای یک سیستم اطلاعاتی برای پشتیبانی از فرایندهای کسب‌وکار است. هزینه‌ی این قابلیت‌ها را نیز باید سازمان‌ها حین توسعه سیستم تأمین کنند تا به موفقیت در کسب‌وکار و ماموریت دست یابند. بسیار حائز اهمیت است که سازمان‌ها واقع‌گرایانه مخاطراتی که عملیات‌های سازمانی، دارایی‌ها، افراد، سایر سازمان‌ها و کشور را تهدید می‌کنند را ارزیابی کنند. ارزیابی واقعی مخاطرات نیازمند شناخت تهدیدات و آسیب‌پذیری‌های داخل سازمان است. علاوه بر این، دانستن احتمال بروز اثرات نامطلوبی که به خاطر بهره‌برداری از چنین آسیب‌پذیری‌هایی رخ می‌دهند نیز نیاز است[۳۰]. در نهایت، الزامات امنیتی باید با داشتن دانش کامل و در نظر گرفتن راهبرد ارزیابی مخاطرات سازمان و با توجه به مشکلات مربوط به هزینه، برنامه و عملکرد به‌کارگیری سیستم‌های اطلاعاتی رعایت شوند[۳۱].

۱–۵– آنچه در ادامه خواهید خواند

فصل دو: این فصل به مفاهیم اصلی مربوط به انتخاب و تعیین کنترل‌های امنیتی می‌پردازد. این مفاهیم عبارتند از: مدیریت چندلایه مخاطرات، ساختار کنترل‌های امنیتی و نحوه سازماندهی آنها در خانواده‌های مختلف، استفاده از کنترل‌های امنیتی معمول و ارث‌بری از توانایی‌های امنیتی، محیط‌های خارجی و تأمین‌کنندگان خدمات، تضمین و امانت و بازبینی و توسعه‌ی کنترل‌های امنیتی و مبناها.

---

[۲۸] شماره ویژه NIST 800-137، راهنمایی‌هایی را در خصوص پایش پیوسته سیستم‌های اطلاعاتی سازمان و محیط عملیاتی آن‌ها ارائه می‌کند.
[۲۹] شماره ویژه NIST 800-64، راهنمایی‌هایی را در خصوص ملاحظات امنیتی اطلاعات در چرخه عمر توسعه سیستم ارائه می‌کند.
[۳۰] شماره ویژه NIST 800-30، راهنمایی‌هایی را در خصوص فرایند بررسی مخاطرات ارائه می‌کند.
[۳۱] علاوه بر الزامات امنیت اطلاعات، سازمان‌ها باید الزامات حریم خصوصی که از قوانین و خطمشی‌های فدرال گرفته می‌شوند را نیز مد نظر قرار دهند. سازمان‌ها می‌توانند کنترل‌های حریم خصوصی مورد اشاره در پیوست د را به همراه کنترل‌های امنیتی پیوست ج مورد استفاده قرار دهند و بدین ترتیب، به مجموعه جامعی از کنترل‌های امنیتی حریم خصوصی دست یابند.

فصل سه: این فصل فرایند انتخاب و تعیین کنترل‌های امنیتی برای سیستم‌های اطلاعات سازمانی را توضیح می‌دهد. این فرایند شامل انتخاب کنترل‌های امنیتی مبنا، مستندسازی فرایند انتخاب کنترل‌های امنیتی و اعمال فرایند انتخاب به سیستم‌های بازمانده از قبل و سیستم‌های جدید.

پیوست‌ها: در این بخش اطلاعاتی بسیار ضروری در رابطه با انتخاب و تشخیص کنترل‌های امنیتی آورده شده است. این اطلاعات عبارتند از: مراجع کلی[۳۲]، اصطلاحات و تعاریف، سرنام‌ها، مجموعه‌های اولیه کنترل‌های امنیتی برای سیستم‌های اطلاعاتی با سطح تأثیر کم، متوسط و زیاد، دستورالعملی برای تضمین و امانت سیستم‌های اطلاعاتی، کاتالوگ کنترل‌های امنیتی[۳۳]، کاتالوگ کنترل‌های مدیریت برنامه امنیت اطلاعات، تطابق با استانداردهای بین‌المللی امنیت اطلاعات، راهنمای توسعه پوشش‌ها توسط سازمان ها یا تشکل‌های علاقمند و فهرستی از کنترل‌های حریم خصوصی.

---

[۳۲] مگر در صورتی که به گونه‌ای دیگر ذکر شده باشد، منظور از تمام ارجاعات به اسناد NIST در سند حاضر (یعنی استانداردهای فدرال **پردازش اطلاعات وشماره**های ویژه)، جدیدترین نسخه آن‌ها است.

[۳۳] کنترل‌های امنیتی مورد اشاره در شماره ویژه NIST 800-53، به صورت آنلاین نیز موجود هستند و می‌توان آن‌ها را از این آدرس اینترنتی دانلود کرد: http://web.nvd.nist.gov/view/800-53/home

فصل دوم

مفاهیم پایه

ساختار[۳۴]، سازماندهی[۳۵]، مجموعه‌های پایه[۳۶] و ضمانت[۳۷] کنترل‌های امنیتی

در این فصل به بررسی مفاهیم پایه مربوط به انتخاب و تشریح کنترل‌های امنیتی می‌پردازیم. این مفاهیم عبارتند از: (۱) مدیریت مخاطره سه مرحله‌ای[۳۸]؛ (۲) ساختار کنترل‌های امنیتی و سازماندهی این کنترل‌ها در کاتالوگ کنترل؛ (۳) اصول کنترل‌های امنیتی؛ (۴) شناسایی کاربردهای کنترل‌های امنیتی معمول؛ (۵) کنترل‌های امنیتی در محیط‌های خارج از سازمان؛ (۶) ضمانت‌های کنترل‌های امنیتی؛ و (۷) بازنگری‌های آینده در کنترل‌های امنیتی، کاتالوگ کنترل و کنترل‌های اولیه[۳۹].

۲-۱- مدیریت مخاطره چند مرحله‌ای

انتخاب و تشریح کنترل‌های امنیتی برای یک سیستم اطلاعاتی، بخشی از برنامه امنیت اطلاعات سازمان برای مدیریت مخاطرات است. این مخاطرات، مواردی هستند که سرمایه‌ها و عملیات سازمان، افراد، سازمان‌های دیگر، و مردمی که عملکرد سیستم عملیاتی بر آن‌ها تأثیر می‌گذارد را تهدید می‌کنند. رویکردهای مبتنی بر مخاطره، برای انتخاب و تشریح کنترل‌های امنیتی به سه عامل اثربخشی، کارایی و محدودیت‌های موجود به موجب راهنمایی‌ها، استانداردها، مقررات، خط‌مشی‌ها، رهنمودها، دستورات اجرایی و قوانین فدرال توجه می‌کنند. به منظور یکپارچه‌سازی فرایند مدیریت مخاطره در سراسر سازمان و برطرف کردن دغدغه‌های موجود در زمینه کسب‌وکار و مأموریت سازمان، از یک رویکرد سه مرحله‌ای استفاده شده است که مخاطرات را در سه سطح مورد بررسی قرار می‌دهد: (۱) سطح سازمان، (۲) سطح فرایند کسب‌وکار/مأموریت، و (۳) سطح سیستم اطلاعاتی. فرایند مدیریت مخاطره در در این سه سطح انجام می‌شود و هدف نهایی آن، ارتقای پیوسته اقدامات سازمان در زمینه کنترل مخاطرات و برقراری ارتباطات مؤثر درون‌سطحی و بین‌سطحی میان تمامی ذی‌نفعانی است که

---

[34] Structure
[35] Organization
[36] Baseline
[37] Assurance
[38] Three-tiered risk management
[39] Baseline controls

موفقیت سازمان در انجام کسب‌وکار و مأموریت خود بر آن‌ها تأثیر می‌گذارد. شکل ۱، رویکرد مدیریت مخاطره سه مرحله‌ای را به تصویر می‌کشد.

****

شکل ۱: رویکرد مدیریت مخاطره سه مرحله‌ای

****

در مرحله اول، بخش‌های مختلف کسب‌وکار و مأموریت سازمان اولویت‌بندی می‌شوند. این اولویت‌بندی به نوبه خود تصمیمات مالی و راهبردهای سرمایه‌گذاری را جهت می‌دهد. بر این اساس، سازمان اقدام به استفاده از فناوری‌های اطلاعاتی کارآمدی می‌کند که متناسب با اهداف و شاخص‌های عملکردی آن باشند. مرحله دوم شامل این موارد است: (۱) تعریف فرایندهای کسب‌وکار و مأموریت‌های مورد نیاز برای پشتیبانی از عملکردهای مربوط به کسب‌وکار و مأموریت سازمان، (۲) تعیین دسته‌های امنیتی سیستم‌های اطلاعاتی مورد نیاز برای اجرای فرایندهای کسب‌وکار و مأموریت سازمان، (۳) ترکیب الزامات امنیت اطلاعات با فرایندهای کسب‌وکار و مأموریت سازمان، (۴) طراحی معماری سازمان (شامل معماری امنیت اطلاعات) جهت تسهیل در اختصاص کنترل‌های امنیتی به سیستم‌های اطلاعاتی سازمان و محیط‌های کاری این سیستم‌ها. چارچوب مدیریت مخاطره (RMF)[۴۰]، که در شکل ۲ به تصویر کشیده شده است، ابزار اولیه برطرف کردن مخاطرات در مرحله سوم است[۴۱]. در این سند به گام دوم RMF، یعنی فرایند انتخاب کنترل امنیتی می‌پردازیم و در این راه به سه مرحله سلسله مراتب مدیریت مخاطره سازمانی توجه ویژه‌ای خواهیم داشت.

****

شکل ۲: چارچوب مدیریت مخاطره

****

[40] Risk Management Framework

[۴۱] شماره ویژه NIST 800-37، راهنمایی‌هایی را در زمینه پیاده‌سازی چارچوب مدیریت مخاطره ارائه کرده است. لیست کامل اسنادی که به چارچوب مدیریت مخاطره پرداخته و در شکل ۲ **مورد اشاره قرار** گرفته‌اند، در پیوست الف ارائه شده است.

چارچوب مدیریت مخاطره، به دغدغه‌های امنیتی سازمان‌ها در زمینه طراحی، توسعه، پیاده‌سازی، به‌کارگیری و کنار گذاشتن سیستم‌های اطلاعاتی و محیط‌های کاری آن‌ها می پردازد. چارچوب مدیریت مخاطره از شش گام زیر تشکیل می‌شود:

گام ۱: دسته‌بندی سیستم‌های اطلاعاتی بر اساس مبحث ارزیابی تأثیرات در سند FIPS 199[۴۲]،

گام ۲: انتخاب مجموعه پایه‌ای از کنترل‌های امنیتی مناسب بر اساس نتایج دسته‌بندی امنیتی و اعمال کردن راهنمایی‌های مربوطه،

گام ۳: پیاده‌سازی کنترل‌های امنیتی و مستندسازی جزئیات مربوط به طراحی، توسعه و پیاده‌سازی این کنترل‌ها،

گام ۴: دسترسی به کنترل‌های امنیتی به منظور تعیین میزان پیاده‌سازی و عملکرد صحیح آن‌ها و دستیابی به نتایج مطلوب در خصوص رعایت الزامات امنیتی سیستم[۴۳]،

گام ۵: صدور مجوز فعالیت سیستم‌های اطلاعاتی بر اساس میزان مخاطرات موجود در پیش روی سرمایه‌ها و عملیات سازمان، افراد و دیگر سازمان‌ها، و به‌کارگیری سیستم اطلاعاتی در صورتی که سطح مخاطره قابل قبول باشد،

گام ۶: پایش کنترل‌های امنیتی در سیستم اطلاعاتی و محیط کاری آن به طور پیوسته، به منظور تعیین اثربخشی کنترل‌ها، تغییرات پدید آمده در سیستم و محیط، و تبعیت از راهنمایی‌ها، استانداردها، مقررات، خط‌مشی‌ها، رهنمودها، دستورات اجرایی و قوانین فدرال.

۲-۲- ساختار کنترل امنیتی

کنترل‌های امنیتی مورد اشاره در این سند، ساختار و سازماندهی تعریف‌شده‌ای دارند. به منظور سهولت کار در فرایندهای انتخاب و تشریح کنترل‌های امنیتی، این کنترل‌ها به ۱۸ خانواده تقسیم می‌شوند[۴۴]. هر خانواده شامل

---

[۴۲] **دستورالعمل** CNSS 1253، راهنمایی‌هایی را در زمینه دسته‌بندی امنیتی سیستم‌های امنیت ملی ارائه کره است.

[۴۳] شماره ویژه NIST 800-53A، راهنمایی‌هایی را در زمینه حصول اطمینان از اثربخشی کنترل‌های امنیتی ارائه کرده است.

[۴۴] از بین ۱۸ خانواده مورد اشاره در شماره ویژه NIST 800-53، **۱۷ مورد از آن‌ها** در کاتالوگ کنترل امنیتی در پیوست ج تشریح شده‌اند. این **۱۷ خانواده متناسب با ۱۷** الزام حداقل امنیت سیستم‌های اطلاعاتی و سیستم‌های اطلاعات فدرال مورد اشاره در سند FIPS 200 هستند. **خانواده** دیگر، یعنی مدیریت برنامه (PM)، کنترل‌های لازم برای برنامه‌های امنیت اطلاعات FISMA را فراهم می‌آورد. این خانواده، هرچند که در FIPS 200 اشاره خاصی به آن نشده است، کنترل‌های امنیتی سطح سازمان (و نه سطح سیستم اطلاعاتی) را فراهم می‌آورد. برای مشاهده اطلاعات بیشتر درباره پیاده‌سازی راهنمایی‌های مربوط به کنترل‌های PM، به پیوست چ مراجعه کنید.

کنترل‌های امنیتی مربوط به موضوعات امنیت عمومی آن است. در هر خانواده از یک شناسه دو کاراکتری منحصر به فرد استفاده می‌شود که خانواده کنترل امنیتی (مانند PS یا امنیت شخصی) را تعیین می‌کند. کنترل‌های امنیتی ممکن است شامل جنبه‌هایی از خط‌مشی، نظارت، فرایندهای دستی، اقدامات افراد، یا مکانیسم‌های خودکار پیاده‌سازی‌شده توسط دستگاه‌ها و سیستم‌های اطلاعاتی باشند. جدول ۱ لیستی از خانواده‌های کنترل امنیتی و شناسه‌های خانواده‌ها در کاتالوگ کنترل امنیتی را ارائه می‌کند[۴۵].

جدول ۱. شناسه‌های کنترل امنیتی و نام خانواده‌ها

شناسه	خانواده	شناسه	خانواده
AC	کنترل دسترسی	MP	حفاظت از رسانه‌ها
AT	اطلاع‌رسانی و آموزش	PE	حفاظت محیطی و فیزیکی
AU	ممیزی و پاسخگویی	PL	برنامه‌ریزی
CA	صدور مجوز و ارزیابی امنیتی	PS	امنیت شخصی
CM	مدیریت پیکربندی	RA	ارزشیابی مخاطره
CP	برنامه‌ریزی احتمالی	SA	مالکیت خدمات و سیستم
IA	شناسایی و صدور مجوز	SC	حفاظت از ارتباطات و سیستم
IR	پاسخ به رویدادها	SI	یکپارچگی اطلاعات و سیستم
MA	حفظ و نگهداری	PM	مدیریت برنامه

ساختار کنترل امنیتی از این مؤلفه‌ها تشکیل شده است: (۱) یک انتخاب کنترل، (۲) یک بخش راهنمایی‌های تکمیلی، (۳) یک بخش کنترل پیشرفته[۴۶]، (۴) یک بخش مراجع، و (۵) یک بخش اولویت‌بندی و تخصیص اولیه[۴۷]. مثال زیر که از خانواده ممیزی و پاسخگویی گرفته شده است، ساختار یک کنترل امنیتی نوعی را نشان می‌دهد.

AU-3: **محتوای سوابق ممیزی**

[۴۵] کنترل‌های حریم خصوصی لیست‌شده در پیوست د، سازماندهی و ساختاری مشابه کنترل‌های امنیتی دارند. به عنوان مثال، در آن‌ها نیز از شناسه‌های دو کاراکتری برای تشخیص هشت خانواده حریم خصوصی استفاده می‌شود.

[46] Control enhancements

[47] Priority and baseline allocation

کنترل: سیستم اطلاعاتی، سوابق ممیزی را تولید می‌کند. این اسناد شامل اطلاعاتی هستند که تعیین می‌کنند چه نوع رویدادهایی به وقوع پیوسته‌اند، این رویدادها چه هنگام رخ داده‌اند، رویدادهای مذکور کجا اتفاق افتاده‌اند، منبع رویدادها چه بوده است، این رویدادها چه پیامدهایی داشته‌اند، و چه افراد و گروه‌هایی در این میان ایفای نقش کرده‌اند.

راهنمایی‌های تکمیلی: محتوای سوابق ممیزی شامل مواردی از جمله مهرهای زمانی، آدرس‌های مبدأ و مقصد، شناسه‌های کاربران و فرایندها، توضیحات مربوط به رویدادها، نشانه‌های دال بر موفقیت یا عدم موفقیت، نام فایل‌های مربوطه، و قوانین کنترل جریان و کنترل دسترسی فراخوانی‌شده هستند. پیامدهای رویدادها، شاخص‌های مربوط به موفقیت یا شکست رویدادها و نتایج آن‌ها (مانند وضعیت امنیتی سیستم اطلاعاتی پس از وقوع رویداد) را شامل می‌شوند. کنترل‌های مربوطه: AU-2, AU-8, AU-12, SI-11.

کنترل پیشرفته:

(۱) محتوای سوابق ممیزی / سایر اطلاعات ممیزی

سیستم اطلاعاتی، سوابق ممیزی را تولید می‌کند که شامل این اطلاعات اضافی هستند:

[اختصاص: اطلاعات اضافی و دقیق تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: اطلاعات دقیقی که ممکن است سازمان در سوابق ممیزی خود در نظر بگیرد، مواردی از جمله متن کامل دستورات ویژه و هویت کاربران حساب‌های گروهی را در بر می‌گیرند. سازمان‌ها این اطلاعات ممیزی اضافی را محدود به مواردی می‌کنند که برای رعایت الزامات ممیزی خاص، لازم هستند. بدین ترتیب، اطلاعات گمراه‌کننده یا اطلاعاتی که مانع یافتن موارد مطلوب می‌شوند، ثبت نمی‌گردند و استفاده از اطلاعات ممیزی آسان‌تر می‌شود.

(۲) محتوای سوابق ممیزی / مدیریت متمرکز محتوای سوابق ممیزی

سیستم اطلاعاتی، امکان مدیریت متمرکز و پیکربندی محتوای گردآوری‌شده در سوابق ممیزی را فراهم می‌آورد. این اسناد توسط [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] تهیه می‌شوند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته لازم می‌دارد که محتوای گردآوری‌شده در سوابق ممیزی از یک مکان متمرکز پیکربندی شوند. بدین ترتیب، استفاده از سیستم‌های اتوماسیون ضروری خواهد بود. سازمان‌ها فرایند انتخاب محتوای ممیزی را به گونه‌ای هماهنگ می‌کنند که از مدیریت متمرکز و قابلیت پیکربندی ارائه‌شده توسط سیستم اطلاعاتی پشتیبانی شود. کنترل‌های مربوطه: AU-6, AU-7.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AU-3 اولویت پایین	AU-3(1) اولویت متوسط	AU-3(1)(2) اولویت بالا

این بخش کنترل، پیشنهاد می‌کند که سازمان یا سیستم اطلاعاتی، اقدامات و فعالیت‌های خاصی را در زمینه امنیت انجام دهند. عبارت «سیستم اطلاعاتی» به عملکردهایی اشاره دارد که در آن‌ها از فناوری‌های اطلاعاتی استفاده می‌شود (مانند سخت‌افزار، نرم‌افزار و ثابت‌افزار). در مقابل، عبارت «سازمان» به فعالیت‌هایی اشاره دارد که مبتنی بر فرایندها یا موجودیت‌ها هستند. به عبارت دیگر، کنترل امنیتی معمولاً از طریق انسان یا اقدامات مبتنی بر روش‌های اجرایی صورت می‌گیرد. آن دسته از کنترل‌های امنیتی که از عبارت سازمان استفاده می‌کنند، ممکن است کماکان به سطحی از خودکارسازی نیاز داشته باشند. به طور مشابه، آن دسته از کنترل‌های امنیتی که از عبارت سیستم اطلاعاتی استفاده می‌کنند، عناصری از فرایند یا موجودیت را در خود دارند. استفاده از عبارت سازمان و/یا سیستم اطلاعاتی، مقدمه پیاده‌سازی کنترل‌های امنیتی در هر یک از سطوح سلسله مراتب مدیریت مخاطره (یعنی سطح سازمانی، سطح فرایند کسب‌وکار و مأموریت، سطح سیستم اطلاعاتی) نیست.

در مورد برخی از کنترل‌های امنیتی در کاتالوگ کنترل، به سازمان اجازه داده می‌شود که برخی مقادیر و پارامترهای مربوط به کنترل‌ها را تعیین کند، و بدین ترتیب سطحی از انعطاف‌پذیری فراهم می‌آید. این انعطاف‌پذیری با استفاده از عبارت‌های «اختصاص» و «انتخاب» در کنترل‌های امنیتی و کنترل‌های پیشرفته مشخص شده است. انتخاب‌ها و اختصاص‌ها به سازمان امکان می‌دهند که کنترل‌های امنیتی و کنترل‌های پیشرفته را بر اساس این موارد به شکل مطلوب درآورد: (۱) الزامات امنیتی برای پشتیبانی از نیازهای عملیاتی، فرایند کسب‌وکار و مأموریت سازمان، (۲) فرایند ارزشیابی مخاطره و سطح تحمل مخاطره توسط سازمان، و (۳) الزامات امنیتی تعریف‌شده در راهنمایی‌ها، استانداردها، مقررات، خط‌مشی‌ها، رهنمودها، دستورات اجرایی و قوانین فدرال[۴۸].

[۴۸] به طور کلی، پارامترهای تعیین‌شده توسط سازمان که در اختصاص‌ها و انتخاب‌ها به آن‌ها اشاره شده است، در مورد کنترل‌های پیشرفته مربوطه نیز مصداق خواهند داشت.

به عنوان مثال، سازمان‌ها می‌توانند اطلاعات اضافی مورد نیاز برای پشتیبانی از فرایند پردازش رویدادهای ممیزی را مشخص نمایند. مثال AU-3(1) را که در بالا ارائه شد، ملاحظه کنید (قسمت [اختصاص: اطلاعات اضافی و دقیق تعیین‌شده توسط سازمان]). این اختصاص‌ها ممکن است شامل اقدامات خاص سیستم اطلاعاتی در صورت شکست ممیزی، بازه‌های زمانی تهیه نسخه پشتیبان سیستم، محدودیت‌هایی برای استفاده از گذرواژه، یا لیست توزیع روش‌های اجرایی و خط‌مشی‌های سازمان باشند[۴۹]. پس از این که مقادیر انتخاب‌ها و اختصاص‌ها تعیین شدند[۵۰]، این مقادیر تبدیل به بخشی از کنترل امنیتی می‌شوند و پیاده‌سازی کنترل با توجه به عبارات کنترلی تکمیل‌شده، بررسی و ارزیابی می‌شود. اختصاص‌ها به گونه‌ای تعریف شده‌اند که امکان انعطاف بالایی را برای سازمان‌ها فراهم آورند. سازمان‌ها می‌توانند مقادیر را به دلخواه خود تعیین کنند و لازم نیست که آن‌ها را از بین چند مقدار از پیش تعریف‌شده، انتخاب نمایند. در مقابل، انتخاب‌ها به گونه‌ای هستند که آزادی عمل زیادی را فراهم نمی‌آورند و سازمان‌ها باید انتخاب خود را از بین چند مقدار تعیین‌شده انجام دهند[۵۱].

بخش راهنمایی‌های تکمیلی، اطلاعات اضافه‌ای را برای کنترل‌های امنیتی خاص ارائه می‌کند. سازمان‌ها می‌توانند راهنمایی‌های تکمیلی را در صورت لزوم در هنگام تعریف، توسعه و/یا پیاده‌سازی کنترل‌های امنیتی به کار گیرند. راهنمایی‌های تکمیلی می‌توانند در فرایند پیاده‌سازی کنترل‌های امنیتی و با توجه به محیط عملیاتی، الزامات مربوط به کسب‌وکار و مأموریت، یا ارزشیابی مخاطره بسیار سودمند باشند. این راهنمایی‌ها همچنین توضیحات مفیدی درباره هدف و معنای کنترل‌ها ارائه می‌کنند. هنگامی که یک راهنمایی مربوط به تمامی کنترل نباشد و و تنها در مورد بخش خاصی از کنترل پیشرفته صدق کند، کنترل پیشرفته مذکور نیز شامل راهنمایی‌های تکمیلی خواهد بود. ممکن است بخش راهنمایی‌های تکمیلی، شامل لیستی از «کنترل‌های مربوطه» باشد. کنترل‌های مربوطه: (۱) به طور مستقیم بر پیاده‌سازی یک کنترل امنیتی یا کنترل پیشرفته تأثیر می‌گذارند یا از آن پشتیبانی می‌کنند، (۲) یک «قابلیت امنیتی» را تکمیل می‌کنند، یا (۳) در بخش راهنمایی‌های تکمیلی به آن‌ها ارجاع می‌شود. کنترل‌های امنیتی پیشرفته، بنا به تعریف، با کنترل اصلی ارتباط دارند. آن دسته از کنترل‌های مربوطه که در راهنمایی‌های تکمیلی کنترل اولیه لیست شده‌اند، در بخش

---

[۴۹] سازمان‌ها تعیین می‌کنند که انتخاب‌ها و اختصاص‌ها در مرحله اول (سطح سازمان)، مرحله دوم (سطک فرایند کسب‌وکار و مأموریت)، سطح سوم (سطح سیستم اطلاعاتی)، یا ترکیبی از این سطوح درج شوند.

[۵۰] ممکن است سازمان‌ها، به جای تکمیل انتخاب‌ها و اختصاص‌ها در کنترل و به عنوان بخشی از طرح امنیتی، مقادیر خاص پارامترهای کنترل امنیتی را در خطمشی‌ها، روش‌های اجرایی یا رهنمایی‌ها تعریف کنند (به گونه‌ای که در مورد بیش از یک سیستم اطلاعاتی صدق نمایند) و در طرح امنیتی به اسناد مبدأ ارجاع دهند.

[۵۱] کنترل‌های امنیتی به طور کلی به شکلی تعریف شده‌اند که مستقل از فناوری و روش پیاده‌سازی باشند، و بنابراین دربردارنده الزامات خاصی در این زمینه نیستند. سازمان‌ها الزامات مورد نیاز را طرح امنیتی سیستم اطلاعاتی می‌گذجانند.

راهنمایی‌های تکمیلی کنترل پیشرفته تکرار نمی‌شوند. اما ممکن است برخی کنترل‌های مربوطه، بدون این که در کنترل اولیه ذکر شده باشند، در بخش کنترل پیشرفته بیایند.

بخش کنترل پیشرفته شامل عبارت‌هایی در زمینه قابلیت‌های امنیتی است که اهداف روبرو را دنبال می‌نمایند: (۱) ارتقای قابلیت‌ها و ویژگی‌های یک کنترل، و/یا (۲) افزایش قدرت یک کنترل. در هر دو حالت، کنترل‌های پیشرفته در آن دسته از سیستم‌های اطلاعاتی و محیط‌های کاری مورد استفاده قرار می‌گیرند که نیازمند سطح حفاظت بالاتری هستند. کنترل‌های پیشرفته به شکل شماره‌گذاری‌شده در هر کنترل لیست شده‌اند، به گونه‌ای که می‌توان به راحتی مشاهده کرد چه پیشرفتی نسبت به کنترل اولیه حاصل شده است. هر کنترل پیشرفته دارای یک زیرعنوان کوتاه است که قابلیت امنیتی ارائه‌شده توسط آن را مشخص می‌کند. در مثال AU-3، اگر نخستین کنترل پیشرفته انتخاب شود، عبارت تعیین‌کننده کنترل به شکل AU-3(1) خواهد بود. البته تنها در صورتی از این عبارت‌ها استفاده می‌شود که نیاز به تعیین یک کنترل پیشرفته در یک کنترل خاص باشد. این عبارت‌ها به هیچ عنوان نشان‌دهنده قدرت کنترل‌های پیشرفته یا جایگاه آن‌ها در یک سلسله مراتب نیستند. کنترل‌های پیشرفته را نمی‌توان به صورت مستقل انتخاب کرد. در واقع در صورتی که یک کنترل پیشرفته انتخاب شده باشد، حتماً کنترل امنیتی اولیه نیز انتخاب شده است. این امر در پیوست‌های ت و ج تشریح شده است.

بخش مراجع، آن دسته از راهنمایی‌ها، استانداردها، مقررات، خط‌مشی‌ها، رهنمودها، دستورات اجرایی و قوانین فدرال را شامل می‌شود که در خصوص یک کنترل امنیتی خاص صدق می‌کنند[۵۲]. این مراجع، شامل قوانین و مقررات فدرال و اطلاعات لازم برای پیاده‌سازی کنترل‌های امنیتی و کنترل‌های پیشرفته هستند. بخش مراجع همچنین شامل وب‌سایت‌هایی است که سازمان‌ها می‌توانند در آن‌ها اطلاعات بیشتری را در مورد پیاده‌سازی و بررسی کنترل‌های امنیتی مشاهده کنند.

بخش اولویت و تخصیص به مجموعه‌های پایه، شامل این موارد است: (۱) کدهای اولویت‌بندی مورد استفاده برای مرتب‌سازی تصمیمات در جریان پیاده‌سازی کنترل‌های امنیتی؛ و (۲) تخصیص اولیه کنترل‌های امنیتی و کنترل‌های پیشرفته به مجموعه‌های پایه. سازمان‌ها می‌توانند با استفاده از کد اولویت‌بندی هر کنترل امنیتی، دریابند که پیاده‌سازی باید به چه ترتیبی انجام شود. به عبارت دیگر، کد اولویت‌بندی ۱ یا P1 در هنگام پیاده‌سازی اولویت بالاتری از کد اولویت‌بندی ۲ یا P2 دارد، کد اولویت‌بندی ۲ یا P2 در هنگام پیاده‌سازی

[۵۲] موارد ذکرشده در بخش مراجع، آخرین نسخه منتشرشده از قوانین مذکور هستند. این مراجع، جامع و کامل هستند و برای کمک به سازمان‌ها در راه پیاده‌سازی کنترل‌های امنیتی ارائه‌شده‌اند.

اولویت بالاتری از کد اولویت‌بندی ۳ یا P3 دارد، و کد اولویت‌بندی ۰ یا P0 در هیچ یک از مجموعه‌های پایه انتخاب نشده است. با استفاده از این اولویت‌بندی، سازمان‌ها می‌توانند ابتدا کنترل‌های امنیتی اصلی را پیاده کنند و سپس به سراغ کنترل‌هایی بروند که وابسته به کنترل‌های اصلی هستند. بدین ترتیب، سازمان‌ها می‌توانند کنترل‌ها را بر اساس منابع موجود، به شکل ساختارمند و با زمان‌بندی بهتری به کار گیرند. پیاده‌سازی کنترل‌های امنیتی بر اساس کدهای اولویت‌بندی به معنای کاهش مخاطرات تا حد تعیین‌شده نیست، مگر این که تمام کنترل‌های امنیتی مورد اشاره در طرح امنیتی پیاده‌سازی شوند. کدهای اولویت‌بندی تنها برای مشخص کردن ترتیب پیاده‌سازی کنترل‌های امنیتی به کار می‌روند و نباید از آن‌ها برای تصمیم‌گیری در خصوص انتخاب کنترل‌های امنیتی استفاده کرد.

۲–۳– مجموعه‌های پایه کنترل‌های امنیتی

سازمان‌ها باید مخاطرات مربوط به استفاده از اطلاعات و سیستم‌های اطلاعاتی در اجرای مأموریت‌ها و عملکردهای کسب‌وکار را به نحو مقتضی کاهش دهند. مهم‌ترین چالش پیش روی سازمان‌ها، تعیین مقرون‌به‌صرفه‌ترین و مناسب‌ترین مجموعه کنترل‌های امنیتی است که در صورت اجرا شدن، می‌توانند ضمن برآورده ساختن الزامات امنیتی تعریف‌شده در راهنمایی‌ها، استانداردها، مقررات، خط‌مشی‌ها، رهنمودها، دستورات اجرایی و قوانین فدرال، مخاطرات را نیز کاهش دهند. هیچ مجموعه‌ای از کنترل‌های امنیتی وجود ندارد که تمام دغدغه‌های امنیتی سازمان را پاسخ گوید. انتخاب بهترین مجموعه از کنترل‌های امنیتی به منظور کاهش مخاطرات به نحو مقتضی، وظیفه مهمی است که برای انجام آن به درک صحیح اولویت‌های سازمان، مأموریت‌ها و عملکردهای کسب‌وکار پشتیبانی‌شده توسط سیستم اطلاعاتی، و محیط کاری این سیستم نیاز است. با داشتن این درک و آگاهی، سازمان‌ها می‌توانند از محرمانگی، یکپارچگی و در دسترس بودن اطلاعات سازمانی و سیستم‌های اطلاعاتی اطمینان حاصل نمایند و نیازهای خود در زمینه کسب‌وکار و مأموریت را برآورده سازند. انتخاب، پیاده‌سازی و حفظ و نگهداری مجموعه مناسب کنترل‌های امنیتی به منظور حفاظت از سیستم اطلاعاتی به‌کارگرفته‌شده توسط سازمان، نیازمند همکاری تنگاتنگ با مالکان سیستم است. بدین ترتیب، سازمان می‌تواند تغییرات رخ‌داده در عملکردهای کسب‌وکار، مأموریت، محیط کاری و نحوه استفاده از سیستم‌ها را درک کند.

مفهوم کنترل اولیه[۵۳] برای این تعریف شده است که سازمان‌ها را یاری کند تا کنترل‌های امنیتی مناسبی را برای سیستم‌های اطلاعاتی انتخاب کنند. کنترل‌های اولیه نقطه آغاز فرایند انتخاب کنترل‌های امنیتی هستند. کنترل‌های امنیتی با توجه به دسته‌بندی امنیتی و میزان تأثیر سیستم‌های اطلاعاتی و بر اساس FIPS 199 و FIPS 200 انتخاب می‌شوند[۵۴]. در پیوست ت، لیستی از کنترل‌های امنیتی اولیه ارائه شده است. سه مجموعه کنترل امنیتی اولیه شناسایی شده‌اند که متناسب با سیستم‌های اطلاعاتی با تأثیر کم[۵۵]، متوسط[۵۶] و زیاد[۵۷] هستند. در این فرایند از علامتی استفاده می‌شود که در FIPS 200 تعریف شده و در بخش ۳,۱ این سند برای تهیه مجموعه پایه‌ای از کنترل‌های امنیتی با سطوح تأثیر مختلف به کار گرفته شده است[۵۸].

پیوست ج لیست جامعی از کنترل‌های امنیتی را برای سازمان‌ها و سیستم‌های اطلاعاتی ارائه می‌کند که بر اساس خانواده کنترل‌ها مرتب شده‌اند. فصل سوم شامل اطلاعاتی در زمینه نحوه استفاده از دسته‌بندی‌های امنیتی FIPS 199 و سطوح تأثیر FIPS 200 برای به‌کارگیری رهنمایی‌های اختصاصی[۵۹] و کاهش مخاطرات تا حد مطلوب است. راهنمایی‌های اختصاصی، که در بخش ۳,۲ به آن‌ها اشاره شده است، سازمان‌ها را یاری می‌کنند تا با استفاده از نتایج بررسی مخاطرات، مجموعه‌های پایه کنترل‌های امنیتی را به نحو مناسب تغییر دهند و تنظیم کنند. اقدامات اختصاصی اولیه عبارتند از: (۱) شناسایی و تخصیص کنترل‌های معمول، (۲) در نظر گرفتن ملاحظات مربوط به دامنه شمول و اعمال کردن آن‌ها، (۳) انتخاب کنترل‌های جبرانی، (۴) تخصیص مقادیر خاص به پارامترهای کنترل‌های امنیتی، (۵) تکمیل کردن مجموعه‌های پایه با تعداد دیگری از کنترل‌های امنیتی یا کنترل‌های پیشرفته، و (۶) ارائه اطلاعات تکمیلی برای پیاده‌سازی کنترل‌ها.

نکاتی برای پیاده‌سازی بهتر:

برخی کنترل‌های امنیتی و کنترل‌های پیشرفته در کاتالوگ کنترل‌های امنیتی (پیوست ج) وجود دارند که تنها در مجموعه‌های پایه با تأثیر بالاتر مشاهده می‌شوند و یا این که در هیچ یک از مجموعه‌های پایه نیستند.

---

[53] Baseline controls

[۵۴] سند CNSS 1253، راهنمایی‌هایی را در خصوص کنترل‌های امنیتی اولیه برای سیستم‌های امنیت ملی ارائه می‌کند.

[55] Low-impact

[56] Moderate-impact

[57] High-impact

[۵۸] کنترل‌های امنیتی اولیه لیست‌شده در پیوست ت، الزاماً مجموعه‌های مطلقی نیستند. این امر بدین دلیل است که سازمان‌ها بر اساس راهنمایی‌های ارائه‌شده در بخش ۳٫۲، می‌توانند مجموعه کنترل‌ها را با توجه به شرایط و ضوابط تعیین‌شده توسط مقامات مسئول و مستندسازی‌شده در طرح‌های امنیتی خود، تغییر دهند.

[59] Tailoring guidance

سازمان‌ها می‌توانند با استفاده از این کنترل‌های امنیتی و کنترل‌های پیشرفته مربوط به سیستم‌های اطلاعاتی، مجموعه‌های پایه کنترل‌های امنیتی را به گونه‌ای تنظیم و اصلاح کنند که به سطح حفاظتی مطلوب خود دست یابند. مجموعه کنترل‌های امنیتی موجود در طرح امنیتی باید برای کاهش مخاطرات موجود بر سر راه سرمایه‌ها و عملیات سازمان، افراد و سایر سازمان‌ها، و رساندن آن به سطح مطلوب کفایت کند.

۲-۴- تخصیص کنترل‌های امنیتی

در پیوست ج، سه نوع تخصیص برای کنترل‌های امنیتی در نظر گرفته شده است. این سه نوع تخصیص، موارد روبرو را تعیین می‌کنند: (۱) دامنه شمول کنترل‌ها، (۲) ماهیت اشتراکی کنترل‌ها، و (۳) مسئولیت توسعه، پیاده‌سازی، بررسی و صدور مجوز مربوط به کنترل‌ها. این تخصیص‌ها شامل کنترل‌های معمول[۶۰]، کنترل‌های سیستمی[۶۱]، و کنترل‌های هیبریدی[۶۲] هستند.

کنترل‌های معمول، آن دسته از کنترل‌های امنیتی هستند که پیاده‌سازی آن‌ها منجر به پدید آمدن قابلیت‌های کنترلی می‌شود که قابل انتقال به یک یا چند سیستم اطلاعاتی در سازمان هستند. کنترل‌های امنیتی در صورتی قابل انتقال به سایر سیستم‌های اطلاعاتی یا مؤلفه‌های سیستم‌های اطلاعاتی هستند که سیستم‌ها یا مؤلفه‌های مذکور تحت حفاظت کنترل‌های پیاده‌سازی‌شده باشند، اما این کنترل‌ها توسط موجودیت‌هایی غیر از موجودیت‌های مسئول، توسعه داده شوند، پیاده‌سازی و بررسی شوند، مجوز دریافت کنند، و پایش شوند. این موجودیت‌ها ممکن است داخل یا خارج سازمان باشند. قابلیت‌های امنیتی ارائه‌شده توسط کنترل‌های معمول می‌تواند نشأت گرفته از منابع مختلف باشد. از جمله این منابع می‌توان به سازمان‌ها، مأموریت‌ها و فرایندهای کسب‌وکار سازمان‌ها، سایت‌ها، بخش‌های مختلف، محیط‌های کاری، یا سایر سیستم‌های اطلاعاتی اشاره کرد. بسیاری از کنترل‌های مورد نیاز برای حفاظت از سیستم‌های اطلاعاتی سازمان (مانند آموزش و اطلاع‌رسانی در زمینه مسائل امنیتی، طرح‌های واکنش به رویدادها، دسترسی فیزیکی به تأسیسات، و قوانین رفتاری) را می‌توان از جمله کنترل‌های معمول به شمار آورد. علاوه بر این‌ها، برخی دیگر از کنترل‌های فناورانه نیز در این دسته قرار می‌گیرند (مانند زیرساخت کلید عمومی [PKI]، پیکربندی استاندارد امن برای سرورها و کلاینت‌ها، سیستم‌های کنترل دسترسی، حفاظت مرزی، و روش‌های بین دامنه‌ای). با مدیریت و مستندسازی متمرکز

[60] Common controls
[61] System-specific controls
[62] Hybrid controls

فرایند توسعه، پیاده‌سازی، بررسی، صدور مجوز و پایش کنترل‌های معمول، می‌توان هزینه‌های امنیی را در سیستم‌های اطلاعاتی مختلف کاهش داد.

سازمان، مسئولیت کنترل‌های عمومی را به مسئولین مربوطه محول می‌کند و فرایند توسعه، پیاده‌سازی، بررسی، صدور مجوز و پایش کنترل‌ها را هماهنگ و مدیریت می‌نماید[۶۳]. شناسایی کنترل‌های معمول را باید در سراسر سازمان انجام داد. لازم است که مدیر ارشد اطلاعات، مدیر ارشد امنیت اطلاعات، مسئول ارشد مدیریت مخاطرات، مقامات صدور مجوز، مالکان اطلاعات و وکلای مربوطه، مالکان سیستم‌های اطلاعاتی و مدیر امنیت سیستم‌های اطلاعاتی نقش فعالی در این فرایند داشته باشند. در این فرایند سازمانی، دسته‌بندی‌های امنیتی سیستم‌های اطلاعاتی و کنترل‌های امنیتی لازم برای کاهش مخاطرات ناشی از این سیستم‌ها در نظر گرفته می‌شوند (به «مجموعه‌های پایه کنترل‌ها امنیتی» در بخش ۲,۳ مراجعه کنید)[۶۴]. شناسایی کنترل‌های معمول که تنها بر بخشی از سیستم‌های اطلاعاتی سازمان تأثیر می‌گذارند نیز به روش مشابهی انجام می‌شود. ذی‌نفعان اصلی با همکاری یکدیگر، موقعیت‌های مناسب استفاده از کنترل‌های معمول در مأموریت و فرایند کسب‌وکار، سایت یا بخش‌های مختلف را شناسایی می‌کنند.

هنگامی که کنترل‌های معمول برای حفاظت از چند سیستم اطلاعاتی با سطوح تأثیر مختلف مورد استفاده قرار می‌گیرند، پیادسازی آن‌ها بر اساس بالاترین سطح تأثیر انجام می‌شود. اگر کنترل‌های معمول در بالاترین سطح تأثیر سیستم‌های اطلاعاتی به کار گرفته نشده باشند، مالکان سیستم باید این عامل را نیز در تحلیل مخاطرات خود مورد توجه قرار دهند (مثلاً تعدادی کنترل امنیتی را به کنترل‌های پیشرفته اضافه کنند، مقادیر تخصیص داده شده به پارامترهای کنترل‌های امنیتی را تغییر دهند، از کنترل‌های جبرانی استفاده کنند، یا برخی وجود خاص مأموریت و فرایند کسب‌وکار سازمان را تغییر دهند). پیاده‌سازی آن دسته از کنترل‌های معمول که مؤثر نیستند یا قابلیت‌های امنیتی کافی را برای سیستم‌های اطلاعاتی با سطح تأثیر بالاتر فراهم نمی‌آورند، می‌تواند تأثیر منفی قابل توجهی بر مأموریت و فرایند کسب‌وکار سازمان داشته باشد.

کنترل‌های معمول به طور کلی در طرح برنامه امنیت اطلاعات[۶۵] مستندسازی می‌شوند، مگر این که به عنوان بخشی از یک سیستم اطلاعاتی خاص پیاده‌سازی شده باشند. در این حالت، کنترل‌های مربوطه در طرح امنیتی

---

[۶۳] مدیر ارشد اطلاعات، مدیر ارشد امنیت اطلاعات یا سایر مقامات مربوطه، وظیفه توسعه، پیاده‌سازی، بررسی، صدور مجوز و پایش کنترل‌های معمول در موجودیت‌های مختلف داخل و خارج سازمان را به افراد مناسب واگذار می‌کنند.

[۶۴] تمامی کنترل‌های معمول شناسایی‌شده توسط سازمان، مورد بررسی قرار می‌گیرند تا مشخص شود که امکان استفاده از آن‌ها در سیستم‌های اطلاعاتی وجود دارد یا خیر. این کار معمولاً توسط مالکان سیستم‌های اطلاعاتی و مسئولین صدور مجوز انجام می‌شود.

[65] Information security program plan

آن سیستم مستندسازی می‌شوند[۶۶]. سازمان‌ها این آزادی عمل را دارند که کنترل‌های معمول را در یک سند یا در چند سند مختلف تشریح کنند. در صورتی که این کار در چند سند مختلف انجام شود، اسناد مذکور در واقع پیوست طرح برنامه امنیت اطلاعات خواهند بود. اگر طرح برنامه امنیت اطلاعات دربردارنده چند سند مختلف باشد، سازمان در هر سند مشخص می‌کند که چه افرادی مسئول فرایند توسعه، پیاده‌سازی، بررسی، صدور مجوز و پایش کنترل‌های معمول بوده‌اند. به عنوان مثال، ممکن است سازمان چنین تصمیم بگیرد که وقتی کنترل‌های حفاظت محیطی و فیزیکی خانواده PE مربوط به یک سیستم اطلاعاتی خاص نبوده و چند سیستم مختلف را پشتیبانی می‌کنند، دفتر مدیریت تأسیسات مسئولیت فرایند توسعه، پیاده‌سازی، بررسی، صدور مجوز و پایش منظم آن‌ها را بر عهده داشته باشد. هنگامی که کنترل‌های معمول در یک طرح امنیتی مجزای مربوط به یک سیستم اطلاعاتی قرار گرفته باشند (مثلاً کنترل‌های امنیتی به‌کارگرفته‌شده به عنوان بخشی از یک سیستم شناسایی ورود غیرمجاز، که امکان حفاظت مرزی قابل انتقال به سایر سیستم‌های اطلاعاتی سازمان را فراهم می‌آورد)، طرح برنامه امنیت اطلاعات بیان می‌کند که کدام طرح امنیتی، کنترل‌های معمول را تشریح می‌کند.

نکاتی برای پیاده‌سازی بهتر:

بهتر است که انتخاب کنترل‌های معمول، در تمامی سطح سازمان و به کمک مدیران ارشد (یعنی مالکان مأموریت و کسب‌وکار، مسئولین صدور مجوز، مدیران ارشد اطلاعات، مدیران ارشد امنیت اطلاعات، مالکان سیستم‌های اطلاعاتی، مالکان اطلاعات و وکلای مربوطه، و مسئولین بررسی مخاطرات) انجام شود. این افراد دانش کافی برای درک اولویت‌های سازمان، اهمیت سرمایه‌ها و عملیات سازمان، و اهمیت سیستم‌های اطلاعاتی را دارند. رهبران ارشد سازمان همچنین بهترین افراد برای انتخاب کنترل‌های معمول برای مجموعه‌های پایه کنترل‌های امنیتی، و تخصیص وظایف توسعه، پیاده‌سازی، بررسی، صدور مجوز و پایش این کنترل‌ها به افراد هستند.

[۶۶] **طرح**های برنامه امنیت اطلاعات در پیوست چ تشریح شده**اند**. **سازمان**ها باید اطمینان حاصل کنند که تمام قابلیت‌های امنیتی ارائه**شده توسط** کنترل‌های معمول (یعنی قابلیت‌های امنیتی منتقل‌شده به سایر موجودیت‌های سازمانی) با جزئیات کامل تشریح شده**اند و موجود**یت‌های مربوطه به درک صحیحی از پیاده‌سازی این کنترل‌ها رسیده**اند**.

مجوز کنترل‌های معمول، چه در سیستم‌های اطلاعاتی سازمان و چه در محیط‌های کاری پیاده‌سازی شوند، توسط مسئولینی صادر می‌شود که سطح اختیارات آن‌ها در مدیریت مخاطرات دست کم به اندازه اختیارات مسئولین سیستم‌های اطلاعاتی است که کنترل‌های مذکور را دریافت می‌کنند. نتیجه فرایند صدور مجوز کنترل‌های معمول، به اطلاع مالکان سیستم‌های اطلاعاتی و مسئولین صدور مجوز می‌رسد. یک طرح عملیاتی به همراه تعدادی هدف و مراحل مختلف نیز برای کنترل‌های معمول در نظر گرفته می‌شود. این کار بر اساس بررسی‌های مستقل انجام می‌شود، تا نتیجه اثربخش باشد. مالکان سیستم‌های اطلاعاتی که کنترل‌های معمول مربوط به آن‌ها چندان اثربخش نیست، در این خصوص تصمیم‌گیری می‌کنند که آیا کنترل‌های مذکور را به کار گیرند و مخاطرات این امر را بپذیرند، یا این که تغییرات و اصلاحاتی را در این کنترل‌ها انجام دهند. این تصمیمات مبتنی بر مخاطره، با توجه به منابع موجود، مدل‌های اعتماد به‌کارگرفته‌شده در سازمان، و میزان تحمل مخاطره سازمان و مسئولین اتخاذ می‌شوند[۶۷].

بررسی و پایش کنترل‌های معمول نیز مانند کنترل‌های خاصی است که در سیستم‌های اطلاعاتی سازمان به کار گرفته می‌شوند. از آنجا که کنترل‌های معمول بیش از یک سیستم را تحت تأثیر قرار می‌دهند، در مورد این کنترل‌ها به سطح اعتماد بالاتری نیاز است.

آن دسته از کنترل‌های امنیتی که جزو کنترل‌ها معمول نیستند، در دسته کنترل‌های سیستمی یا کنترل‌های هیبریدی قرار می‌گیرند. پیاده‌سازی کنترل‌های سیستمی، مسئولیت اولیه مالکان سیستم‌های اطلاعاتی و مسئولین صدور مجوز است. کنترل‌های هیبریدی آن دسته از کنترل‌ها هستند که بخشی از آن‌ها معمول و بخشی دیگر از آن‌ها سیستمی است. به عنوان مثال، ممکن است یک سازمان تصمیم بگیرد که کنترل امنیتی «روش‌های اجرایی و خط‌مشی واکنش به رویدادها» (IR-1) را به عنوان یک کنترل هیبریدی پیاده‌سازی نماید. در این حالت، بخشی از کنترل که مربوط به خط‌مشی است به عنوان بخش معمول و بخشی از آن که مربوط به روش‌های اجرایی است، به عنوان بخش سیستمی در نظر گرفته می‌شود. کنترل‌های هیبریدی همچنین ممکن است به عنوان قالبی برای تغییرات و اصلاحات آینده در نظر گرفته شوند. مثلاً ممکن است سازمان، کنترل امنیتی «برنامه‌ریزی اضطراری» (CP-2) را به عنوان قالب از پیش تعیین‌شده‌ای برای برنامه‌ریزی اضطراری کلی خود پیاده‌سازی کند و در ادامه در صورتی که نیاز باشد، مالکان سیستم‌های اطلاعاتی اقدام به اصلاح و تغییر آن برای سیستم‌های خود خواهند کرد.

---

[۶۷] **شماره** NIST 800-39 راهنمایی‌هایی را در خصوص مدل‌های اعتماد ارائه می‌کند. در این شماره، به مدل‌های اعتماد معتبر، تاریخی، میانجی و اجباری پرداخته شده است.

تقسیم‌بندی کنترل‌های امنیتی به کنترل‌های معمول و هیبریدی و سیستمی، سبب کاهش هزینه‌های سازمان در زمینه بررسی و پیاده‌سازی و همچنین منجر به استفاده منسجم‌تر و بهتر کنترل‌های امنیتی در سراسر سازمان می‌شود. هر چند که تقسیم‌بندی کنترل‌های امنیتی به کنترل‌های معمول و هیبریدی و سیستمی، یک مفهوم ساده و شهودی است، اما انجام این کار در عمل نیاز به هماهنگی و برنامه‌ریزی زیادی دارد. در سطح سیستم‌های اطلاعاتی، تعیین کنترل‌های معمول و هیبریدی و سیستمی نیازمند انجام اقدامات اولیه خاصی است. پیش از آن که سازمان در زمینه چگونگی پیاده‌سازی، اجرا و حفظ و نگهداری کنترل‌های امنیتی تصمیم‌گیری کند، ابتدا باید مشخص کند که به چه ظرفیت‌های امنیتی نیاز است.

طرح‌های امنیتی مربوط به سیستم‌های اطلاعاتی مشخص می‌کنند که کدام یک از کنترل‌های امنیتی مورد نیاز این سیستم‌ها در دسته کنترل‌های معمول قرار می‌گیرند و کدام یک به عنوان کنترل‌های سیستمی یا هیبریدی در نظر گرفته می‌شوند. مالکان سیستم‌های اطلاعاتی مسئولیت تعیین جزئیات پیاده‌سازی کنترل‌های معمول در کاربردهای سیستمی را بر عهده دارند. این جزئیات پیاده‌سازی، در طرح امنیتی سیستم‌های اطلاعاتی تعیین و تشریح می‌شوند. مدیران ارشد اطلاعاتی سازمان‌ها، با همکاری ارائه‌دهندگان کنترل‌های معمول (مانند مدیران سایت‌ها و تأسیسات، مدیران منابع انسانی، و مالکان سیستم‌های تعیین ورود غیرمجاز)، اقدامات لازم را انجام می‌دهند تا اطمینان حاصل شود که کنترل‌های مورد نیاز تهیه و پیاده‌سازی شده‌اند و اثربخشی آن‌ها بررسی شده است. طرح‌های امنیتی سیستم‌های اطلاعاتی به همراه طرح‌های برنامه امنیت اطلاعات سازمان، تمامی کنترل‌های امنیتی مورد استفاده در سازمان را پوشش می‌دهند.

دسته‌بندی کنترل‌های امنیتی به عنوان کنترل‌های معمول، هیبریدی و سیستمی، به شرایط و زمینه کاربرد آن‌ها بستگی دارد. تنها با بررسی زبان کنترل نمی‌توان معمول، سیستمی یا هیبریدی بودن آن را تعیین کرد. به عنوان مثال، ممکن است یک کنترل برای یک سیستم اطلاعاتی خاص سیستمی باشد، اما برای یک سیستم دیگر (که کنترل را از سیستم اول دریافت می‌کند) معمول به شمار آید. یکی از راه‌های تعیین این که یک کنترل سیستمی می‌تواند یک کنترل معمول برای سیستم‌های اطلاعاتی دیگر باشد یا خیر این است که بررسی کنیم چه افراد یا فرایندهای دیگری تحت تأثیر اجرای آن کنترل قرار می‌گیرند. اگر بخشی از سیستم اطلاعاتی که خارج از مرزهای سیستم قرار دارد به کنترل بستگی داشته باشد، کنترل مورد نظر می‌تواند معمول به شمار آید.

نکاتی برای پیاده‌سازی بهتر:

- سازمان‌ها، مخاطرات انتقالی[۶۸] حاصل استفاده از کنترل‌های معمول را در نظر می‌گیرند. پس از این که اطلاعات توسط مقامات مسئول کنترل‌ها بازنگری و تأیید شدند، طرح‌های امنیتی، گزارشات بررسی امنیت و طرح‌ها و اقدامات و اهداف در نظر گرفته شده برای کنترل‌های معمول (یا خلاصه‌ای از این اطلاعات) در اختیار مالکان سیستم‌های اطلاعاتی (در مورد سیستم‌هایی که کنترل‌ها به آن‌ها انتقال یافته‌اند) قرار می‌گیرند.

- سازمان‌ها اطمینان حاصل می‌نمایند که ارائه‌دهندگان کنترل‌های معمول، اطلاعات کنترلی را به‌روز نگه می‌دارند، زیرا این کنترل‌ها معمولاً در چند سیستم اطلاعاتی سازمان به کار گرفته می‌شوند. طرح‌های امنیتی، گزارشات بررسی امنیت و طرح‌ها و اقدامات و اهداف در نظر گرفته شده برای کنترل‌های معمول، توسط مسئولین صدور گواهی در تصمیم‌گیری‌های مبتنی بر مخاطره به کار گرفته می‌شوند. بنابراین، مخاطرات انتقالی از کنترل‌های معمول، عامل مهمی در اتخاذ تصمیمات مبتنی بر مخاطره است.

- سازمان‌ها اطمینان حاصل می‌کنند که ارائه‌دهندگان کنترل‌های معمول، می‌توانند تغییرات صورت‌گرفته در کنترل‌های معمول را که تأثیر منفی بر عملکرد آن‌ها دارند، به سرعت اطلاع‌رسانی نمایند. هنگامی که مشکلی در کنترل‌های معمول انتقالی رخ دهد (مثلاً هنگامی که بررسی اولیه یا بررسی مجدد یک کنترل معمول نشان دهد که نقایصی در آن وجود دارد، یا هنگامی که تعدید جدیدی بروز یابد که کنترل معمول توان حفاظت در برابر آن را نداشته باشد)، ارائه‌دهندگان کنترل‌های معمول مراتب را به مالکان سیستم اطلاع می‌دهند.

- سازمان‌ها تشویق می‌شوند که برای حفظ سوابق کنترل‌های معمول به‌کارگرفته‌شده در هر یک از سیستم‌های اطلاعاتی سازمان، از سیستم‌های مدیریت خودکار استفاده کنند. بدین ترتیب، ارائه‌دهندگان کنترل‌های معمول می‌توانند به طور سریع‌تر و بهتری با مالکان سیستم در ارتباط باشند.

- در صورتی که کنترل‌های معمول توسط موجودیت‌های خارجی (مانند ارائه‌دهندگان خدمات خارجی و/یا اشتراکی) به سازمان ارائه شوند، سازمان هماهنگی‌های لازم را با این موجودیت‌ها انجام می‌دهد تا اطلاعات مربوط به اثربخشی کنترل مورد استفاده را دریافت کند. اطلاعات دریافت‌شده از این موجودیت‌های خارجی در زمینه اثربخشی کنترل‌ها، در تصمیم‌گیری‌های صدور گواهی در نظر گرفته خواهد شد.

[68] Inherited risk

۲–۵– ارائه‌دهندگان خدمات خارجی

سازمان‌ها هر روز بیش از گذشته برای انجام فعالیت‌های کسب‌وکار خود به خدمات سیستم‌های اطلاعاتی ارائه‌شده توسط ارائه‌دهندگان خارج از سازمان وابسته می‌شوند. خدمات سیستم‌های اطلاعاتی خارجی عبارتند از فناوری‌های اطلاعاتی و پردازشی که خارج از مرزهای امنیتی سنتی به کار گرفته می‌شوند که سازمان برای سیستم‌های اطلاعاتی خود تعیین نموده است. این مرزهای سنتی، که با حوزه فیزیکی و کنترل سرمایه‌های سازمان ارتباط دارند، در اثر افزایش استفاده از خدمات خارجی، در حال گسترش هستند (چه از لحاظ فیزیکی و چه از لحاظ منطقی). خدمات خارجی توسط این موجودیت‌ها ارائه می‌شوند: (۱) موجودیت‌های اخل سازمان که خارج از مرزهای امنیتی تعیین‌شده برای سیستم‌های اطلاعاتی سازمان قرار دارند، (۲) موجودیت‌های خارج از سازمان در بخش عمومی (مانند مؤسسات فدرال) یا بخش خصوصی (مانند ارائه‌دهندگان خدمات تجاری)، و (۳) ترکیبی از بخش عمومی و خصوصی. خدمات سیستم‌های اطلاعاتی خارجی شامل مواردی از جمله استفاده از معماری‌های خدمت‌محور (SOA)، خدمات مبتنی بر کلاد (زیرساخت‌ها، پلت‌فرم‌ها و نرم‌افزارها)، یا مراکز داده هستند. خدمات سیستم‌های اطلاعاتی خارجی ممکن است توسط سیستم‌های اطلاعاتی سازمان به کار گرفته شوند، اما معمولاً بخشی از این سیستم‌ها به شمار نمی‌آیند. ممکن است در برخی شرایط، خدمات سیستم‌های اطلاعاتی خارجی به طور کامل جایگزین سیستم‌های اطلاعاتی داخل سازمان شوند یا عملکرد آن‌ها را به شدت افزایش دهند.

خط‌مشی‌های FISMA و OMB، ادارات فدرال استفاده‌کننده از خدمات خارجی برای پردازش، ذخیره‌سازی و انتقال اطلاعات فدرال را ملزم می‌دارند تا اطمینان حاصل نمایند که استفاده از این خدمات بر اساس الزامات امنیتی فدرال است. الزمات امنیتی مربوط به ارائه‌دهندگان خدمات خارجی، از جمله کنترل‌های امنیتی سیستم‌های اطلاعاتی خارجی، در قراردادها یا سایر موافقت‌نامه‌های رسمی تشریح شده‌اند[۶۹]. سازمان‌ها مسئول مخاطرات امنیتی حاصل از به‌کارگیری خدمات سیستم‌های اطلاعاتی ارائه‌شده توسط سازمان‌های دیگر هستند. این مخاطرات به عنوان بخشی از شرایط و ضوابط قرارداد با ارائه‌دهندگان خارجی، در چارچوب مدیریت مخاطره (RMF) تشریح شده‌اند. سازمان‌ها می‌توانند از ارائه‌دهندگان خارجی بخواهند تا تمام مراحل تشریح‌شده در RMF به جز مرحله صدور مجوز امنیتی را انجام دهند. انجام این مرحله از مسئولیت‌های فدرال است و با

---

[۶۹] هنگامی که سازمان‌ها خدمات کلاد را از ارائه‌دهندگان خارجی تهیه می‌کنند، با برنامه مدیریت صدور مجوز و مخاطرات فدرال (FedRAMP) مشورت می‌نمایند. FedRAMP، کنترل‌های امنیتی و بررسی‌های مستقل برای خدمات کلاد مختلف را ارائه می‌کند. برای کسب اطلاعات بیشتر، به **آدرس** اینترنتی http://www.fedramp.gov مراجعه کنید.

مدیریت مخاطرات امنیت اطلاعات در اثر استفاده از خدمات سیستم‌های اطلاعاتی خارجی ارتباط دارد[۷۰]. سازمان‌ها همچنین می‌توانند از ارائه‌دهندگان خارجی بخواهند تا مدارک دال بر رعایت الزامات فدرال را ارائه نمایند. اما در هر حال، مسئولیت نهایی تأیید امنیت این خدمات بر عهده ادارات فدرال است. در واقع این ادارت هستند که به سیستم‌های اطلاعاتی ارائه‌دهنده این خدمات، مجوز فعالیت می‌دهند.

رابطه با ارائه‌دهندگان خدمات خارجی به طرق مختلفی صورت می‌گیرد. به عنوان مثال، این کار ممکن است از طریق سرمایه‌گذاری مشترک، مشارکت تجاری، برون‌سپاری (به واسطه قراردادها، موافقت‌نامه‌های بین ادارات، همکاری‌های تجاری، و موافقت‌نامه‌های خدماتی)، اعطای مجوز و/یا مبادلات در زنجیره تأمین انجام شود. استفاده فزاینده از ارائه‌دهندگان خدمات خارجی و روابط در حال شکل‌گیری بین سازمان‌ها و این ارائه‌دهندگان، چالش‌های مهمی را برای سازمان‌ها، به ویژه در زمینه امنیت اطلاعات، پدید آورده است. این چالش‌ها عبارتند از:

- تعریف انواع خدمات سیستم‌های اطلاعاتی خارجی ارائه‌شده به سازمان‌ها
- تشریح چگونگی حفاظت از این خدمات خارجی بر اساس الزامات امنیت اطلاعات سازمان‌ها
- ضمانت قابل‌قبول بودن میزان مخاطرات حاصل از این خدمات خارجی برای سرمایه‌ها و فرایندهای سازمانی، افراد و سایر سازمان‌ها

میزان اعتماد به قابل قبول بودن سطح مخاطرات، به اعتماد سازمان به ارائه‌دهندگان خدمات خارجی بستگی دارد. در برخی موارد، این اعتماد وابسته به میزان کنترل سازمان بر ارائه‌دهندگان خدمات خارجی در زمینه به‌کارگیری کنترل‌های امنیتی و همچنین وابسته به شواهد و مدارک ارائه‌شده در خصوص اثربخشی این کنترل‌ها است[۷۱]. میزان کنترل سازمان بر ارائه‌دهندگان خارجی معمولاً تابع شرایط و ضوابط مندرج در قراردادها و موافقت‌نامه‌های امضاشده است. این کنترل می‌تواند بسیار زیاد (مانند موافقت‌نامه‌ها و قراردادهایی که الزامات امنیتی دقیقی برای ارائه‌دهندگان در آن‌ها گنجانده شده است) یا بسیار کم (مانند قراردادها یا موافقت‌نامه‌هایی برای دریافت خدمات عمومی مانند خدمات تجاری مخابراتی) باشد[۷۲]. در سایر موارد، میزان اعتماد مبتنی بر

---

[۷۰] به منظور مدیریت مؤثر مخاطرات امنیت اطلاعات، سازمان‌ها به آن دسته از سیستم‌های اطلاعاتی ارائه‌دهندگان خارجی که بخشی از خدمات و فناوری‌های اطلاعاتی (مانند زیرساخت‌ها، **پلت‌فرم**‌ها و نرم‌افزارها) ارائه‌شده به دولت فدرال هستند، اجازه فعالیت می‌دهند. الزامات صدور مجوز امنیتی، در بخش شرایط و ضوابط قرارداد با ارائه‌دهندگان خارجی این خدمات و فناوری‌ها تشریح شده**اند**.

[۷۱] میزان اعتماد سازمان به ارائه‌دهندگان خدمات خارجی می**تواند بسیار** متفاوت باشد. برخی از این ارائه‌دهندگان کاملاً مورد اعتماد هستند (مانند شرکای تجاری در یک سرمایه‌گذاری مشترک که از مدل کسب‌وکار و اهداف یکسان با سازمان تبعیت می‌کنند)، در حالی که برخی دیگر کمتر مورد اعتماد هستند و مخاطرات بیشتری را برای سازمان به دنبال دارند (مانند شرکای تجاری در یکی از فعالیت‌های سازمان، که در بخش دیگری از بازار جزو رقبا به شمار می‌آیند). شماره NIST 800-39، **مدل**‌های اعتماد مختلفی را ارائه می‌کند که سازمان می‌تواند در هنگام برقراری روابط با ارائه‌دهندگان خارجی از آن‌ها تبعیت نماید.

[۷۲] **ارا**ئه‌دهندگان تجاری خدمات عمومی معمولاً خدمات و مدل‌های کسب‌وکار خود را مبتنی بر مفهوم استفاده از ابزارها و منابع مشترک برای مشتریان مختلف طراحی می‌کنند. از این رو، سازمان‌ها باید از کنترل‌های امنیتی جبرانی برای حفاظت مناسب از سیستم‌های اطلاعاتی مبتنی بر

کنترل‌های امنیتی به‌کارگرفته‌شده و شواهد دال بر سطح اثربخشی این کنترل‌ها خواهد بود. به عنوان مثال، خدمات سیستم‌های اطلاعاتی ارائه‌شده به سازمان در روابط تجاری مستحکم، می‌توانند در حیطه پذیرش مخاطرات مسئولین سازمان، تا حد زیادی مورد اعتماد این مسئولین واقع شوند.

ارائه خدمات توسط ارائه‌دهندگان خارجی ممکن است باعث شود که برخی خدمات بدون امضای هیچگونه موافقت‌نامه‌ای بین دو سازمان مورد استفاده قرار گیرند. در صورتی که امکان تهیه و امضای موافقت‌نامه وجود داشته باشد (مثلاً از طریق قراردادها یا موافقت‌نامه‌های خدماتی)، سازمان‌ها اقدام به امضای آن‌ها می‌کنند و پیاده‌سازی کنترل‌های امنیتی لیست‌شده در پیوست ج سند حاضر را به عنوان شرطی ضروری قید می‌کنند. در صورتی که سازمان موقعیت امضای موافقت‌نامه با ارائه‌دهندگان خارجی را نداشته باشد (مثلاً در صورتی که خدمات به سازمان‌ها تحمیل شده باشند یا خدمات ارائه‌شده، خدمات عمومی باشند)، فروض امنیتی خاصی را در مورد خدمات ارائه‌شده تهیه و مستندسازی می‌کند. در صورتی که سازمان، خدمات سیستم‌های اطلاعاتی را از طریق روش‌های متمرکز (مانند قراردادهای دولتی با سازمان‌ها) فراهم کند، شاید بهتر و مقرون‌به‌صرفه‌تر باشد که پیش از امضای موافقت‌نامه، سطحی از اعتماد بین سازمان و ارائه‌دهنده خدمات خارجی ایجاد شود (مثلاً کنترل‌های امنیتی مورد نیاز تعیین شوند و مشخص شود که چه ضمانتی برای ارائه خدمات وجود دارد). سازمان‌هایی که خدمات سیستم‌های اطلاعاتی را از طریق قراردادهای متمرکز به دست می‌آورند، می‌توانند از طریق مذاکره به سطحی از اعتماد دست یابند. بدین ترتیب، نیازی به صرف هزینه و اعتمادسازی در مراحل بعد نخواهد بود[۷۳]. روش‌های متمرکز دریافت خدمات (مانند قراردادها) ممکن است نیازمند همکاری فعالانه سازمان‌ها نیز باشند. مثلاً ممکن است بر اساس شرایط و ضوابط قراردادها و موافقت‌نامه‌ها، لازم باشد که سازمان‌ها اقدام به نصب نرم‌افزارهای رمزگذاری کلید عمومی توصیه‌شده توسط ارائه‌دهندگان خدمات خارجی نمایند.

مسئولیت کاهش مخاطرات پیش‌بینی‌نشده استفاده از خدمات سیستم‌های اطلاعاتی خارجی، در نهایت بر عهده مسئولین صدور مجوز خواهد بود. در صورت بروز مشکلات امنیتی در اثر استفاده از خدمات خارجی، سازمان‌ها یک زنجیره اعتماد را با ارائه‌دهندگان این خدمات برقرار می‌نمایند. بر اساس سطح اعتماد تعیین‌شده، ارائه‌دهندگان خدمات، حفاظت کافی را در خصوص خدمات ارائه‌شده به سازمان تأمین می‌نمایند. بسته به تعداد

خدمات این ارائه‌دهندگان استفاده کنند، مگر این که همواره خدمات کاملاً متعهدانه‌ای را از آن‌ها دریافت کرده باشند. این تصمیمات باید بر اساس بررسی مخاطرات سازمانی و فعالیت‌های انجام‌شده برای کاهش این مخاطرات اتخاذ شوند.

[۷۳] به عنوان مثال، مسئولین تدارکات می‌**توانند** بر اساس شرایط و ضوابط قراردادها، برای سیستم‌های اطلاعاتی ارائه‌کننده خدمات خارجی به دولت فدرال صدور مجوز نمایند. بدین ترتیب، نیازی نخواهد بود که ادارات فدرال دریافت‌کننده این خدمات نیز پس از دریافت، برای این سیستم‌های اطلاعاتی مجوز صادر کنند (مگر این که خدماتی را درخواست کرده باشد که خارج از دامنه شمول قرارداد اولیه باشند).

سازمان‌های موجود در زنجیره مشتری-تأمین‌کننده و همچنین نوع روابط بین طرفین، زنجیره اعتماد می‌تواند شکل پیچیده‌ای به خود بگیرد. حتی ممکن است ارائه‌دهندگان خدمات خارجی، برخی از خدمات خود را به سازمان‌های دیگر برون‌سپاری کنند و بدین ترتیب مدیریت زنجیره اعتماد دشوارتر از قبل شود. بسته به ماهیت این خدمات، ممکن است سازمان‌ها متوجه شوند که اعتماد کردن کامل به ارائه‌دهندگان خدمات خارجی امکان‌پذیر نیست. این امر به دلیل غیر قابل اعتماد بودن ارائه‌دهندگان خدمات نیست، بلکه به دلیل مخاطرات طبیعی ناشی از برخی خدمات است[۷۴].

در صورتی که خدمات خارجی و/یا ارائه‌دهندگان آن‌ها به حد کافی مورد اعتماد نباشند، سازمان‌ها می‌توانند: (۱) مخاطرات را با استفاده از کنترل‌های جبرانی کاهش دهند، (۲) مخاطرات را تا حد تعیین‌شده تحمل نمایند، (۳) با بیمه کردن برخی ضررهای احتمالی، مخاطرات را منتقل نمایند، یا (۴) از برخی ارائه‌دهندگان خاص خدمات دریافت نکنند و بدین ترتیب از مخاطرات دوری کنند (این کار باعث تضعیف عملکرد سازمان در مأموریت‌ها و فرایندهای کسب‌وکار خود، و یا از دست رفتن عملکرد به طور کلی می‌شود)[۷۵]. به عنوان مثال، در مورد خدمات و/یا سیستم‌های اطلاعاتی مبتنی بر کلاد، سازمان‌ها ممکن است به عنوان یک کنترل جبرانی درخواست کنند که تمام اطلاعات ذخیره‌شده در کلاد رمزگذاری شود. از سوی دیگر، ممکن است سازمان‌ها تنها بخواهند بخشی از اطلاعات ذخیره‌شده در کلاد را رمزگذاری کنند (بسته به حساسیت اطلاعات). در این صورت سازمان مخاطرات بیشتری را می‌پذیرد، اما از سوی دیگر مخاطره ذخیره نکردن تمام اطلاعات به صورت غیر رمزگذاری‌شده را کاهش می‌دهد.

۲-۶- ضمانت و قابلیت اعتماد

ضمانت و قابلیت اعتماد سیستم‌های اطلاعاتی، مؤلفه‌های سیستم و خدمات سیستم‌های اطلاعاتی، تبدیل به یکی از بخش‌های مهم راهبرد مدیریت مخاطرات سازمان‌ها شده است. سیستم‌های اطلاعاتی چه برای پشتیبانی از سیستم کنترل ترافیک هوایی کشور و چه برای حمایت از مؤسسات مالی، نیروگاه‌های هسته‌ای یا خدمات نظامی به کار گرفته شده باشند، باید قابل اعتماد باشند و بتوانند با تهدیداتی که هر روز پیشرفته‌تر می‌شوند مقابله نمایند. برای درک این که سازمان‌ها چگونه سیستم‌های قابل اعتماد را انتخاب می‌کنند و ضمانت‌های سیستم‌ها چه نقشی در افزایش قابلیت اعتماد آن‌ها دارند، ابتدا باید عبارت «اعتماد» را تعریف کنیم. به طور

---

[۷۴] توقف برخی عملکردها به دلیل مسائل امنیتی نیز ممکن است مخاطراتی به همراه داشته باشد. امنیت تنها یکی از مسائلی است که باید در هنگام تعیین مخاطرات در نظر گرفت.

[۷۵] ممکن است ارائه‌دهندگان دیگری وجود داشته باشند که سطح اعتماد خدمات آن‌ها بیشتر باشد. البته معمولاً این ارائه‌دهندگان قیمت‌های بالاتری را نیز طلب می‌کنند.

کلی، اعتماد عبارت است از باور به این که یک موجودیت رفتاری قابل پیش‌بینی خواهد داشت و عملکردهای خود را در محیط‌های مختلف و شرایط مختلف به خوبی انجام خواهد داد. این موجودیت می‌تواند یک شخص، فرایند، سیستم اطلاعاتی، مؤلفه سیستم، مجموعه‌ای از سیستم‌ها یا هر ترکیبی از این موارد باشد.

از چشم‌انداز امنیت اطلاعات، اعتماد عبارت است از باور به این که یک موجودیت مرتبط با امنیت، رفتاری قابل پیش‌بینی در زمینه برآورده ساختن الزامات امنیتی در شرایط مختلف و در هنگام برخورد با وقفه‌ها، خطاهای انسانی، نقص عملکرد مؤلفه‌ها، و حملات مهاجمان خواهد داشت. اعتماد معمولاً پیوندی نزدیک با قابلیت‌های امنیتی دارد[۷۶] و می‌توان آن را با توجه به هر یک از مؤلفه‌های سیستم یا با در نظر گرفتن کلیت سیستم ارزیابی نمود. اما در سطح سیستم اطلاعاتی، اعتماد از طریق تشکیل مجموعه‌ای از مؤلفه‌های قابل اعتماد به دست نمی‌آید. اعتماد در این سطح در واقع برخاسته از تعاملات پیچیده بین موجودیت‌ها (یعنی مؤلفه‌های فنی، مؤلفه‌های فیزیکی و افراد) است. در این فرایند باید به عوامل تأثیرگذار بر مدیریت، توسعه، عملکرد و ثبات سیستم توجه داشت. در واقع برای اعتماد به یک قابلیت امنیتی، باید مبنای مناسبی برای اعتماد به موجودیت‌های مربوطه وجود داشته باشد تا بتوان اطمینان حاصل نمود که موجودیت‌های مذکور می‌توانند قابلیت‌های مورد نظر را فراهم آورند.

قابلیت اعتماد سیستم‌های اطلاعاتی، متأثر از این است که این سیستم‌ها تا چه حد می‌توانند محرمانگی، یکپارچگی و در دسترس بودن اطلاعات پردازش‌شده، ذخیره‌شده و منتقل‌شده را ضمانت کنند. سیستم‌های اطلاعاتی قابل اعتماد، آن دسته از سیستم‌های اطلاعاتی هستند که با وجود اختلالات محیطی، خطاهای انسانی، نقص‌های ساختاری، و حملات هدفمند مهاجمان، می‌توانند فعالیت‌های خود را در محدوده مخاطرات سازمان به صورت موفقیت‌آمیز انجام دهند –یعنی سیستم‌هایی که قابلیت اعتماد لازم برای انجام فرایندهای کسب‌وکار و مأموریت‌های محوله در شرایط تنش و عدم اطمینان را دارا هستند[۷۷].

قابلیت امنیتی

---

[۷۶] یک قابلیت امنیتی، ترکیبی است از کنترل‌های امنیتی متقابل (اقدامات حفاظتی و فعالیت‌های مقابله با حملات) اجرا شده با استفاده از ابزارهای فنی (عملکردهای سخت‌افزار، نرم‌افزار و ثابت‌افزار)، ابزارهای فیزیکی (ابزارهای حفاظتی و دستگاه‌های فیزیک)، و/یا ابزارهای رویه‌ای (رویه‌های به کار گرفته شده توسط افراد).

[۷۷] هرچند که اطلاعات مهم‌ترین مسئله است، مفهوم قابلیت اعتماد در مورد تمام سرمایه‌های مهم سازمان مصداق دارد. علاوه بر این، حفاظت از طریق فناوری (یعنی سخت‌افزار، نرم‌افزار و ثابت‌افزار)، عناصر فیزیکی (یعنی درها، قفل‌ها، و ابزارهای نظارتی)، و عناصر انسانی (یعنی افراد، فرایندها و رویه‌ها) انجام می‌شود.

سازمان‌ها می‌توانند پیش از انتخاب کنترل‌های امنیتی، مجموعه‌ای از قابلیت‌های امنیتی را تعریف نمایند. مفهوم قابلیت امنیتی بیان می‌دارد که حفاظت از اطلاعات پردازش‌شده، ذخیره‌شده یا منتقل‌شده توسط سیستم‌های اطلاعاتی، به ندرت تنها توسط ابزار حفاظتی (یعنی کنترل امنیتی) انجام می‌شود. در بسیاری از موارد، این حفاظت توسط ترکیبی از کنترل‌های امنیتی مختلف صورت می‌گیرد. به عنوان مثال، ممکن است سازمان‌ها بخواهند یک قابلیت امنیتی را برای احراز هویت امن از راه دور تعیین کنند. با انتخاب و ترکیب مجموعه‌ای از کنترل‌های امنیتی مورد اشاره در پیوست ج می‌توان به این قابلیت امنیتی دست یافت (مثلاً می‌توان از کنترل‌های IA-2[1]، IA-2[2]، IA-2[8]، IA-2[9] و SC-8[1] استفاده کرد). علاوه بر این، قابلیت‌های امنیتی ممکن است حوزه‌های مختلفی را پوشش دهند. به عنوان مثال می‌توان از ابزارهای فنی، ابزارهای فیزیکی، ابزارهای رویه‌ای و ترکیبی از آن‌ها استفاده کرد. ممکن است سازمان‌ها بخواهند علاوه بر قابلیت دسترسی امن از راه دور، از برخی قابلیت‌های دیگر که مبتنی بر ابزارهای فیزیکی هستند نیز برخوردار باشند.

با افزایش شمار کنترل‌های امنیتی لیست‌شده در پیوست ج در واکنش به ظهور تهدیدات جدیدتر و پیشرفته‌تر، سازمان‌ها باید قابلیت‌های امنیتی لازم برای حفاظت از مأموریت و فرایند کسب‌وکار خود را بشناسند و مجموعه‌ای از کنترل‌های امنیتی را برای تحقق این قابلیت‌ها شناسایی و تأمین کنند. این کنترل‌های امنیتی باید به نحو مناسبی طراحی، توسعه و اجرا شوند تا سازمان بتواند به قابلیت‌های مورد نظر دست یابد. آنچه تشریح شد نشان می‌دهد که سازمان‌ها باید چه دیدگاهی نسبت به مسائل امنیتی و حفاظتی خود داشته باشند. در واقع فراهم آوردن قابلیت‌های امنیتی، روش مناسبی است برای گردآوردن کنترل‌های امنیتی لازم و استفاده از آن‌ها برای تحقق یک هدف مشترک. این امر، مثلاً در هنگام ارزیابی اثربخشی کنترل‌های امنیتی، از اهمیت بالایی برخوردار است.

در گذشته تک تک کنترل‌ها به طور مجزا در نظر گرفته می‌شدند و بررسی می‌شد که هر یک از آن‌ها با موفقیت (کنترل رضیت‌بخش) یا با شکست (کنترل غیر رضایت‌بخش) همراه بوده‌اند. اما در واقع ممکن است شکست یک کنترل و یا حتی مجموعه‌ای از کنترل‌ها، تأثیری بر قابلیت امنیتی کلی مد نظر سازمان نگذارد. علاوه بر این، ساختن یک قابلیت امنیتی گسترده‌تر به سازمان اجازه می‌دهد تا شدت آسیب‌پذیری‌های مشاهده‌شده در سیستم‌های اطلاعاتی خود را بررسی کند و تعیین نماید که شکست یک کنترل خاص یا عدم استفاده از آن چه تأثیری بر قابلیت کلی مد نظر سازمان برای حفاظت از مأموریت‌ها و فرایندهای کسب‌وکار خود می‌گذارد. بدین ترتیب می‌توان عوامل اصلی را تحلیل کرد و پی برد که آیا شکست یک کنترل خاص سبب شکست سایر کنترل‌های مرتبط با آن نیز می‌شود یا خیر. در نهایت، تصمیمات صدور مجوز (یعنی تصمیمات پذیرش مخاطره)

بر اساس میزان تحقق قابلیت‌های امنیتی و میزان رعایت الزامات امنیتی اتخاذ می‌شوند. تصمیمات مبتنی بر مخاطره، ارتباط مستقیمی با سطح تحمل مخاطره سازمان دارند. این سطح تحمل بخشی از راهبرد مدیریت مخاطره سازمان است.

دو مؤلفه اصلی تأثیرگذار بر قابلیت اعتماد سیستم‌های اطلاعاتی عبارتند از عملکرد امنیتی[۷۸] و ضمانت امنیتی[۷۹]. عملکرد امنیتی معمولاً بر اساس ویژگی‌های امنیتی، عملکردها، مکانیسم‌ها، خدمات، روش‌های اجرایی، و معماری‌های به‌کارگرفته‌شده در سیستم‌های اطلاعاتی سازمان یا محیط‌های کاری تعریف می‌شود. ضمانت امنیتی، شاخصی است که نشان می‌دهد عملکرد امنیتی تا چه حد به خوبی پیاده‌سازی شده، بر اساس اهداف تعیین‌شده اجرا گردیده، الزامات امنیتی را رعایت کرده، به نتایج مطلوب انجامیده است، و بدین ترتیب خط‌مشی‌های امنیتی را اجرا کرده است. کنترل‌های امنیتی به گونه‌ای تعیین شده‌اند که هم عملکرد امنیتی و هم ضمانت امنیتی در آن‌ها در نظر گرفته شده است. تمرکز عمده برخی کنترل‌ها بر عملکرد امنیتی است (مانند PE-3 یا کنترل دسترسی فیزیکی، IA-2 یا شناسایی و احراز هویت، SC-13 یا حفاظت رمزنگاری، AC-2 یا مدیریت حساب‌ها). تمرکز عمده برخی دیگر از کنترل‌ها نیز بر ضمانت امنیتی است (مانند CA-2 یا برسی امنیتی، SA-17 یا طراحی و معماری امنیتی تولیدکنندگان، CM-3 یا کنترل تغییرات پیکربندی). برخی از کنترل‌ها نیز می‌توانند هم ضمانت امنیتی و هم عملکرد امنیتی را پشتیبانی کنند (مانند RA-5 یا شناسایی آسیب‌پذیری‌ها، SC-3 یا تفکیک عملکردهای امنیتی، AC-25 یا ایش ارجاعات). کنترل‌های امنیتی با یکدیگر ترکیب می‌شوند و یک قابلیت امنیتی را شکل می‌دهند. در ادامه، کنترل‌های ضمانتی مورد استفاده قرار می‌گیرند تا درجه اطمینان مطلوبی را در چاچوب تحمل مخاطرات سازمان فراهم آورند.

شواهد ضمانتی مربوط به فعالیت‌های توسعه‌ای و عملیاتی

ضمانت امنیتی مبتنی بر اقداماتی است که توسعه‌دهندگان، مجریان، اپراتورها، پرسنل تعمیر و نگهداری، و ارزیابان سیستم‌های اطلاعاتی انجام می‌دهند. اقدامات انجام‌شده توسط افراد و گروه‌های مختلف در جریان توسعه و پیاده‌سازی سیستم‌های اطلاعاتی، شواهد ضمانتی را تشکیل می‌دهند. بر اساس این شواهد، سطحی از اعتماد شکل می‌گیرد و مشخص می‌شود که عملکردهای امنیتی تا چه حد می‌توانند قابلیت‌های امنیتی مورد

[78] Security functionality
[79] Security assurance

نظر سازمان را فراهم آورند. عمق و دامنه شمول این اقدامات (چنان که در پیوست ث تشریح شده است)، نشان‌دهنده اثربخشی شواهد و تعیین‌کننده میزان اعتماد است. شواهد فراهم‌آمده توسط توسعه‌دهندگان، مجریان، اپراتورها، ارزیابان و پرسنل تعمیر و نگهداری در چرخه توسعه سیستم (شامل مراحی مانند طراحی و توسعه، ارزیابی، ضمانت و صدور گواهی)، سبب درک صحیح کنترل‌های امنیتی مورد استفاده سازمان می‌شود.

قدرت عملکرد امنیتی[۸۰] نقش مهمی در حصول قابلیت امنیتی مورد نیاز و رعایت الزامات امنیتی سازمان دارد. توسعه‌دهندگان سیستم‌های اطلاعاتی می‌توانند این موارد را در فرایند توسعه نرم‌افزار و سخت‌افزار و ثابت‌افزار در نظر گیرند و بدین ترتیب عملکرد امنیتی را ارتقا دهند: (۱) مدل‌ها و خط‌مشی‌های امنیتی مناسب، (۲) روش‌های طراحی و توسعه دقیق و ساختارمند، و (۳) اصول مهندسی امنیت و مهندسی سیستم مقتضی. محصولات ساخته‌شده توسط این فعالیت‌های توسعه‌ای (مانند ویژگی‌های عملکردی، طراحی‌های سطح بالا و سطح پایین، اطلاعات مربوط به چگونگی پیاده‌سازی [کدهای مبدأ و طراحی‌های سخت‌افزار]، نتایج آزمون‌های دینامیک/استاتیک و تحلیل کدها) شواهدی هستند که قابلیت اعتماد و اطمینان سیستم‌های اطلاعاتی و مؤلفه‌های تشکیل‌دهنده آن‌ها را نشان می‌دهند. شواهد امنیتی همچنین می‌توانند حاصل آزموهایی باشند که سازمان‌های مستقل و مورد اعتماد انجام می‌دهند (مانند کتابخانه‌های آزمون دارای معیار مشترک[۸۱]، کتابخانه‌های آزمون امنیتی و رمزنگاری[۸۲]، و سایر فعالیت‌های انجام‌شده توسط دولت و سازمان‌های بخش خصوصی)[۸۳].

علاوه بر شواهد تولیدشده در محیط‌های توسعه‌ای، سازمان‌ها می‌توانند در محیط‌های عملیاتی مربوط به ضمانت عملکرد و قابلیت‌های امنیتی نیز اقدام به تهیه این شواهد نمایند. شواهد عملیاتی شامل مواردی از جمله گزارشات نقایص، اسناد اقدامات جبرانی، نتایج گزارشات حوادث، و نتایج پایش‌های سازمانی هستند. این شواهد سازمان را یاری می‌کنند تا اثربخشی کنترل‌های امنیتی، تغییرات سیستم‌های اطلاعاتی و محیط‌های کاری، و تبعیت از استانداردها، خط‌مشی‌ها، مقررات، رهنمودها، و قوانین فدرال را بررسی کند. شواهد امنیتی، چه از فعالیت‌های عملیاتی و چه از فعالیت‌های توسعه‌ای به دست آمده باشند، سازمان‌ها را کمک می‌کنند تا به درک

---

[۸۰] قدرت امنیتی یک مؤلفه سیستم اطلاعاتی (یعنی سخت‌**افزار**، **نرم**‌افزار یا ثابت‌افزار) وابسته به این است که عملکرد امنیتی مؤلفه مذکور تا چه حد صحیح و کامل است و تا چه میزان می‌تواند در برابر حملات مستقیم (قدرت مکانیسم) و نیز در برابر دور زدن و دستکاری **اطلاعات از خود** مقاومت نشان دهد.

[81] Common Criteria Testing Laboratories

[82] Cryptographic/Security Testing Laboratories

[۸۳] به عنوان مثال، سازمان‌های ارزیاب، خدمات کلاد و ارائه‌دهندگان این خدمات را بر اساس برنامه مدیریت احراز هویت و مخاطرات فدرال (FedRAMP) ارزیابی می‌کنند. کتابخانه‌های آزمون دارای معیار مشترک، محصولات IT **را بر اساس استاندارد** ISO/IEC 15408 **آزمون** می‌کنند. کتابخانه‌های آزمون امنیتی و رمزنگاری، ماژول‌های رمزنگاری را با استفاده از استاندارد FIPS 140-2 آزمون می نمایند.

بهتری از کنترل‌های امنیتی مورد استفاده خود دست یابند. اقداماتی انجام‌شده توسط توسعه‌دهندگان، مجریان، اپراتورها، پرسنل تعمیر و نگهداری و ارزیابی، به عنوان شواهدی که از این اقدامات به دست آمده‌اند، سازمان‌ها را قادر می‌سازند تا تعیین کنند که عملکردهای امنیتی در سیستم‌های اطلاعاتی تا چه حد به طور مناسب اجرا شده‌اند، به اهداف مورد نظر دست یافته‌اند، الزامات امنیتی را رعایت کرده‌اند، و خط‌مشی‌های امنیتی را اجرا کرده‌اند. بدین ترتیب، اعتماد به قابلیت‌های امنیتی سازمان افزایش می‌یابد.

مباحثی در خصوص ضمانت امنیتی

سازمان‌ها، کنترل‌های ضمانتی را تعیین می‌کنند و با استفاده از آن‌ها، فعالیت‌های انجام‌شده برای گردآوری شواهد درباره رفتار و عملکرد سیستم‌های اطلاعاتی را مشخص می‌نمایند و این شواهد را به مؤلفه‌های ارائه‌دهنده آن رفتار یا عملکرد ارتباط می‌دهند. بر اساس شواهد مذکور، تا حدی اطمینان حاصل می‌شود که سازمان قادر به رعایت الزامات امنیتی و پشتیبانی از مأموریت و فرایند کسب‌وکار خود با توجه به تهدیدات موجود در محیط است.

عمق و دامنه شمول شواهد امنیتی می‌تواند ضمانت‌کننده اجرای عملکردها باشد. ویژگی‌های عمق و دامنه شمول، مربوط به روش‌های ارزیابی و تولید شواهد امنیتی هستند. روش‌های ارزیابی را می‌توان برای بررسی ضمانت‌های توسعه‌ای و عملیاتی به کار گرفت. در مورد ضمانت‌های توسعه‌ای، عمق با مسائلی همچون دقت، میزان جزئیات، و رسمیت محصولات تولیدشده در جریان طراحی و توسعه مؤلفه‌های سخت‌افزاری، نرم‌افزاری و ثابت‌افزاری سیستم‌های اطلاعاتی (از جمله ویژگی‌های عملکردی، طراحی سطح بالا، طراحی سطح پایین، کد مبدأ این مؤلفه‌ها) ارتباط دارد. در مورد ضمانت‌های عملیاتی، عمق به مسائلی همچون تعداد و نوع کنترل‌های امنیتی ضمانتی انتخاب و اجراشده می‌پردازد. در مقابل، دامنه شمول با روش‌های ارزیابی به‌کارگرفته‌شده در فرایندهای توسعه‌ای و عملیاتی ارتباط دارد و نشان می‌دهد که چه حیطه‌ای از مسائل در بررسی‌ها در نظر گرفته می‌شوند (مانند تعداد و نوع آزمون‌های انجام‌شده روی کد مبدأ، تعداد ماژول‌های نرم‌افزاری بررسی‌شده، تعداد

گره‌های شبکه و دستگاه‌های همراهی که آسیب‌پذیری‌های آن‌ها بررسی شده است، تعداد افرادی که با آن‌ها مصاحبه شده است تا درک اولیه آن‌ها از مسئولیت‌هایشان مشخص شود)[۸۴].

بررسی کنترل‌های امنیتی در جریان توسعه سیستم، سازمان‌ها را یاری می‌کند تا سیستم‌های اطلاعاتی و مؤلفه‌های قابل‌اعتمادتری در اختیار داشته باشند. با استفاده از این کنترل‌ها می‌توان اطمینان حاصل نمود که توسعه‌دهندگان، اصول و خط‌مشی‌های مناسبی را در زمینه امنیت سیستم به کار گرفته‌اند، یک معماری امن را طراحی کرده‌اند، فرایند پیکربندی را به خوبی مدیریت نموده‌اند، و تغییرات نرم‌افزارها و سیستم‌های امنیتی را به درستی تحت نظر دارند. پس از این که سیستم‌های اطلاعاتی اجرا شدند، با استفاده از کنترل‌های ضمانتی می‌توان از قابلیت اعتماد آن‌ها اطمینان حاصل نمود. با استفاده از این کنترل‌ها می‌توان صحت و یکپارچگی مؤلفه‌های نرم‌افزارها و ثابت‌افزارها را بررسی کرد، آزمون‌هایی را برای تعیین آسیب‌پذیری‌های سیستم‌های اطلاعاتی انجام داد، تنظیمات پیکربندی را پایش کرد، و خط‌مشی‌ها و رویه‌هایی را در خصوص پشتیبانی از عملیات و استفاده از سیستم‌ها توسعه داد.

مفاهیم تشریح‌شده (شامل الزامات امنیتی، قابلیت‌های امنیتی، کنترل‌های امنیتی، عملکرد امنیتی، و ضمانت امنیتی)، در قالب یک مدل با هم ترکیب شده‌اند. این مدل، قابلیت اعتماد سیستم‌های اطلاعاتی و مؤلفه‌های آن‌ها را بررسی می‌کند. شکل ۳ مؤلفه‌های اصلی این مدل و رابطه بین آن‌ها را نشان می‌دهد.

****

شکل ۳: مدل قابلیت اعتماد

****

فعالیت‌های توسعه‌ای و عملیاتی برای دستیابی به ضمانت بالا

دستیابی به سطح بالایی از ضمانت می‌تواند برای سازمان‌ها دشوار و پرهزینه باشد، اما گاهی اوقات این امر برای حصول اطمینان از انجام صحیح مأموریت‌ها، فرایندهای کسب‌وکار و عملیات اصلی سازمان ضرورت دارد. تعیین این که در کدام بخش‌های زیرساخت IT سازمان به ضمانت بالاتری نیاز است، بخشی از مرحله اول و مرحله دوم فرایند مدیریت مخاطرات سازمان به شمار می‌آید (شکل ۱ فصل دوم را ملاحظه کنید). این فعالیت‌ها هنگامی رخ می‌دهند که سازمان، الزامات امنیتی مورد نیاز برای حفاظت از عملیات سازمان (یعنی مأموریت، عملکردها،

[۸۴] **شماره** NIST 800-35A راهنمایی‌هایی را در خصوص تولید شواهد امنیتی در ارزیابی‌های امنیتی در حین توسعه سیستم ارائه می‌کند.

تصویر سازمان، و شهرت و اعتبار سازمان)، سرمایه‌های سازمان، افراد سازمان، سایر سازمان‌ها، و مردم را تعیین می‌نماید. تعیین الزامات امنیتی و قابلیت‌های امنیتی مربوطه، بخشی از فرایند مدیریت مخاطرات سازمان است که در شماره ویژه NIST 800-39 تشریح شده است. این امر به طور خاص در توسعه راهبرد واکنش به مخاطرات اهمیت دارد که پس از بررسی مخاطرات انجام می‌شود (هنگامی که سازمان اقدام به تعیین اولویت‌ها، فروض، محدودیت‌ها و سطح تحمل مخاطرات، بررسی تهدیدات، آسیب‌پذیری‌ها، مأموریت و فرایندهای کسب‌وکار، و احتمال وقوع مخاطرات می‌کند). پس از این که الزامات امنیتی و قابلیت‌های امنیتی در مراحل اول و دوم مشخص شدند (شامل الزامات ضمانتی برای فراهم آوردن شاخص‌های اعتماد به قابلیت‌های مطلوب)، الزامات و قابلیت‌های مذکور در طراحی معماری سازمان، مأموریت‌ها و فرایندهای کسب‌وکار، و سیستم‌های اطلاعاتی مورد نیاز برای پشتیبانی از این فرایندها به کار گرفته می‌شوند. سازمان‌ها می‌توانند با استفاده از چاچوب مدیریت مخاطرات (RMF) که در شمار ویژه NIST 800-37 تشریح شده است، اطمینان حاصل نمایند که سطح ضمانت مناسبی وجود دارد و سیستم‌های اطلاعاتی و مؤلفه‌های آن‌ها می‌توانند فرایندهای کسب‌وکار و مأموریت‌های سازمان را به خوبی انجام دهند. این فرایند معمولاً بخشی از مرحله سوم است، اما مثلاً برای انتخاب کنترل‌های معمول، می‌تواند همپوشانی‌هایی با مراحل اول و دوم نیز داشته باشد.

از دیدگاه توسعه سیستم‌ها و نرم‌افزار، ساختن سیستم‌های اطلاعاتی قابل اعتماد کار دشواری است. با این حال، اصولی در زمینه طراحی، معماری و اجرا وجود دارند که با استفاده از آن‌ها می‌توان قابلیت اعتماد را افزایش داد. اصول امنیتی[۸۵] اصلی عبارتند از سادگی، ماژول‌بندی[۸۶]، لایه‌بندی، تفکیک دامنه‌ها، حداقل بودن اختیارات، حداقل بودن عملکرد[۸۷]، تفکیک منابع و موارد دیگری از این دست. انتظار می‌رود که محصولات و سیستم‌های IT قابل اعتماد (یعنی محصولات و سیستم‌هایی که ضمانت امنیتی و عملکرد امنیتی خواسته‌شده را دارند)، مشکلات طراحی و ایرادات اجرایی کمتر و قابلیت بالاتری برای مقاومت در برابر تهدیدات مختلف داشته باشند. از جمله این تهدیدات می‌توان به مواردی از جمله حملات سایبری پیشرفته، بلایای طبیعی، تصادفات، و خطاهای ارادی و غیرارادی اشاره کرد[۸۸]. آسیب‌پذیری‌های مأموریت و فرایند کسب‌وکار سازمان و سیستم‌های

[85] Security principles
[86] Modularity
[87] Least functionality
[۸۸] **سازمان**‌ها از دیدگاه عملیاتی نیز اتکای زیادی به ضمانت‌های امنیتی دارند. این امر در بخش کنترل‌های ضمانتی و در جداول E-1 **تا** E-3 تشریح شده است. فعالیت‌های لازم برای ضمانت عملیاتی، متفاوت از فعالیت‌های مربوط به ضمانت توسعه‌ای هستند. از جمله این فعالیت‌ها می**توان** به تعیین و اعمال تنظیمات پیکربندی امنیتی روی محصولات IT، تهیه رویه‌ها و خطمشی‌ها، بررسی کنترل‌های امنیتی، و اجری پایش‌های مستمر اشاره کرد. در برخی موارد که سازمان‌ها فناوری اطلاعات ضعیفی را در اختیار دارند، ضمانت‌های عملیاتی گسترده‌تری را فراهم می**آورند تا** ضعف خود در زمینه مسائل IT را جبران کنند.

اطلاعاتی مربوطه در برابر تهدیدات، محیط کاری این سیستم‌ها، و حداکثر سطح قابل قبول مخاطرات امنیتی، تعیین‌کننده قابلیت اعتماد مورد نیاز هستند.

پیوست ث، حداقل الزامات ضمانتی برای سازمان‌ها و سیستم‌های اطلاعاتی فدرال را تشریح می‌کند و بر نقش کنترل‌های ضمانتی مورد اشاره در پیوست ت برای حصول اطمینان از رعایت این الزامات تأکید می‌نماید[۸۹].

چرا ضمانت امنیتی مهم است؟

اهمیت ضمانت امنیتی را می‌توان با استفاده از مثال کلید برق روی دیوار هال خانه توضیح داد. می‌توان کلید را در حالت روشن و خاموش قرار داد و مشاهده کرد که کلید، بر اساس ویژگی‌های عملکردی خود کار می‌کند. این فرایند، مشابه آزمایش کردن عملکرد سیستم اطلاعاتی و مؤلفه‌های آن به عنوان یک جعبه سیاه است. با این حال، سؤالات مهم‌تری نیز مطرح می‌شوند:

- آیا کلید برق کاری به جز آن چه برایش در نظر گرفته شده است را نیز انجام می‌دهد؟

- کلید برق از پشت دیوار چگونه به نظر می‌رسد؟

- در تولید کلید برق از چه مؤلفه‌هایی استفاده شده است و کلید چگونه سر هم شده است؟

- آیا تولید کننده کلید برق در ساخت این کلید از بهترین تجربیات صنعتی موجود در این زمینه بهره برده است؟

این مثال مشابه بسیاری از فعالیت‌های توسعه‌ای است که به کیفیت عملکرد امنیتی سیستم اطلاعاتی و مؤلفه‌های آن می‌پردازند. به عنوان مثال، می‌توان از اصول طراحی، روش‌های کدگذاری، تحلیل کد، آزمون و ارزیابی نام برد.

الزامات ضمانت امنیتی و کنترل‌های ضمانتی مربوطه در پیوست ث، مثال کلید برق را از نمای جلو دیوار بررسی می‌کنند. البته بسته به میزان اعتماد مورد نیاز برای مؤلفه، می‌توان بررسی‌های انجام‌شده را از نمای پشت دیوار نیز در نظر گرفت. در مورد آن دسته از مأموریت‌ها و فرایندهای کسب‌وکار که اهمیت کمتری دارند (یعنی سطح

[۸۹] **دستورالعمل** CNSS 1253، مجموعه پایه کنترل‌های امنیتی برای سیستم‌های امنیت ملی را برمی‌شمارد. بنابراین، کنترل‌های ضمانتی مربوط به سیستم‌های امنیت ملی می‌توانند با کنترل‌های امنیتی مربوط به سیستم‌های دیگر متفاوت **باشند**.

تأثیر پایینی دارند)، ممکن است سطح پایین‌تری از ضمانت نیز کافی باشد. اما با افزایش اهمیت مأموریت‌ها و فرایندهای کسب‌وکار (یعنی سطح تأثیر متوسط یا زیاد)، و همچنین با افزایش مخاطرات موجود در برابر سازمان‌ها و سیستم‌های اطلاعاتی، به سطح بالاتری از ضمانت نیز نیاز خواهد بود. علاوه بر این، با افزایش وابستگی سازمان‌ها به خدمات خارجی سیستم‌های اطلاعاتی و ارائه‌دهندگان این خدمات، مقوله ضمانت نیز اهمیت بالاتری به خود می‌گیرد. در این موارد، ضمانت بیشتر سبب می‌شود که سازمان‌ها بهتر بتوانند قابلیت‌های امنیتی خدمات ارائه‌شده به دولت فدرال و ارائه‌دهندگان این خدمات را بررسی و تأیید کنند. بنابراین، هنگامی که تهدیدات موجود در برابر سرمایه‌ها و عملیات سازمان، افراد، دیگر سازمان‌ها، و مردم زیاد و قابل‌توجه باشد، باید بیش از حالت‌های دیگر به بررسی مسائل امنیتی «از پشت دیوار» پرداخت.

۲-۷- بازبینی و توسعه

کنترل‌های امنیتی لیست‌شده در این سند، رهنودهایی عملی را برای مقابله با مخاطرات به سازمان‌ها و سیستم‌های اطلاعاتی فدرال ارائه می‌کنند. این کنترل‌های امنیتی[۹۰] به طور دوره‌ای و به دقت بررسی و بازبینی می‌شوند تا از پوشش داده شدن موارد زیر در آن‌ها اطمینان حاصل شود:

- تجربیات آموخته‌شده از به‌کارگیری این کنترل‌ها
- خط‌مشی‌ها، مقررات، رهنمودها، دستورات اجرایی، و قوانین جدید فدرال
- الزامات امنیتی جدید
- روش‌های حمله، آسیب‌پذیری‌ها و تهدیدات نوظهور
- موجود بودن فناوری‌های نوین

انتظار می‌رود که کنترل‌های امنیتی مورد اشاره در کاتالوگ کنترل‌های امنیتی به مرور زمان تغییر کنند، زیرا برخی کنترل‌ها باطل می‌شوند، بازبینی می‌شوند و یا اضافه می‌گردند. کنترل‌های امنیتی تعریف‌شده در مجموعه‌های پایه سطح کم، متوسط و زیاد نیز به مرور زمان عوض می‌شوند، زیرا سطح امنیت و تلاش‌هایی که سازمان‌ها باید برای مقابله با مخاطرات انجام دهد نیز تغییر می‌کنند. علاوه بر نیاز به تغییر، سازمان‌ها باید مسئله نیاز به ثبات را نیز مدنظر قرار دهند. بدین منظور، تغییرات صورت‌گرفته در کنترل‌های امنیتی باید توسط بخش خصوصی و بخش دولتی بازبینی و بررسی شوند تا اجماع و توافقی در زمینه این تغییرات صورت گیرد. با انجام

[۹۰] کنترل‌های حریم خصوصی لیست‌شده در پیوست د نیز بر اساس معیارهای مشابه، به صورت منظم به‌روزرسانی می‌شوند.

این کار، دولت فدرال و پیمانکاران و سایر سازمان‌ها به مرور زمان به یک کاتالوگ امنیتی دست خواهند یافت که شامل مجموعه باثبات، منعطف و مناسبی از کنترل‌های امنیتی است.

فصل سوم

فرایند

انتخاب و تعیین ویژگی‌های کنترل‌های امنیتی

در این فصل، فرایند انتخاب و تعیین ویژگی‌های کنترل‌های امنیتی و کنترل‌های پیشرفته سیستم‌های اطلاعاتی سازمان‌ها را بررسی می‌کنیم و به این موارد می‌پردازیم: (۱) انتخاب مجموعه‌های پایه مناسبی از کنترل‌های امنیتی؛ (۲) اصلاح و ارتقای مجموعه‌های پایه؛ (۳) مستندسازی فرایند انتخاب کنترل‌های امنیتی؛ و (۴) پیاده‌سازی فرایند انتخاب کنترل در سیستم‌های جدید و سیستم‌های بازمانده از قبل.

۳–۱– انتخاب مجموعه‌های پایه مناسبی از کنترل‌های امنیتی

به منظور انتخاب کنترل‌های امنیتی مناسب برای سیستم‌های اطلاعاتی و محیط کاری آن‌ها، و همچنین به منظور تعیین ویژگی‌های این کنترل‌ها، سازمان‌ها ابتدا اهمیت و حساسیت اطلاعاتی که باید توسط این سیستم‌ها پردازش، ذخیره یا منتقل شوند را بررسی می‌کنند. این فرایند که دسته‌بندی امنیتی نام دارد، در FIPS 199 تشریح شده است[۹۱]. استاندارد دسته‌بندی امنیتی، مبتنی بر یک مفهوم ساده و شناخته‌شده است. این مفهوم عبارت است از تعیین اثرات منفی بالقوه روی سیستم‌های اطلاعاتی سازمان. بر اساس نتایج دسته‌بندی امنیتی، می‌توان کنترل‌های امنیتی (یعنی ابزارهای حفاظت و مقابله با تهدیدات) را به گونه‌ای انتخاب کرد که حفاظت مناسبی از سیستم‌های اطلاعاتی به عمل آید. کنترل‌های امنیتی انتخاب‌شده برای سیستم‌های اطلاعاتی، متناسب با تهدادتی هستند که در صورت از دست رفتن محرمانگی و یکپارچگی اطلاعات یا از دسترس خارج شدن آن‌ها، سرمایه‌ها و عملیات سازمان، افراد، سایر سازمان‌ها و مردم را تهدید می‌کنند. سند FIPS 199، سازمان‌ها را ملزم می‌کند تا سیستم‌های اطلاعاتی را با توجه به اهداف امنیتی محرمانگی، یکپارچگی و در دسترس بودن، به عنوان سیستم‌های با تأثیر کم، متوسط یا زیاد دسته‌بندی کنند (گام اول چارچوب مدیریت مخاطره). این تأثیرات بالقوه تخصیص‌یافته به اهداف امنیتی، بالاترین مقادیری هستند که در دسته‌های امنیتی برای هر یک از انواع اطلاعات پردازش‌شده، ذخیره‌شده، و منتقل‌شده توسط سیستم‌های

[۹۱] **دستورالعمل** CNSS 1253، راهنمایی‌هایی را در خصوص دسته‌بندی امنیتی سیستم‌های امنیت ملی ارائه می‌کند.

اطلاعاتی در نظر گرفته شده‌اند[۹۲]. قالب تعمیم‌یافته برای بیان دسته امنیتی (SC) یک سیستم اطلاعاتی به شرح زیر است:

دسته امنیتی سیستم اطلاعاتی = {(محرمانگی، تأثیر)، (یکپارچگی، تأثیر)، (در دسترس بودن، تأثیر)}

که مقدار تخصیص‌یافته به عبارت «تأثیر» می‌تواند کم، متوسط یا زیاد باشد

از آنجا که تأثیر عوامل محرمانگی، یکپارچگی و در دسترس بودن ممکن است همواره برای یک سیستم اطلاعاتی خاص یکسان نباشد، در FIPS 200 برای انتخاب مجموعه پایه مناسبی از کنترل‌های امنیتی از میان سه مجموعه ارائه‌شده در پیوست ت، از مفهوم واترمارک قوی[۹۳] (که در FIPS 199 معرفی شده) استفاده شده است[۹۴]. بدین ترتیب، یک سیستم اطلاعاتی با تأثیر کم به عنوان سیستمی تعریف می‌شود که تمام اهداف امنیتی آن سطح پایین هستند. یک سیستم با تأثیر متوسط، سیستمی است که دست کم یکی از اهداف امنیتی آن سطح متوسط است و هیچ یک از اهداف امنیتی آن نیز سطح بالا نیستند. در نهایت، یک سیستم با تأثیر زیاد سیستمی است که دست کم یکی از اهداف امنیتی آن سطح بالا است.

نکاتی برای پیاده‌سازی بهتر:

برای تعیین سطح تأثیر یک سیستم اطلاعاتی:

- ابتدا انواع مختلف اطلاعاتی که باید توسط سیستم پردازش، ذخیره یا منتقل شوند را تعیین کنید. شماره ویژه NIST 800-60، اطلاعاتی را در این خصوص ارائه کرده است.

- در مرحله دوم، محرمانگی، یکپارچگی و در دسترس بودن هر یک از انواع اطلاعات را بر اساس سطوح تأثیر به دست آمده از FIPS 199 و توصیه‌های ارائه‌شده در شماره ویژه NIST 800-60 دسته‌بندی کنید.

---

[۹۲] شماره ویژه NIST 800-600 **با نام** «راهنمایی‌هایی برای اختصاص دادن انواع مختف اطلاعات و سیستم‌های اطلاعاتی به دسته‌های امنیتی»، اطلاعاتی را در مورد اختصاص دسته‌های امنیتی به سیستم‌های اطلاعاتی ارائه می‌کند.

[93] high water mark

[۹۴] مفهوم واترمارک قوی به این دلیل به کار گرفته می‌شود که وابستگی‌های زیادی بین اهداف امنیتی محرمانگی، یکپارچگی و در دسترس بودن وجود دارد. در بسیاری از موارد، توجه کمتر به یکی از این اهداف امنیتی، بر سایر اهداف امنیتی نیز تأثیر می‌گذارد. در نتیجه، کنترل‌های امنیتی بر اساس اهداف امنیتی دسته‌بندی نمی‌شوند. در عوض، کنترل‌های امنیتی به یک سری مجموعه پایه تقسیم می‌شوند تا بتوانند از دسته‌های مختلف سیستم‌های اطلاعاتی بر اساس میزان تأثیر آن‌ها محافظت به عمل آورند.

- در مرحله سوم، دسته امنیتی سیستم اطلاعاتی را از میان دسته‌های موجود تعیین کنید. بدین منظور باید بالاترین میزان تأثیر اهداف امنیتی (محرمانگی، یکپارچگی و در دسترس بودن) را مشخص نمایید.

- در مرحله چهارم، میزان تأثیر کلی سیستم اطلاعاتی را با توجه به سطوح تأثیر اهداف امنیتی تعیین کنید.

توجه: سازمان‌ها برای دسته‌بندی سیستم‌های امنیت ملی از CNSSI 1253 استفاده می‌کنند.

پس از این که سطح تأثیر سیستم اطلاعاتی مشخص شد، سازمان‌ها فرایند انتخاب کنترل‌های امنیتی را آغاز می‌کنند (گام دوم چارچوب مدیریت مخاطره). مرحله اول انتخاب و تعیین ویژگی‌های کنترل‌های امنیتی سیستم‌های اطلاعاتی، انتخاب مجموعه پایه مناسبی از کنترل‌های امنیتی است[۹۵]. انتخاب مجموعه پایه کنترل‌های امنیتی، بر اساس سطوح تأثیر مورد اشاره در FIPS 200 و همچنین فرایند دسته‌بندی امنیتی فوق انجام می‌شود. سازمان‌ها یکی از سه مجموعه پایه کنترل‌های امنیتی مورد اشاره در پیوست ت را انتخاب می‌کنند که متناظر با سیستم‌های اطلاعاتی با تأثیر کم، متوسط و زیاد هستند[۹۶]. توجه داشته باشید که تمام کنترل‌های امنیتی به مجموعه‌های پایه تخصیص داده نمی‌شوند. این امر در جدول ت-۲ با عبارت «انتخاب‌نشده» نشان داده شده است. به طور مشابه، همان طور که در جدول‌های ت-۳ تا ت-۱۹ نشان داده شده است، همه کنترل‌های پیشرفته نیز به مجموعه‌های پایه تخصیص داده نمی‌شوند. آن دسته از کنترل‌های پیشرفته که به مجموعه‌های پایه اختصاص داده شده‌اند، با علامت X در ستون‌های تأثیر کم و متوسط و زیاد قابل شناسایی هستند. عبارت «مجموعه پایه» به صورت عامدانه انتخاب شده است. کنترل‌های امنیتی و کنترل‌های پیشرفته موجود در مجموعه‌های پایه، در واقع نقطه آغاز هستند و بر اساس راهنمایی‌هایی که در بخش ۳،۲ ارائه شده است، می‌توان برخی از آن‌ها را حذف کرد، کنترل‌های دیگری به آن‌ها افزود، یا این که آن‌ها را تغییر داد.

مجموعه‌های پایه کنترل‌های امنیتی مورد اشاره در پیوست ت، برای تأمین نیازهای امنیتی دسته گسترده‌ای از افراد و سازمان‌ها در نظر گرفته شده‌اند. برخی فروضی که در پیوست ت در مورد مجموعه‌های پایه در نظر گرفته شده‌اند عبارتند از: (۱) محیط‌های کاری سیستم‌های اطلاعاتی سازمان؛ (۲) ماهیت عملیات انجام‌شده توسط سازمان؛ (۳) عملکردهای به‌کارگرفته‌شده در سیستم‌های اطلاعاتی؛ (۴) انواع تهدیداتی که سازمان‌ها، مأموریت‌ها

[۹۵] فرایند کلی انتخاب کنترل‌های امنیتی را می‌توان بر اساس راهنمایی‌های ارائه‌شده در بخش ۳/۳ با نام «ایجاد پوشش‌ها»، و همچنین بر اساس موارد مطرح‌شده در پیوست د با نام «قالب‌ها»، ارتقا داد.

[۹۶] دستورالعمل CNSS 1253، مجموعه‌های پایه کنترل‌های امنیتی مربوط به سیستم‌های امنیت ملی را تشریح می‌کند.

و فرایندهای کسب‌وکار، و سیستم‌های اطلاعاتی با آن‌ها مواجه‌اند؛ و (۵) انواع اطلاعات پردازش‌شده، ذخیره‌شده یا منتقل‌شده توسط سیستم‌های اطلاعاتی. تبیین این فروض، یکی از گام‌های اصلی در «تعیین چارچوب مخاطرات» است که در شماره ویژه NIST 800-39 به آن پرداخته شده است. برخی از فروض مربوط به مجموعه‌های پایه مورد اشاره در پیوست ت عبارتند از:

- سیستم‌های اطلاعاتی در تأسیسات فیزیکی تعبیه شده‌اند؛
- اطلاعات و داده‌های کاربری در سیستم‌های اطلاعاتی تقریباً پایدار هستند[۹۷]؛
- سیستم‌های اطلاعاتی، عملیات خود را به صورت چندکاربری[۹۸] انجام می‌دهند (به صورت پشت‌سرهم یا به صورت هم‌زمان)؛
- برخی داده‌ها و اطلاعات کاربری موجود در سیستم‌های اطلاعاتی را نمی‌توان با کاربران مجاز دیگری که به این سیستم‌ها دسترسی دارند، به اشتراک گذاشت؛
- سیستم‌های اطلاعاتی در محیط‌های شبکه‌ای کار می‌کنند؛
- سیستم‌های اطلاعاتی اهداف عمومی مختلفی دارند؛
- سازمان‌ها دارای ساختارها، منابع و زیرساخت‌های لازم برای پیاده‌سازی کنترل‌ها هستند[۹۹].

در صورتی که یک یا چند مورد از این فروض رعایت نشده باشند، ممکن است برخی کنترل‌های امنیتی اختصاص‌یافته به مجموعه‌های پایه در پیوست ت نیز عملی نباشند. برای حل این مشکل می‌توان کنترل‌ها را با توجه به موارد گفته‌شده در بخش ۳,۲ و نتایج بررسی مخاطرات سازمانی، اصلاح کرد. برخی شرایط نیز وجود دارند که ممکن است در مجموعه‌های پایه به آن‌ها پرداخته نشده باشد. این شرایط عبارتند از:

- وجود تهدیدات داخلی در درون سازمان؛
- پردازش، ذخیره یا منتقل شدن اطلاعات و داده‌های محرمانه توسط سیستم‌های اطلاعاتی؛
- وجود تهدیدات جدی و دائمی (APT)[۱۰۰] در درون سازمان؛
- لزوم حفاظت ویژه از برخی اطلاعات و داده‌ها به موجب خط‌مشی‌ها، مقررات، رهنمودها و قوانین فدرال؛
- لزوم برقراری ارتباط بین سیستم‌های اطلاعاتی با سایر سیستم‌های فعال در حوزه‌های امنیتی مختلف.

---

[۹۷] **اطلاعات و داده**‌های پایدار، آن دسته از داده‌ها و اطلاعاتی هستند که برای مدت طولانی (مثلاً روزها یا هفته‌ها) باقی می‌مانند.

[98] multi-user

[۹۹] به طور کلی، ادارات و دفاتر فدرال این فروض را رعایت می‌کنند. رعایت این موارد برای سازمان‌های غیر فدرال مانند شهرداری‌ها و پیمانکاران کوچک دشوارتر است. این سازمان‌ها ممکن است اندازه کوچکی داشته یا منابع کافی برای تحقق این قابلیت‌های امنیتی را در اختیار نداشته باشند. سازمان‌ها، این موارد را در تصمیم‌گیری‌های خود در زمینه مخاطرات لحاظ می‌کنند.

[100] advanced persistent threats

در صورت وجود هر یک از شرایط فوق، ممکن است نیاز به پیاده‌سازی برخی کنترل‌های امنیتی دیگر باشد که در پیوست ج لیست شده‌اند. در این صورت همچنین می‌توان کنترل‌های امنیتی را با توجه به موارد گفته‌شده در بخش ۳,۲ و نتایج بررسی مخاطرات سازمانی اصلاح کرد (به ویژه در مورد مکمل‌های کنترل‌های امنیتی).

۳-۲- تغییر و اصلاح کنترل‌های امنیتی اولیه

پس از انتخاب مجموعه پایه کنترل‌های امنیتی از پیوست ت، سازمان‌ها فرایند تغییر و اصلاح را شروع می‌کنند تا کنترل‌های امنیتی انطباق بیشتری با شرایط خاص سازمان داشته باشند (منظور از این شرایط، مأموریت و فرایند کسب‌وکار سازمان، سیستم‌های اطلاعاتی و محیط‌های کاری آن‌ها است). فرایند تغییر و اصلاح شامل مراحل زیر است:

- تعیین و اختصاص کنترل‌های معمول در مجموعه‌های پایه کنترل‌های امنیتی؛
- در نظر گرفتن ملاحظات مربوط به دامنه شمول در خصوص مجموعه‌های بعدی کنترل‌های اولیه؛
- انتخاب کنترل‌های امنیتی جبرانی، در صورت لزوم؛
- اختصاص مقادیر خاص به پارامترهای کنترل‌های امنیتی تعیین‌شده توسط سازمان از طریق عبارت‌های انتخاب و اختصاص؛
- تکمیل مجموعه‌های پایه با استفاده از تعدادی دیگر از کنترل‌های امنیتی و کنترل‌های پیشرفته، در صورت لزوم؛
- ارائه اطلاعات اضافی در مورد پیاده‌سازی کنترل‌های امنیتی، در صورت لزوم.

فرایند تغییر و اصلاح (به عنوان یکی از مراحل انتخاب و تعیین ویژگی‌های کنترل‌های امنیتی) در واقع بخشی از فرایند جامع مدیریت مخاطرات سازمان است. مراحل فرایند مدیریت مخاطرات سازمان عبارتند از تعیین چارچوب، بررسی، واکنش به مخاطرات امنیت اطلاعات و پایش این مخاطرات. سازمان‌ها از راهنمایی‌های مدیریت مخاطرات به منظور تصمیم‌گیری بهتر در خصوص این مخاطرات استفاده می‌کنند و بر این اساس تعیین می‌نمایند که کنترل‌های امنیتی موجود در مجموعه‌های پایه تا چه حد قابل اجرا هستند. در نهایت، سازمان‌ها می‌توانند با استفاده از فرایند تغییر و اصلاح، به یک خط‌مشی امنیتی مقرون به صرفه مبتنی بر مخاطرات دست یابند که به خوبی از مأموریت و فرایند کسب‌وکار آن‌ها پشتیبانی نماید. پیش از پیاده‌سازی کنترل‌های امنیتی، مسئولین صدور مجوز با همکاری برخی مقامات سازمانی (یعنی مدیر ارشد مخاطرات، مدیر ارشد اطلاعات، مدیر ارشد امنیت اطلاعات، مالکان سیستم‌های اطلاعاتی، و ارائه‌دهندگان کنترل‌های معمول) اقدام به تأیید تغییرات

و اصلاحات می‌کنند. سازمان‌ها می‌توانند تغییرات و اصلاحات مربوط به تمامی سیستم‌های اطلاعاتی را در سطح سازمانی، در پشتیبانی از یک مأموریت یا فرایند کسب‌وکار خاص، در سطح هر یک از سیستم‌های اطلاعاتی، یا بر اساس ترکیبی از هر یک از این موارد اجرا کنند[۱۰۱].

سازمان‌ها نمی‌توانند برای سهولت عملیات، اقدام به حذف کنترل‌های امنیتی نمایند. تغییرات و اصلاحات باید بر اساس مأموریت‌ها و فرایندهای کسب‌وکار و همچنین با توجه به مخاطرات موجود در پیش روی سازمان، انجام‌پذیر و عملی باشند[۱۰۲]. تصمیمات مربوط به تغغیر و اصلاح، و همچنین منطق نهفته در پس این تصمیمات، در طرح‌های امنیتی سیستم‌های اطلاعاتی سازمان ثبت و مستندسازی می‌شوند. هر یک از کنترل‌های امنیتی موجود در مجموعه‌های پایه، توسط سازمان (یعنی ارائه‌دهنده کنترل معمول) یا مالک سیستم اطلاعاتی تشریح می‌شود. اگر یک کنترل امنیتی کنار گذاشته شود، منطق این امر در طرح امنیتی مستندسازی می‌شود (یا ارجاعاتی به اسناد مربوطه داده می‌شود) و به عنوان بخشی از فرایند تأیید طرح امنیتی، به تأیید مسئولین سازمانی ذی‌ربط می‌رسد[۱۰۳].

مستندسازی تصمیمات مهم مدیریت مخاطرات، یکی از موارد ضروری در فرایند انتخاب کنترل‌های امنیتی است. بدین ترتیب، مسئولین صدور مجوز اطلاعات کافی را به دست می‌آورند و می‌توانند تصمیمات آگاهانه‌ای در خصوص صدور مجوز برای سیستم‌های اطلاعاتی اتخاذ کنند. از آنجا که ممکن است سیستم‌های اطلاعاتی، محیط‌های کاری و کارکنان فعال در حیطه توسعه سیستم تغییر کنند، مستندسازی و فراهم آوردن اطلاعات مربوط به فروض، محدودیت‌ها و دلایل تصمیمات باعث می‌شود که وضعیت آینده امنیت سیستم‌های اطلاعاتی و محیط کاری آن‌ها را بهتر بتوان درک کرد و در صورتی که تصمیمات مربوط به مخاطرات بازبینی شده باشند، به سادگی تغییرات را شناسایی نمود.

تعیین و تخصیص کنترل‌های معمول

کنترل‌های معمول، آن دسته از کنترل‌های امنیتی هستند که ممکن است به یک یا چند سیستم اطلاعاتی دیگر منتقل شود. اگر یک کنترل معمول به یک سیستم اطلاعاتی منتقل شود، نیازی نیست که سیستم مذکور کنترل را به وضوح پیاده‌سازی کند (یعنی این که قابلیت امنیتی توسط یک موجودیت دیگر تأمین می‌شود). بنابراین

---

[۱۰۱] برای کسب اطلاعات بیشتر، به بخش **۳٫۳ با نام** «تولید پوشش‌ها» و همچنین به پیوست خ یعنی «**قالب**‌های تولید پوشش‌ها» مراجعه کنید.

[۱۰۲] تصمیمات مربوط به تغییرات و اصلاحات می‌توانند مبتنی بر زمان‌بندی و امکان‌پذیری کنترل‌های امنیتی منتخب در شرایط خاص باشند. به **عبار**ت دیگر، ممکن است کنترل‌های امنیتی در تمام شرایط قابل اعمال نباشند، یا این که مقادیر تعیین‌شده برای پارامترها در عبارات اختصاص، در شرایط متفاوت تغییر کنند. پوشش‌ها می‌توانند برای تعیین این شرایط و ملاحظات زمان‌بندی مورد استفاده قرار گیرند.

[۱۰۳] میزان جزئیات مورد نیاز برای مستندسازی این تصمیمات در فرایند انتخاب کنترل‌های امنیتی، به صلاحدید سازمان‌ها تعیین می**شود و نشان**دهنده سطح تأثیر سیستم‌های اطلاعاتی اجراکننده این کنترل‌ها است.

هنگامی که کنترل‌های امنیتی مورد اشاره در پیوست ج از سیستم اطلاعاتی می‌خواهند که یک عملکرد امنیتی خاص را انجام دهد، این امر بدین معنی نیست که همه سیستم‌های اطلاعاتی که بخشی از سیستم‌های بزرگتر و پیچیده‌تر هستند، یا تمام مؤلفه‌های یک سیستم اطلاعاتی، باید عملکرد مذکور را انجام دهند. تصمیمات سازمانی تعیین‌کننده کنترل‌های معمول، می‌توانند تأثیر قابل‌توجهی بر مسئولیت‌های مالکان سیستم‌های اطلاعاتی در زمینه اجرای کنترل‌های موجود در یک مجموعه پایه خاص داشته باشند. انتخاب کنترل‌های معمول همچنین می‌تواند بر هزینه‌های سازمان نیز تأثیر بگذارد (هر چه تعداد کنترل‌های پیاده‌سازی‌شده بیشتر باشد، احتمالاً صرفه‌جویی‌های هزینه‌ای نیز بیشتر خواهد بود).

در نظر گرفتن ملاحظات مربوط به دامنه شمول

ملاحظات مربوط به دامنه شمول، در کنار راهنمایی‌های مربوط به مدیریت مخاطرات، سازمان‌ها را قادر می‌سازند تا تصمیمات آگاهانه‌تری در زمینه مخاطرات اتخاذ کنند[۱۰۴]. در نظر گرفتن ملاحظات مربوط به دامنه شمول می‌تواند باعث حذف کنترل‌های امنیتی غیر ضروری از مجموعه‌های پایه شود و سازمان‌ها را یاری کند تا تنها آن دسته از کنترل‌های امنیتی را انتخاب کنند که برای فراهم آوردن سطح حفاظت مناسب از سیستم‌های اطلاعاتی لازم هستند (یعنی حفاظت بر اساس مأموریت‌ها و فرایندهای کسب‌وکار پشتیبانی‌شده توسط سیستم‌های اطلاعاتی و محیط‌های کاری آن‌ها). سازمان‌ها می‌توانند با رعایت ملاحظات مربوط به دامنه شمول زیر، تصمیمات بهتری را در زمینه انتخاب و تعیین ویژگی‌های کنترل‌های امنیتی اتخاذ کنند. این تصمیمات می‌توانند بر نحوه پیاده‌سازی کنترل‌های امنیتی اولیه نیز تأثیر بگذارند.

- ملاحظات مربوط به تخصیص و استقرار کنترل‌های امنیتی

عبارت سیستم اطلاعاتی می‌تواند به دسته گسترده‌ای از سیستم‌ها اشاره داشته باشد، از «سیستم سیستم‌ها» گرفته تا سیستم‌های تک‌کاربری. پیچیدگی فزاینده بسیاری از سیستم‌های اطلاعاتی سبب می‌شود که نیاز به انجام تحلیل‌های دقیق در زمینه تخصیص و استقرار کنترل‌های امنیتی وجود داشته باشد. این تحلیل‌ها باید در هر سه مرحله سلسله مراتب مدیریت مخاطرات (یعنی سطح سازمانی، سطح مأموریت و فرایندهای کسب‌وکار، و سطح سیستم‌های اطلاعاتی) انجام شوند، بدون این که هیچ معماری یا روش خاصی تحمیل شود[۱۰۵]. کنترل‌های امنیتی موجود در مجموعه‌های پایه، ممکن است در

---

[۱۰۴] ملاحظات مورد اشاره در این بخش، تنها به عنوان مثال ارائه شده‌اند و هدف این نیست که سازمان‌ها نتوانند تصمیمات خود را بر اساس سایر ملاحظات و با داشتن یک منطق مناسب اتخاذ کنند.

[۱۰۵] این امر به ویژه در مورد معماری‌های خدمت‌محور صدق می‌کند که در آن‌ها از سرویس‌های خاصی برای انجام یک عملکرد خاص استفاده می‌شود.

در تمامی مؤلفه‌های سیستم قابل پیاده‌سازی نباشند. کنترل‌های امنیتی تنها در آن دسته از مؤلفه‌های سیستم‌های اطلاعاتی قابل پیاده‌سازی هستند که قابلیت امنیتی ارائه‌شده توسط آن‌ها را پشتیبانی کنند[۱۰۶]. سازمان‌ها باید تصمیم بگیرند که کنترل‌های امنیتی خاص را در کدام بخش‌های سیستم‌های اطلاعاتی به کار گیرند تا قابلیت امنیتی مورد نیاز حاصل شود و الزامات امنیتی رعایت شوند[۱۰۷]. مثالی از این نوع تخصیص، اعمال الزامات مورد اشاره در AC-18(1) (یعنی محافظت از دسترسی بی‌سیم به سیستم‌های اطلاعاتی با استفاده از روش‌های احراز هویت و رمزگذاری) در مورد تمام دسترسی‌های بی‌سیم، به جز دسترسی بی‌سیم به شبکه‌های فرعی است که به سایر مؤلفه‌های سیستم متصل نیستند.

- ملاحظات محیطی و عملیاتی

برخی از کنترل‌های امنیتی موجود در مجموعه‌های پایه، مبتنی بر فرض وجود برخی عوامل محیطی و عملیاتی خاص هستند. در صورتی که این عوامل وجود نداشته باشند یا تفاوت زیادی با فرضیات داشته باشند، می‌توان مجموعه‌های پایه را تغییر داد و اصلاح نمود. برخی از عوامل محیطی و عملیاتی مرسوم عبارتند از:

- قابلیت حمل

قابلیت حمل محیط‌های میزبانی فیزیکی، می‌تواند کنترل‌های امنیتی انتخاب‌شده برای سیستم‌های اطلاعاتی سازمان را تحت تأثیر قرار دهد. چنان که پیشتر هم گفته شد، در تخصیص کنترل‌های امنیتی به مجموعه‌های پایه مورد اشاره در پیوست ت، چنان فرض شده است که سیستم‌های اطلاعاتی در تأسیسات و مکان‌های ثابت کار می‌کنند. اگر سیستم‌های اطلاعاتی در محیط‌های متحرک کار کنند، مجموعه‌های پایه کنترل‌های امنیتی نیز باید به گونه‌ای تغییر داده و اصلاح شوند که مسئله تغییر مکان فیزیکی سیستم‌ها در آن‌ها در نظر گرفته شود. به عنوان مثال، بسیاری از کنترل‌های امنیتی خانواده حفاظت فیزیکی و محیطی (PE) که در هر سه مجموعه پایه انتخاب شده‌اند، مبتنی بر این فرض هستند که سیستم‌های اطلاعاتی در تأسیسات و مکان‌هایی قرار دارند

---

۱۰۶ به عنوان مثال، کنترل‌های ممیزی به طور معمول در آن دسته از مؤلفه‌ها قابل پیاده‌سازی هستند که قابلیت ممیزی را ارائه می‌کنند (مانند سرورها و مواردی از این دست). این کنترل‌ها، الزاماً در تمامی ایستگاه‌های کاربری درون سازمان قابل پیاده‌سازی نیستند. سازمان‌ها باید به دقت مؤلفه‌های تشکیل‌دهنده سیستم‌های اطلاعاتی خود را بررسی کنند و تعیین نمایند که کدام کنترل‌های امنیتی در کدام مؤلفه‌ها قابل پیاده‌سازی هستند.

۱۰۷ با پیشرفت فناوری اطلاعات، اکنون می‌توان عملکردهای مختلف و پیچیده‌ای را در گوشی‌های هوشمند، تبلت‌ها، و سایر دستگاه‌های همراه مشاهده کرد. هر چند که ممکن است در راهنمایی‌های اصلاحی گفته شده باشد که نباید یک کنترل امنیتی خاص را به یک دستگاه یا فناوری خاص تخصیص داد، اما مخاطرات حاصله را باید در بررسی مخاطرات مورد بررسی قرار داد تا بهترین شکل حمایت از سرمایه‌ها و عملیات سازمانی، **افراد**، سایر سازمان‌ها و مردم به عمل آید.

که باید حفاظت فیزیکی مناسب از آن‌ها به عمل آید. این کنترل‌ها احتمالاً دارای ویژگی‌های خاصی برای محیط‌های متحرکی مانند کشتی، هواپیما، اتومبیل، یا سیستم‌های فضایی نیستند[۱۰۸].

- عملیات و سیستم‌های تک‌کاربری

در مورد آن دسته از سیستم‌های اطلاعاتی که به عنوان سیستم‌های تک‌کاربری طراحی شده‌اند (مانند گوشی‌های هوشمند)، ممکن است نیازی به برخی کنترل‌های امنیتی مربوط به اشتراک‌گذاری داده‌ها نباشد. یک دستگاه یا سیستم تک‌کاربری، دستگاه یا سیستمی است که تنها برای استفاده یک شخص در نظر گرفته شده است (یعنی یک کاربر انحصاری دارد). دستگاه‌ها یا سیستم‌هایی که بین چند کاربر به اشتراک گذاشته می‌شوند، جزء دستگاه‌ها و سیستم‌های تک‌کاربری به شمار نمی‌آیند. در عملیات و سیستم‌های تک‌کاربری، احتمالاً نیازی به کنترل‌های امنیتی مانند AC-10 یا کنترل نشست همزمان، SC-4 یا اطلاعات در منابع اشتراک‌گذاری‌شده، و AC-3 یا ارتقای دسترسی[۱۰۹] نخواهد بود. در این موارد، سازمان می‌تواند کنترل‌های مذکور را به صلاحدید خود حذف نماید.

- اتصال و پهنای باند

هر چند که بسیاری از سیستم‌های اطلاعاتی به یکدیگر پیوسته‌اند، اما برخی سیستم‌ها نیز وجود دارند که به دلایل عملیاتی یا امنیتی، قابلیت شبکه‌شدن ندارند. در واقع، این سیستم‌ها از شبکه‌های غیرامن جدا شده‌اند. در مورد سیستم‌های شبکه‌نشده، نمی‌تون از برخی کنترل‌های امنیتی مانند AC-17 یا دسترسی راه دور، SC-8 یا یکپارچگی و محرمانگی انتقال، و SC-7 یا حفاظت مرزی استفاده کرد. در این موارد، سازمان می‌تواند کنترل‌های مذکور را به صلاحدید خود حذف نماید. علاوه بر سیستم‌های شبکه‌نشده، سیستم‌هایی نیز وجود دارند که پهنای باند آن‌ها نامنظم یا بسیار محدود است (مانند سیستم‌هایی که از عملیات نظامی یا مأموریت‌های اجرای قانون پشتیبانی می‌کنند). در مورد این سیستم‌ها، باید در هنگام پیاده‌سازی کنترل‌های امنیتی بسیار هوشیار بود، زیرا پهنای باند نامنظم یا بسیار محدود آن‌ها می‌تواند بر پیاده‌سازی کنترل‌ها یا حملات سایبری دشمنان تأثیر داشته باشد.

- سیستم‌ها یا مؤلفه‌های با عملکرد محدود

---

[۱۰۸] **مستگاه** های قابل حمل ممکن است برای مدتی در یک تأسیسات یا مکان ثابت مستقر باشند. در این مدت زمان، می‌توان از کنترل‌های PE **در مورد آن**ها استفاده کرد.

[۱۰۹] **سازمان**ها پیش از حذف کنترل AC-3 از مجموعه پایه، بررسی می‌کنند که آیا افراد کاربر به امتیازات سطح راهبری دسترسی دارند یا خیر.

بر اساس قانون E-Government سال ۲۰۰۲، سیستم‌های اطلاعاتی حیطه گسترده‌ای از دستگاه‌ها را در بر می‌گیرند. دستگاه‌های فکس، پرینترها، اسکنرها، پیجرها، گوشی‌های هوشمند، تبلت‌ها، ریدرها و دوربین‌های دیجیتال، همگی از جمله سیستم‌های اطلاعاتی (یا مؤلفه‌های این سیستم‌ها) به شمار می‌آیند. این سیستم‌ها و مؤلفه‌ها ممکن است قابلیت‌های پردازشی کلی در نظر گرفته شده در مجموعه‌های پایه را دارا نباشند. بدین ترتیب، دامنه تهدیداتی که این کنترل‌ها می‌توانند کنترل نمایند محدود می‌شود، و ممکن است همه کنترل‌های امنیتی در مورد آن‌ها قابل پیاده‌سازی نباشند. بنابراین، کنترلی مانند SI-3 یا حفاظت در برابر کدهای مخرب (که در تمام مجموعه‌های پایه وجود دارد)، ممکن است برای سیستم‌ها و مؤلفه‌هایی که قابلیت اجرای کدها را ندارند (مانند پیجرهای متنی) کاربردی نباشد. اما از آنجا که معمولاً هیچ تمایز واضحی بین این انواع سیستم‌های اطلاعاتی و مؤلفه‌ها وجود ندارد (مثلاً گوشی‌های هوشمند ترکیبی از قابلیت‌های تلفن، دوربین و کامپیوتر را دارند) باید در هنگام پیاده‌سازی کنترل‌های امنیتی به مواردی از جمله کاربرد سیستم‌ها، قابلیت‌های سیستم‌ها، و مخاطرات موجود توجه نمود.

- دائمی نبودن سیستم‌ها و اطلاعات

معمولاً چنین فرض می‌شود که اطلاعات کاربری برای مدت زمان بسیار طولانی در سیستم‌های اطلاعاتی سازمان باقی می‌مانند. اما در مورد برخی از برنامه‌های کاربردی و محیط‌های کاری (مانند سیستم‌های نظامی و سیستم‌های کنترل صنعتی)، این اطلاعات معمولاً برای مدت زمان اندکی نگهداری می‌شوند. در مورد آن دسته از سیستم‌های اطلاعاتی که این اطلاعات غیر دائمی را پردازش، ذخیره یا منتقل می‌کنند، ممکن است برخی کنترل‌های امنیتی خانواده برنامه‌ریزی اضطراری (CP) مانند CP-6 یا مکان ذخیره‌سازی جایگزین، CP-7 یا مکان پردازش جایگزین، و CP-9 یا نسخه پشتیبان سیستم اطلاعاتی قابل استفاده نباشند. در این موارد، سازمان می‌تواند کنترل‌های مذکور را به صلاحدید خود حذف نماید. به دلایل مشابه، کنترل‌هایی مانند MP-6 یا پاکسازی رسانه‌ها[۱۱۰] و SC-28 یا حفاظت از اطلاعاتی که در حال استفاده شدن نیستند، گزینه‌های مناسبی برای حذف از مجموعه‌های پایه به شمار می‌آیند[۱۱۱]. علاوه بر اطلاعات، خدمات و سیستم‌های اطلاعاتی نیز می‌توانند غیر دائمی باشند. با استفاده از روش‌های مجازی‌سازی می‌توان

[110] Media Sanitization

[۱۱۱] **سازمان**‌ها، تعادلی بین میزان ماندگار بودن اطلاعات و حساسیت آن‌ها برقرار می‌کنند. اطلاعات غیر دائمی ممکن است پس از حذف شدن نیازمند پاکسازی نیز باشند. علاوه بر این، سازمان‌ها طول مدت حساس بودن اطلاعات را نیز در نظر می‌گیرند. ممکن است برخی اطلاعات دائمی، فقط برای مدت زمان محدودی حساس باشند.

نسخه‌های غیر دائمی از برنامه‌های کاربردی و سیستم‌های عملیاتی را نصب کرد. بسته به طول مدت نصب این برنامه‌های کاربردی و سیستم‌ها، برخی کنترل‌های اولیه ممکن است کاربردی نباشند.

- دسترسی عمومی

هنگامی که دسترسی عمومی به سیستم‌های اطلاعات سازمان مجاز باشد، کنترل‌های امنیتی را باید با احتیاط مورد استفاده قرار داد، زیرا برخی از آن‌ها که از مجموعه‌های پایه خاص گرفته شده‌اند (مانند کنترل‌های امنیتی شخصی، شناسایی و احراز هویت)، ممکن است برای دسترسی عمومی قابل استفاده نباشند. بنابراین در مورد وبسایت‌های دولتی که امکان دسترسی عمومی به آن‌ها وجود دارد (مثلاً امکان دانلود کردن فرم‌ها و اطلاعات آماده‌سازی اضطراری در آن‌ها فراهم آمده است)، کنترل‌های امنیتی مانند AC-7 یا تلاش‌های ورود ناموفق، AC-17 یا دسترسی راه دور، IA-2 یا شناسایی و احراز هویت، IA-4 یا مدیریت شناسه‌ها، و IA-5 یا مدیریت احراز هویت، چندان برای احراز هویت یا تأیید امتیازات ویژه راهگشا نخواهند بود. اما این کنترل‌ها را باید برای شناسایی و احراز هویت کارکنان سازمان به کار گرفت، تا این کارکنان بتوانند وظیفه خود در نگهداری و پشتیبانی از سیستم‌های اطلاعاتی این وبسایت‌ها را انجام دهند. به طور مشابه، ممکن است بسیاری از این کنترل‌های امنیتی برای کاربرانی که از طریق سیستم‌های اطلاعاتی غیر عمومی به واسطه‌های عمومی دسترسی پیدا می‌کنند، لازم باشند.

- ملاحظات مربوط به اهداف امنیتی

وظایف آن دسته از کنترل‌های امنیتی که تنها از یک یا دو مورد از اهداف امنیتی محرمانگی، یکپارچگی، یا در دسترس بودن پشتیبانی می‌کنند را می‌توان در صورت وجود شرایطی که در ادامه می‌آیند، به کنترل‌های یک مجموعه پایه پایین‌تر منتقل کرد (یا در صورتی که در مجموعه پایه پایین‌تر تعریف نشده باشند، می‌توان آن‌ها را تغییر داد یا حذف کرد): (۱) فرایند انتقال به مجموعه پایین‌تر باید بر اساس دسته‌بندی امنیتی FIPS 199 پیش از ارتقا به سطح تأثیر FIPS 200 (یعنی واترمارک قوی) باشد[۱۱۲]؛ (۲) این فرایند باید مبتنی بر بررسی مخاطرات سازمانی باشد؛ و (۳) این فرایند نباید تأثیر

[۱۱۲] در هنگام اعمال واترمارک قوی در بخش **۳/۱**، ممکن است برخی از اهداف امنیتی اصلی محرمانگی، یکپارچگی، یا در دسترس بودن FIPS 199، به یک مجموعه پایه بالاتر کنترل‌های امنیتی ارتقا یافته باشند. در این فرایند ممکن است برخی کنترل‌های امنیتی انحصاری محرمانگی، یکپارچگی و در دسترس بودن، به طور غیر ضروری به سطح بالاتر ارتقا پیدا کرده باشند. در نتیجه، توصیه می‌شود که سازمان‌ها امکان انتقال به سطح پایین‌تر را فراهم آورند تا در نهایت برای پیاده‌سازی کنترل‌های امنیتی از یک فرایند مقرون‌به‌**صرفه** و مبتنی بر مخاطره استفاده شود.

منفی بر سطح حفاظت اطلاعات امنیتی در سیستم‌های اطلاعاتی سازمانی داشته باشد[۱۱۳]. به عنوان مثال، اگر محرمانگی و/یا یکپارچگی یک سیستم اطلاعاتی در سطح متوسط اما در دسترس بودن آن در سطح کم باشد و در نتیجه سیستم مذکور به عنوان سیستمی با سطح تأثیر کم دسته‌بندی شود، برخی کنترل‌ها وجود دارند که تنها از هدف امنیتی در دسترس بودن پشتیبانی می‌کنند و می‌توان آن‌ها را به مجموعه‌های پایه سطح پایین منتقل کرد. به عبارت دیگر، ممکن است بهتر باشد که از کنترل CP-2(1) استفاده نشود، زیرا این کنترل پیشرفته تنها از در دسترس بودن پشتیبانی می‌کند و در مجموعه پایه سطح متوسط انتخاب شده اما در مجموعه پایه سطح پایین انتخاب نشده است. کنترل‌های امنیتی و کنترل‌های پیشرفته زیر را احتمالاً می‌توان به سطح پایین منتقل کرد[۱۱۴]:

- محرمانگی: AC-21, MA-3(3), MP-3, MP-4, MP-5, MP-5(4), MP-6(1), MP-6(2), PE-4, PE-5, SC-4, SC-8, SC-8(1)
- یکپارچگی: CM-5, CM-5(1), CM-5(3), SC-8, SC-8(1), SI-7, SI-7(1), SI-7(5), SI-10
- در دسترس بودن: CP-2(1), CP-2(2), CP-2(3), CP-2(4), CP-2(5), CP-2(8), CP-3(1), CP-4(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(4), CP-9(1), CP-9(2), CP-9(3), CP-9(5), CP-10(2), CP-10(4), MA-6, PE-9, PE-10, PE-11, PE-11(1), PE-13(1), PE-13(2), PE-13(3), PE-15(1)

- ملاحظات مربوط به فناوری

آن دسته از کنترل‌های امنیتی که به فناوری‌های خاص (مانند فناوری‌های بی‌سیم، رمزنگاری، زیرساخت‌های کلید عمومی) اشاره دارند، تنها در صورتی عملی هستند که فناوری‌های مذکور در سیستم‌های اطلاعاتی سازمان به کار گرفته شده باشند یا چنین الزامی در سیستم‌های اطلاعاتی وجود داشته باشد. برخی کنترل‌های امنیتی را می‌توان به طور آشکار یا به طور ضمنی با استفاده از مکانیسم‌های خودکار پشتیبانی کرد. در صورتی که این مکانیسم‌ها در محصولات تجاری یا دولتی وجود نداشته باشند، نیازی به توسعه آن‌ها نخواهد بود. در صورتی وجود نداشتن این مکانیسم‌ها، برای

---

[۱۱۳] اطلاعات امنیتی سطح سیستم اطلاعاتی (مانند فایل‌های گذرواژه، جداول مسیریاب‌های شبکه، اطلاعات مدیریت کلیدهای رمزنگاری) با اطلاعات سطح کاربر در همان سیستم اطلاعاتی تفاوت دارند. برخی از کنترل‌های امنیتی برای پشتیبانی از اهداف امنیتی محرمانگی و یکپارچگی در هر دو سطح در نظر گرفته شده‌اند. در هنگام انتقال این کنترل‌ها به سطح پایین‌تر باید دقت لازم را به عمل آورد و اطمینان حاصل نمود که این کار موجب حفاظت نامناسب اطلاعات امنیتی در سیستم اطلاعاتی نمی‌شود. اطلاعات امنیتی باید در واترمارک قوی حفاظت شوند، تا از تمام اهداف امنیتی مربوط به اطلاعات سطح کاربر، حفاظت یکسانی به عمل آید.

[۱۱۴] انتقال دادن به سطح پایین‌تر، در مورد مجموعه‌های پایه سطح متوسط و زیاد قابل انجام نیست. آن دسته از کنترل‌های امنیتی که منحصر به اهداف امنیتی محرمانگی، یکپارچگی یا در دسترس بودن هستند (مانند AC-16, AU-10, IA-7, PE-12, PE-14, SC-5, SC-13, SC-16) و در حالت عادی به سطح پایین‌تر منتقل می‌گردند، از ملاحظات گنار گذاشته می‌شوند، زیرا یا برای استفاده در تمام مجموعه‌های پایه در نظر گرفته شده‌اند و هیچ کنترل پیشرفته قابل انتقالی ندارند، یا اختیاری هستند و برای استفاده در هیچ مجموعه پایه‌ای انتخاب نشده‌اند. سازمان‌ها باید در هنگام انتقال کنترل‌هایی که در لیست بخش ۳/۲ لیست نشده‌اند، بسیار محتاط باشند و اطمینان حاصل نمایند که انتقال آن‌ها به سطح پایین‌تر، سبب به خطر افتادن اهداف امنیتی نمی‌شود.

دستیابی به ویژگی‌های مطلوب کنترل‌های امنیتی یا کنترل‌های پیشرفته، از کنترل‌های امنیتی جبرانی مقرون به صرفه و عملی استفاده می‌شود که با استفاده از روش‌ها و مکانیسم‌های غیر خودکار پیاده‌سازی می‌شوند (در اداه می‌توانید شرایط و ضوابط پیاده‌سازی کنترل‌های جبرانی را مطالعه کنید).

- ملاحظات مربوط به الزامات مأموریتی

در صورتی که پیاده‌سازی برخی کنترل‌های امنیتی منجر به ایجاد اخلال و وقفه در مأموریت‌ها و فرایندهای کسب‌وکار سازمان شود، استفاده از آن‌ها عملی (یا مناسب) نخواهد بود. به عنوان مثال، اگر برای انجام مأموریت سازمان نیاز به این باشد که در کنسول اپراتور (مانند کنسول کنترل ترافیک هوایی) اطلاعات حساسی به طور پیوسته نمایش داده شوند، احتمالاً پیاده‌سازی کنترل‌های AC-11 یا قفل کردن نشست و SC-10 یا قطع کردن شبکه کار درستی نخواهد بود.

انتخاب کنترل‌های امنیتی جبرانی

ممکن است سازمان‌ها گاهی اوقات به این نتیجه برسند که باید از کنترل‌های امنیتی جبرانی استفاده نمایند. کنترل‌های جبرانی، گاهی به جای برخی کنترل‌های امنیتی در مجموعه‌های پایه با سطح تأثیر کم، متوسط و زیاد به کار گرفته می‌شوند. این کنترل‌های جبرانی، سیستم‌های اطلاعاتی سازمان و اطلاعات پردازش‌شده، ذخیره‌شده یا منتقل‌شده توسط این سیستم‌ها را تقریباً معادل کنترل‌های امنیتی اصلی حفاظت می‌نمایند[۱۱۵]. این امر مثلاً هنگامی رخ می‌دهد که سازمان‌ها نمی‌توانند کنترل‌های امنیتی موجود در مجموعه‌های پایه را به درستی پیاده‌سازی کنند، یا هنگامی که به دلیل ماهیت خااص سیستم‌های اطلاعاتی یا محیط کاری آن‌ها، کنترل‌های امنیتی مذکور مقرون به صرفه نیستند. کنترل‌های جبرانی معمولاً بعد از در نظر گرفتن راهنمایی‌های اختصاصی انتخاب می‌شوند. این کنترل‌ها با شرایط زیر توسط سازمان‌ها مورد استفاده قرار می‌گیرند:

- سازمان‌ها کنترل‌های جبرانی را از پیوست ج انتخاب می‌کنند؛ اگر کنترل‌های جبرانی مناسبی وجود نداشته باشند، سازمان‌ها کنترل‌های جبرانی مناسب را از منابع دیگر به کار می‌گیرند[۱۱۶]؛

---

[۱۱۵] برای فراهم آوردن سطح حفاظتی معادل آن چه در پیوست ج در مورد برخی کنترل‌های امنیتی گفته شده است، ممکن است نیاز باشد که از بیش از یک کنترل جبرانی استفاده شود. به عنوان مثال، برخی سازمان‌ها با کمبود شدید نیروی انسانی مواجه هستند. این سازمان‌ها می‌توانند برای جبران کنترل امنیتی تفکیک وظایف، از کنترل‌های امنیتی ممیزی، پاسخگویی و پرسنل استفاده کنند.

[۱۱۶] **سازمان**‌ها باید تمام تلاش خود را به کار گیرند تا کنترل‌های جبرانی را از کاتالوگ کنترل‌های امنیتی ارائه‌شده در پیوست ج انتخاب نمایند. **کنترل**‌های جبرانی دیگر تنها در صورتی به کار گرفته می‌شوند که سازمان به این نتیجه برسد که کاتالوگ کنترل‌های امنیتی شامل هیچ کنترل جبرانی مناسبی نیست.

- سازمان‌ها تشریح می‌کنند که چرا کنترل‌های جبرانی انتخاب‌شده می‌توانند سطح حفاظتی معادل کنترل‌های امنیتی اولیه ارائه کنند، و این که چرا نمی‌توان از کنترل‌های امنیتی اولیه استفاده کرد؛ و
- سازمان‌ها مخاطرات مربوط به پیاده‌سازی کنترل‌های جبرانی در سیستم‌های اطلاعاتی سازمان را بررسی می‌کنند و این مخاطرات را می‌پذیرند.

تخصیص مقادیر به پارامترهای کنترل‌های امنیتی

آن دسته از کنترل‌های امنیتی و کنترل‌های جبرانی که دارای پارامترهایی هستند (یعنی دارای عبارات انتخاب و اختصاص هستند)، به سازمان‌ها این انعطاف را می‌دهند که برخی از الزامات سازمانی را با استفاده از بخش خاصی از کنترل‌های امنیتی و کنترل‌های پیشرفته برآورده کنند. پس از در نظر گرفتن ملاحظات اولیه و انتخاب کنترل‌های جبرانی، سازمان‌ها به بررسی کنترل‌های امنیتی و کنترل‌های پیشرفته می‌پردازند تا عبارات انتخاب و اختصاص آن‌ها را تعیین کنند. در این فرایند، سازمان‌ها مقادیری را برای پارامترهای مورد اشاره در این عبارات تعیین می‌کنند. مقادیر این پارامترها ممکن است در خط‌مشی‌ها، دستورات اجرایی، مقررات، استانداردها، رهنمودها و قوانین فدرال تعیین شده باشند. پس از این که سازمان‌ها مقادیر پارامترهای کنترل‌های امنیتی و کنترل‌های پیشرفته را تعیین کردند، عبارات انتخاب و اختصاص تبدیل به بخشی از کنترل‌های امنیتی و کنترل‌های پیشرفته می‌شوند[۱۱۷]. ممکن است سازمان‌ها تصمیم بگیرند که این مقادیر را پیش از انتخاب کنترل‌های جبرانی تعیین کنند، زیرا تعیین مقادیر پارامترها در واقع بخشی از فرایند تعریف کنترل‌ها است و ممکن است در ادامه بر روند انتخاب کنترل‌های جبرانی تأثیر داشته باشد. همکاری در تعیین مقادیر پارامترها می‌تواند مزایای زیادی برای سازمان‌ها داشته باشد. سازمان‌هایی که به طور منظم با یکدیگر همکاری می‌کنند، می‌توانند مجموعه‌ای از مقادیر را با همفکری و مشوری هم تعیین کنند. بدین ترتیب، سازمان‌ها می‌توانند در هنگام استفاده از سیستم‌های اطلاعاتی یا خدمات یکدیگر، همکاری بهتر و کارایی بالاتری داشته باشند.

تکمیل مجموعه‌های پایه کنترل‌های امنیتی

تعیین نهایی مجموعه مناسبی از کنترل‌های امنیتی برای تأمین امنیت سیستم‌های اطلاعاتی و محیط کاری آن‌ها، منوط به بررسی مخاطرات و اقدامات لازم برای کاهش مخاطرات مربوط به سرمایه‌ها و عملیات سازمانی، افراد، سایر سازمان‌ها و مردم است[۱۱۸]. در بسیاری از موارد، مقابله با تهدیدات و پوشش دادن آسیب‌پذیریهای

---

[۱۱۷] **دستورالعمل** CNSS 1253، حداقل مقادیر مربوط به متغیرها را برای سیستم‌های امنیتی ملی تعیین می‌کند. مقادیر پارامترها همچنین ممکن **است در پوشش‌های** تشریح‌**شده در بخش ۳٫۴** تعیین شده باشد.

[۱۱۸] ملاحظات مربوط به تأثیر دسته‌بندی سیستم‌های اطلاعاتی سازمان روی مردم و سایر سازمان‌ها، در قانون USA PATRIOT و رهنمودهای ریاست‌جمهوری در زمینه امنیت داخلی آمده است.

موجود در سازمان‌ها، مأموریت‌ها و فرایندهای کسب‌وکار، و سیستم‌های اطلاعاتی، و همچنین رعایت الزامات مورد اشاره در خط‌مشی‌ها، دستورات اجرایی، مقررات، استانداردها، رهنمودها و قوانین فدرال، نیازمند استفاده از تعدادی دیگر از کنترل‌های امنیتی و کنترل‌های پیشرفته است (علاوه بر آن چه در قالب مجموعه‌های پایه در پیوست ت تعیین شده است)[۱۱۹]. بررسی مخاطرات در فرایند انتخاب کنترل‌های امنیتی، اطلاعات مهمی را در اختیار سازمان‌ها قرار می‌دهد تا بر آن اساس، کنترل‌های امنیتی و کنترل‌های پیشرفته لازم و کافی را تعیین نمایند. به سازمان‌ها توصیه می‌شود که بیشترین استفاده را از پیوست ج داشته باشند و بر اساس موارد مطرح‌شده در آن، مجموعه‌های پایه را با استفاده از کنترل‌های امنیتی و کنترل‌های پیشرفته مناسب تکمیل نمایند[۱۲۰].

شرایطی که در آن‌ها احتمالاً نیاز به تکمیل مجموعه‌های پایه وجود دارد

سازمان‌ها ممکن است به دلایل محیطی یا عملیاتی، یا به دلیل تهدیدات موجود، در شرایطی قرار گیرند که برای محافظت شایسته از مأموریت‌ها و فرایندهای کسب‌وکار و سیستم‌های اطلاعاتی پشتیبان آن‌ها، نیاز به استفاده از کنترل‌های اضافه‌ای داشته باشند. در ادامه برخی از این شرایط تشریح شده‌اند.

- تهدید مستمر پیشرفته

مجموعه‌های پایه کنترل‌های امنیتی مبتنی بر این فرض نیستند که دشمنان به اهداف خود رسیده‌اند و تهدیدات بیشتری را بر علیه سازمان و سیستم‌های اطلاعاتی آن ایجاد نمی‌کنند. به عبارت دیگر، سازمان‌ها با شرایط تهدید مستمر پیشرفته (APT) مواجه هستند. دشمنان باز هم به سیستم‌های اطلاعاتی و زیرساخت‌های IT سازمان حمله خواهند کرد و برخی از حملات خود را نیز با موفقیت انجام می‌دهند. برای پاسخ دادن بهتر به شرایط تهدید مستمر پیشرفته، سازمان‌ها می‌توانند مفاهیمی همچون حفاظت در برابر تهدیدات داخلی ((CM-5(4))، عدم تجانس (SC-29)، فریب (SC-26 و SC-30)، عدم استمرار (SC-25 و SC-34)، بخش‌بندی ((SC-7(13)) را در نظر بگیرند.

- خدمات بین‌دامنه‌ای

مجموعه‌های پایه کنترل‌های امنیتی مبتنی بر این فرض نیستند که سیستم‌های اطلاعاتی باید در چند دامنه امنیتی مختلف فعالیت کنند. مجموعه‌های پایه کنترل‌های امنیتی، دیدگاه تخت و غیرمنعطفی

---

[۱۱۹] در نسخه‌های قبلی شماره ویژه NIST 800-53، منظور از تغییر و اصلاح راهنمایی‌ها تنها حذف کنترل‌های امنیتی از مجموعه‌های پایه و منظور از تکمیل تنها اضافه کردن کنترل‌ها به مجموعه‌های پایه بود. اما در این سند، منظور از تغییر و اصلاح هم حذف و هم اضافه کردن کنترل‌های امنیتی است.

[۱۲۰] کنترل‌های امنیتی و کنترل‌های پیشرفته انتخاب‌شده برای تکمیل مجموعه‌های پایه، به همان شکلی برای مؤلفه‌های سیستم‌های اطلاعاتی انتخاب می‌شوند که کنترل‌های اولیه برای مجموعه‌های پایه برگزیده می‌شوند.

درباره جریان اطلاعات دارند (یعنی این که در هنگام عبور اطلاعات از مرز حوزه‌ها، خط‌مشی‌های امنیتی واحد در چند دامنه مختلف مصداق پیدا می‌کنند). برای پرداختن به تراکنش‌ها و خدمات بین‌دامنه‌ای، می‌توان زیرمجموعه‌ای از کنترل‌های پیشرفته AC-4 را مورد استفاده قرار داد تا از امنیت اطلاعات منتقل‌شده بین سیستم‌های اطلاعاتی دارای خط‌مشی‌های امنیتی مختلف اطمینان حاصل شود.

- قابلیت جابجایی

برای استفاده از دستگاه‌های همراه، ممکن است نیاز به کنترل‌های امنیتی و کنترل‌های پیشرفته اضافه‌ای باشد که در مجموعه‌های پایه وجود ندارند. به عنوان مثال، کنترل امنیتی AC-7(2) که به موجب آن اطلاعات پس از تعداد مشخصی تلاش ورود ناموفق پاک می‌شوند، یا کنترل امنیتی MP-6(8) که به موجب آن می‌توان اطلاعات را از راه دور پاک کرد، می‌توانند برای مقابله با تهدید سرقت یا از دست رفتن دستگاه‌های همراه به کار گرفته شوند.

- اطلاعات محرمانه

در برخی محیط‌ها، ممکن است اطلاعات محرمانه و حساسی[۱۲۱] در سیستم‌های امنیت ملی وجود داشته باشند که همه کاربران اجازه دسترسی به آن‌ها را نداشته باشند. در این شرایط به کنترل‌های امنیتی دیگری هم نیاز است تا اطمینان حاصل شود که اطلاعات مذکور در دسترس افراد غیرمجاز قرار نمی‌گیرند. به عنوان مثال، می‌توان از کنترل‌های امنیتی دقیق AC-3(3) یا AC-16 بدین منظور استفاده کرد. در صورتی که اطلاعات محرمانه توسط سیستم‌هایی پردازش و ذخیره و منتقل شوند که مالکیت مشترک آن‌ها در اختیار چند موجودیت مختلف است (مانند طرفین ائتلاف‌های نظامی)، باید از کنترل‌های امنیتی دقیق‌تری استفاده کرد که از آن جمله می‌توان به MA-5(4) اشاره نمود.

فرایند شناسایی سایر کنترل‌های امنیتی مورد نیاز

سازمان‌ها می‌توانند برای انتخاب کنترل‌های امنیتی و کنترل‌های پیشرفته مورد نیاز برای تکمیل مجموعه‌های پایه، از رویکرد «تعریف الزامات» یا رویکرد «تحلیل کمبودها» استفاده کنند. در رویکرد تعریف الزامات، سازمان‌ها اطلاعات خاص و معتبری را درباره تهدیدات و فعالیت‌های دشمنان دریافت می‌کنند (یا به فروضی منطقی در این زمینه می‌رسند) و بر آن اساس تعیین می‌نمایند که دشمنان چه توانایی‌ها و قابلیت‌هایی برای

[۱۲۱] **دستورالعمل** CNSS 1253 راهنمایی‌های ویژه‌ای را درباره کنترل‌های امنیتی مورد نیاز برای سیستم‌های امنیت ملی ارائه می‌کند.

حمله دارند (مثلاً چه تخصص‌ها، مهارت‌ها و منابعی برای انجام حملات در اختیار دارند)[۱۲۲]. برای این که سازمان‌ها بتوانند به خوبی با حملات سایبری دشمنان مقابله کنند، باید از سطح خاصی از قابلیت دفاعی و آمادگی سایبری برخوردار باشند. سازمان‌ها می‌توانند برای رسیدن به این قابلیت‌ها و آمادگی‌ها، کنترل‌های امنیتی و کنترل‌های پیشرفته دیگری را از پیوست ج انتخاب کنند. اما در روش تحلیل کمبودها، سازمان‌ها کار را با بررسی قابلیت دفاعی و آمادگی سایبری خود آغاز می‌کنند. پس از این بررسی اولیه، سازمان‌ها تعیین می‌نمایند که قابلیت مقابله با کدام نوع حملات را دارند. در صورتی که سطح فعلی قابلیت دفاعی و آمادگی سایبری سازمان کافی نباشد، باید تعیین کرد که به چه قابلیت‌ها و آمادگی‌های دیگری نیاز است. در ادامه سازمان‌ها کنترل‌های امنیتی و کنترل‌های پیشرفته مورد نیاز برای رسیدن به سطح مطلوب را از پیوست ج انتخاب می‌کنند. هر دو ویکرد، نیازمند اطلاعات دقیق و به‌هنگامی در مورد تهدیدات هستند. بنابراین، لازم است که سازمان‌ها این اطلاعات را کسب کنند تا بتوانند اقدامات مقتضی را انجام دهند.

در فرایند تغییر و اصلاح، سازمان‌ها اقدام به بازبینی کد اولویت‌بندی کنترل‌های امنیتی خود می‌کنند تا دریابند که آیا تغییر این اولیویت‌ها به صلاح سازمان هست یا خیر. این امر به ویژه زمانی حائز اهمیت است که سازمان‌ها بخواهند برخی کنترل‌های امنیتی را به مجموعه‌های پایه خود بیفزایند، زیرا این کنترل‌ها کد اولویت‌بندی P0 دارند. بازبینی کدهای اولویت‌بندی می‌تواند بر اساس بررسی مخاطرات سازمان یا تصمیمات طراحی و توسعه مربوط به معماری امنیتی سیستم‌های اطلاعاتی و فرایندهای مهندسی امنیت انجام شود که ممکن است نیازمند ترتیب خاصی در پیاده‌سازی کنترل‌های امنیتی باشند.

ارتقای امنیت اطلاعات بدون تغییر دادن کنترل‌های انتخاب‌شده

ممکن است شرایطی پیش آید که سازمان‌ها نتوانند کنترل‌های امنیتی کافی را در سیستم‌های اطلاعاتی خود به کار گیرند و به گونه مقتضی مخاطرات را کاهش دهند (مثلاً در هنگام استفاده از انواع خاصی از فناوری‌های اطلاعاتی یا پیاده‌سازی برخی روش‌های پردازشی خاص). در این شرایط، باید از راهبردهای دیگری برای جلوگیری از تضعیف و به خطر افتادن مأموریت‌ها و فرایندهای کسب‌وکار سازمانی استفاده کرد. در این راهبردها، سازمان‌ها بررسی می‌کنند که استفاده بیش از حد از فناوری‌های اطلاعاتی می‌تواند چه مخاطراتی برای مأموریت‌ها و فرایندهای کسب‌وکار سازمانی ایجاد کند. می‌توان در کنار کنترل‌های امنیتی تکمیلی، و یا به جای استفاده از آن‌ها، محدودیت‌هایی را در مورد استفاده از انواع خاصی از فناوری‌ها یا چگونگی به‌کارگیری

[۱۲۲] این مثال تنها در مورد حفاظت از سیستم‌های اطلاعاتی در برابر حملات هدفمند است، اما مطالب گفته‌شده در مورد اخلال‌های محیطی و خطاهای انسانی نیز صدق می‌کند.

سیستم‌های اطلاعاتی سازمانی در نظر گرفت. ممکن است وضع این محدویت‌ها، تنها راه سازمان‌ها برای انجام صحیح مأموریت‌ها و فرایندهای کسب‌وکار خود و مقابله با تهدیدات دشمنان باشد. به عنوان مثالی از این محدودیت‌ها، می‌توان به موارد زیر اشاره کرد:

- محدود کردن اطلاعاتی که سیستم‌های اطلاعاتی می‌توانند ذخیره، پردازش یا منتقل کنند، یا محدود کردن روش خودکارسازی مأموریت‌ها و فرایندهای کسب‌وکار سازمانی؛
- منع دسترسی خارجی به اطلاعات سازمانی، از طریق حذف برخی مؤلفه‌های سیستم‌های اطلاعاتی از شبکه؛ و
- ممنوع کردن قرار دادن اطلاعات با تأثیر متوسط یا زیاد در آن دسته از سیستم‌های اطلاعاتی سازمانی که دسترسی عمومی به آن‌ها وجود دارد، مگر این که بر اساس بررسی مخاطرات، این دسترسی مجاز باشد.

فراهم آوردن سایر اطلاعات مورد نیاز برای پیاده‌سازی کنترل‌ها

از آن جا که کنترل‌های امنیتی به طور مختصر به قابلیت‌های امنیتی اشاره می‌کنند، ممکن است اطلاعات کافی برای پیاده‌سازی مناسب در آن‌ها وجود نداشته باشد. بنابراین، ممکن است به اطلاعات بیشتری نیاز باشد تا بتوان به اهداف کنترل‌های امنیتی پی برد و اطمینان حاصا نمود که الزامات امنیتی مربوطه رعایت شده‌اند. به عنوان مثال، ممکن است اطلاعاتی در فرایند پیاده‌سازی کنترل‌ها و تعیین الزامات فراهم آیند. این اطلاعات ممکن است شامل اصلاح جزئیات پیاده‌سازی، اصلاح دامنه شمول، یا پیاده‌سازی متفاوت یک کنترل امنیتی در حوزه‌های مختلف باشد. در صورتی که اطلاعات موجود (مانند عبارت‌ها انتخاب و اختصاص) برای تعیین دقیق اهداف کنترل‌های امنیتی کافی نباشند، سازمان‌ها باید اطلاعات لازم را فراهم آورند. سازمان‌ها این آزادی عمل را دارند که تعیین کنند اطلاعات اضافی مورد نیاز در قالب عبارت‌های کنترل، راهنمایی‌های تکمیلی، یا در یک پیوست مجزا ارائه شوند. در هنگام ارائه این اطلاعات، سازمان‌ها باید توجه داشته باشند که هدف کنترل امنیتی یا زبان مورد استفاده در کنترل را تغییر ندهند. این اطلاعات اضافی می‌توانند در قالب طرح‌های امنیتی یا طرح‌های مهندسی امنیت یا مهندسی سیستم ثبت و مستندسازی شوند. نمونه‌ای از اطلاعات اضافی مورد نیاز برای تعیین دقیق چگونگی پیاده‌سازی کنترل‌های امنیتی، در ادامه و در قالب مثال SI-7(6) ارائه شده است:

SI-7: یکپارچگی اطلاعات، ثابت‌افزار و سخت‌افزار

(۶) یکپارچگی اطلاعات، ثابت‌افزار و سخت‌افزار / حفاظت رمزنگاری

سیستم اطلاعاتی، از مکانیسم‌های رمزنگاری برای شناسایی تغییرات غیرمجاز نرم‌افزار، سخت‌افزار و اطلاعات استفاده می‌کند.

راهنمایی‌های تکمیلی: به عنوان مثالی از مکانیسم‌های رمزنگاری مورد استفاده برای حفاظت از یکپارچگی، می‌توان به این موارد اشاره کرد: امضای دیجیتال و محاسبه و اعمال درهم‌سازی‌های امضا شده با استفاده از رمزنگاری نامتقارن، حفاظت از محرمانگی کلید مورد استفاده برای تولید درهم‌ساز، و استفاده از کلید عمومی برای تأیید اطلاعات درهم‌سازی. کنترل مربوطه: SC-13.

اطلاعات اضافی مورد نیاز برای پیاده‌سازی SI-7(6):

در مورد تمام ترافیکی که اصل عدم انکار در مورد آن‌ها صدق می‌کند، باید از امضاهای دیجیتال استفاده کرد. امضای دیجیتال از طریق الگوریتم SHA-256 یا هر الگوریتم NIST معتبری انجام شود که دست کم قدرتی برابر با قدرت مکانیسم SHA-256 داشته باشد.

۳-۳- تولید پوشش‌ها

در بخش‌های قبل بررسی کردیم که سازمان‌ها چگونه می‌توانند مجموعه‌های پایه کنترل‌های امنیتی را تغییر دهند و اصلاح کنند تا به قابلیت‌های امنیتی مورد نظر خود دست یابند. در برخی شرایط خاص، ممکن است برای سازمان‌ها بهتر باشد که فرایند اصلاح و تغییر را به گونه‌ای انجام دهند که مجموعه‌ای از کنترل‌های امنیتی برای تمامی سازمان‌ها فراهم شود، یا این که الزامات، فناوری‌ها، محیط‌ها یا مأموریت‌های خاصی را مد نظر قرار دهند[۱۲۳]. به عنوان مثال، ممکن است دولت فدرال تصمیم بگیرد که مجموعه‌ای از کنترل‌های امنیتی و راهنمایی‌های را برای پیاده‌سازی آن‌ها در سطح ملی در این زمینه‌ها تعیین کند: (۱) سیستم‌های مربوط به زیرساخت‌های عمومی اصلی (PKI)[۱۲۴]، به گونه‌ای که بتوان این راهنمایی‌ها را به طور یکنواخت برای تمام سیستم‌های PKI در ادارات فدرال به کار گرفت؛ (۲) سیستم‌های اطلاعاتی مبتنی بر کلاد، به گونه‌ای که بتوان این راهنمایی‌ها را به طور یکنواخت برای تمام ادارات فدرال استفاده‌کننده از خدمات کلاد مورد استفاده قرار داد؛ یا (۳) سیستم‌های کنترل صنعتی (ICS)[۱۲۵] در تأسیسات فدرال تولیدکننده برق یا کنترل‌کننده سیستم‌های محیطی در این تأسیسات. به عنوان مثالی دیگر، ممکن است وزارت دفاع بخواهد الزاماتی را برای برخی

[۱۲۳] این نوع تغییر و اصلاح ممکن است در سطح فدرال یا توسط هر یک از سازمان‌ها انجام شود.

[124] public key infrastructure

[125] industrial control systems

بخش‌های خاص تهیه کند و بدین منظور، مجموعه‌های پایه کنترل‌های امنیتی استاندارد سیستم‌های امنیت ملی را تغییر دهد و اصلاح کند و بدین ترتیب به مجموعه‌ای از کنترل‌های امنیتی و راهنمایی‌های پیاده‌سازی اختصاصی دست یابد. در هر یک از این مثال‌ها، مجموعه‌های پایه اصلاح‌شده را می‌توان برای هر یک از حوزه‌های فناوری اطلاعات تهیه کرد یا آن‌ها را با شرایط و محیط‌های خاص منطبق ساخت و به سازمان‌های مختلفی ارائه نمود. بدین ترتیب، می‌توان به قابلیت‌های امنیتی مورد نظر دست یافت، روش‌های یکسانی را برای پیاده‌سازی کنترل‌های امنیتی عرضه کرد، و امنیت را به صورت مقرون‌به‌صرفه تأمین نمود.

برای ارائه مجموعه‌های ویژه کنترل‌های امنیتی قابل استفاده در سیستم‌های اطلاعاتی سازمان‌های مختلف، مفهوم «پوشش»[۱۲۶] را تعریف می‌کنیم. یک پوشش در واقع مجموعه‌ای کاملاً اختصاصی از کنترل‌های امنیتی، کنترل‌های پیشرفته و راهنمایی‌های تکمیلی است که حاصل پیاده‌سازی راهنمایی‌های اختصاصی مورد اشاره در بخش ۳,۲ روی مجموعه‌های پایه کنترل‌های امنیتی مورد اشاره در پیوست ت هستند[۱۲۷]. پوشش‌ها، مجموعه‌های پایه کنترل‌های امنیتی را از این راه‌ها تکمیل می‌نمایند: (۱) فراهم آوردن موقعیتی برای اضافه کردن یا حذف کردن کنترل‌ها؛ (۲) قابل اجرا کردن کنترل‌های امنیتی و تفسیر کاربرد آن‌ها در فناوری‌های اطلاعات، پارادایم‌های پردازشی، محیط‌های کاری، انواع سیستم‌های اطلاعاتی، انواع عملیات و مأموریت‌ها، حالت‌های عملیاتی، بخش‌های صنعتی، و الزامات قانونی و مقرراتی؛ (۳) تعیین مقادیر پارامترها در عبارات انتخاب و اختصاص کنترل‌های امنیتی و کنترل‌های پیشرفته، به گونه‌ای که برای تمام سازمان‌ها قابل استفاده باشد؛ و (۴) توسعه راهنمایی‌های تکمیلی برای کنترل‌های امنیتی، در صورت لزوم. معمولاً سازمان‌ها در صورتی اقدام به استفاده از مفهوم پوشش می‌کنند که مشاهده کنند فروض اولیه مورد استفاده برای تولید مجموعه‌های پایه کنترل‌های امنیتی به درستی اعمال نشده‌اند و انحرافاتی در این زمینه وجود دارد (بخش ۳,۱ را ملاحظه کنید). اگر سازمان‌ها انحرافی از فروض مذکور نداشته باشند، احتمالاً هیچ نیازی به تهیه پوشش نیز نخواهد بود. همچنین ممکن است برخی فروض اولیه در نظر گرفته نشده باشند و بدین ترتیب تهیه یک پوشش با فروض جدید توجیه گردد.

برای پشتیبانی از موارد گفته‌شده، سازمان‌ها می‌توانند تغییرات و اصلاحات مختلفی را به کار گیرند و بدین ترتیب رویکرد منظم و ساختارمندی را تهیه نمایند. با استفاده از پوشش‌ها می‌توان اجماعی را بین سازمان‌های

---

[126] overlay

[۱۲۷] **دستورالعمل** CNSS 1253 راهنمایی‌های اختصاصی و مجموعه‌های پایه کنترل‌های امنیتی را برای سیستم‌های امنیت ملی ارائه می‌کند.

مختلف پدید آورد و مجموعه‌ای از طرح‌های امنیتی را برای آن‌ها تهیه کرد که مبتنی بر شرایط و موقعیت‌های خاص طراحی شده باشند. به عنوان مثالی از دسته‌ها مختلف پوشش‌ها، می‌توان به موارد زیر اشاره کرد:

- سازمان‌های دارای منافع یکسان، بخش‌های صنعتی یا همکاری‌ها و ائتلافات سازمانی (مانند بهش بهداشت و درمان، نهادهای مجری قانون، نهادهای اطلاعاتی، مؤسسات مالی، شرکت‌های حمل‌ونقل، تولیدکنندگان انرژی، و ائتلافات و همکاری‌های سازمانی)؛
- پارادایم‌های پردازشی و فناوری‌های اطلاعاتی (مانند کلاد، دستگاه‌های همراه، PKI، شبکه‌های هوشمند، و روش‌هایی که حوزه‌های مختلف را پوشش می‌دهند)؛
- محیط‌های کاری (مانند محیط‌های فضایی یا نظامی)؛
- انواع سیستم‌های اطلاعاتی یا حالت‌های عملیاتی (مانند سیستم‌های کنترل فرایند و سیستم‌های کنترل صنعتی، سیستم‌های تسلیحاتی، سیستم‌های تک‌کاربری، سیستم‌های مستقل)؛
- انواع عملیات و مأموریت‌ها (مانند مبارزه با تروریسم، واکنش سریع، تحقیق، توسعه، آزمون و ارزیابی)؛ و
- الزامات قانونی و مقرراتی (مانند قانون نظارت بر اطلاعات خارجی[۱۲۸]، قانون پاسخگویی و قابلیت انتقال بیمه درمانی[۱۲۹]، قانون حریم خصوصی[۱۳۰]).

سازمان‌ها می‌توانند در هنگام تهیه پوشش‌ها، از مفاهیم مدیریت مخاطره که در شماره ویژه NIST 800-39 آمده است استفاده کنند. توسعه موفقیت‌آمیز پوشش‌ها نیازمند ایفای نقش این کارشناسان است: (۱) کارشناسان امنیت اطلاعات که با موضوع اصلی پوشش‌ها آشنا هستند؛ و (۲) کارشناسان حوزه تخصصی پوشش‌ها که کنترل‌های امنیتی مورد اشاره در پیوست ج و مجموعه‌های پایه مورد اشاره در پیوست ت را می‌شناسند. قالب و ساختار پوشش‌ها در پیوست خ تشریح شده است.

می‌توان از چند پوشش برای یک مجموعه پایه واحد از کنترل‌های امنیتی استفاده کرد. مجموعه‌های پایه اصلاح‌شده در جریان فرایند تهیه پوشش‌ها، می‌توانند کمابیش دقیق‌تر از مجموعه‌های پایه کنترل‌های امنیتی باشند. سازمان‌ها در فرایند بررسی مخاطرات به اطلاعاتی دست می‌یابند که می‌توانند بر اساس آن تعیین کنند آیا مخاطرات ناشی از پیاده‌سازی مجموعه‌های پایه اصلاح‌شده، در محدوده تحمل مخاطرات سازمان قرار می‌گیرد یا خیر. اگر از چند پوشش مختلف استفاده شود، ممکن است تضاد و تعارضی بین این کنترل‌ها پدید آید. اگر این امر باعث شود که سازمان بر سر دو راهی پیاده‌سازی یا حذف کنترل‌های امنیتی قرار گیرد،

[128] Foreign Intelligence Surveillance Act
[129] Health Insurance Portability and Accountability Act
[130] Privacy Act

مسئولین صدور مجوز (یا افراد منصوب آن‌ها) با همفکری مالکان مأموریت/کسب و کار یا مالکان سیستم‌های اطلاعاتی، تصمیم‌گیری‌های لازم برای حل تعارض را انجام می‌دهند. به طور کلی، پوشش‌ها مجموعه‌ای از کنترل‌های امنیتی و کنترل‌های پیشرفته را بر اساس شرایط و موقعیت‌های معمول سازمان انتخاب می‌کنند، به گونه‌ای که نیاز به تغییر و اصلاح موقتی مجموعه‌های پایه کمتر شود. اما استفاده از پوشش‌ها مانع از این نمی‌شود که سازمان‌ها تغییرات و اصلاحات بیشتری را انجام دهند تا نیازها و محدودیت‌های خود را برآورده سازند. تغییر و اصلاح پوشش‌ها بر اساس محدودیت‌های موجود انجام می‌شود و ممکن است نیازمند تأیید مسئولین صدور مجوز یا سایر افراد مسئول باشد. به عنوان مثال، پوششی که برای یک سیستم کنترل صنعتی (ICS) تهیه شده است، ممکن است نیازمند تغییر و اصلاح باشد تا بتوان آن را در نوع خاصی از این سیستم‌ها و محیط‌های کاری آن‌ها مورد استفاده قرار داد. اما انتظار می‌رود که استفاده از پوشش‌ها، سبب کاهش دفعات و حجم تغییرات و اصلاحات سازمانی شود.

۳-۴- مستندسازی فرایند انتخاب کنترل‌ها

سازمان‌ها، تصمیمات اتخاذشده در جریان انتخاب کنترل‌های امنیتی را مستندسازی می‌کنند و بدین ترتیب، منطق نهفته در پس این تصمیمات را ثبت می‌نمایند. این مستندسازی برای بررسی ملاحظات امنیتی سیستم‌های اطلاعاتی و همچنین مأموریت و فرایند کسب‌وکار سازمان ضرورت دارد. مجموعه کنترل‌های امنیتی انتخاب‌شده و منطق انتخاب آن‌ها در قالب طرح‌های امنیتی مستندسازی می‌شوند. مستندسازی تصمیمات مهم مدیریت مخاطرات بدین دلیل ضرورت دارد که مسئولین صدور مجوز می‌توانند با توجه به آن‌ها، اطلاعات لازم برای تصمیم‌گیری در خصوص سیستم‌های اطلاعاتی سازمان را به دست آورند[۱۳۱]. بدون در اختیار داشتن این اطلاعات، مسئولین مذکور در صورت تغییر محیز سیستم‌های اطلاعاتی یا بازبینی تصمیمات اولیه، به دانش، فروض، محدودیت‌ها و منطق پشتیبان تصمیمات مدیریت مخاطرات نیز دسترسی نخواهند داشت. شکل ۴ فرایند انتخاب کنترل‌های امنیتی را به اختصار شرح می‌دهد. در این شکل به فرایند انتخاب مجموعه‌های پایه و تغییر و اصلاح آن‌ها با استفاده از راهنمایی‌های ارائه‌شده در بخش ۳,۲ نیز پرداخته شده است.

****

شکل ۴: فرایند انتخاب کنترل‌های امنیتی

[۱۳۱] فرایند انتخاب کنترل‌های امنیتی، در مورد ارائه‌دهندگان کنترل‌های معمول و مسئولین صدور مجوز که در خصوص پیاده‌سازی این کنترل‌ها در سازمان تصمیم‌گیری می‌کنند نیز انجام می‌شود.

****

ماهیت تکرارشونده و پویای فرایند تغییر و اصلاح کنترل‌های امنیتی

فرایند تغییر و اصلاح کنترل‌های امنیتی که در بالا به آن اشاره شد، هرچند که در ابتدا به صورت سلسله‌ای از مراحل به نظر می‌رسد، اما ماهیتی تکرارشونده نیز دارد. سازمان‌ها می‌توانند مراحل مختلف این فرایند را به ترتیب دلخواه انجام دهند. این ترتیب بر اساس نیازهای سازمان و اطلاعات گردآوری‌شده در مرحله بررسی مخاطرات خواهد بود. به عنوان مثال، برخی سازمان‌ها ممکن است مقادیر پارامترها را پیش از انتخاب کنترل‌های جبرانی تعیین نمایند. اما برخی سازمان‌های دیگر ممکن است ابتدا فعالیت‌های تکمیلی را انجام دهند و سپس به سراغ تعیین مقادیر بروند. ممکن است پس از تعیین کامل کنترل‌های امنیتی برای محیط‌های کاری مورد نظر، مشکلاتی پیش آید که نیاز به کنترل‌های اضافه (تکمیلی) را فراهم آورد. در پایان نیز باید گفت که فرایند تغییر و اصلاح کنترل‌های امنیتی، فرایندی ایستا نیست. به عبارت دیگر، سازمان‌ها هر گاه لازم باشد اقدام به بازبینی فرایند تغییر و اصلاح می‌کنند. این نیاز بر اساس اطلاعاتی تعیین می‌شود که از فرایند بررسی مخاطرات سازمانی به دست آمده است.

علاوه بر ماهیت تکرارشونده و پویای فرایند تغییر و اصلاح کنترل‌های امنیتی، ممکن است حذف یا اضافه کردن کنترل‌های امنیتی به مجموعه‌های پایه، اثرات جانبی را برای سازمان به دنبال داشته باشد. کنترل‌های امنیتی مورد اشاره در پیوست ج ممکن است به سایر کنترل‌ها وابسته باشند یا همپوشانی‌هایی را از لحاظ عملکردی با آن‌ها داشته باشند. در بسیاری از حالت‌ها، کنترل‌های امنیتی به همراه یکدیگر به کار گرفته می‌شوند تا در مجموع یک قابلیت امنیتی به دست آید. بنابراین، حذف یکی از کنترل‌ها از مجموعه پایه ممکن است اثراتی بر سایر کنترل‌ها داشته باشد. همچنین، اضافه کردن یک کنترل امنیتی به مجموعه پایه ممکن است نیاز به برخی کنترل‌های خاص را کاهش دهد یا به طور کلی برطرف سازد، زیرا شاید کنترل جدید قابلیت امنیتی بهتری را نسبت به سایر کنترل‌ها فراهم آورد. به عنوان مثال، اگر سازمان‌ها کنترل امنیتی SC-30(2) را با استفاده از روش‌های مجازی‌سازی پیاده نمایند تا بدین ترتیب برنامه‌های کاربردی و سیستم‌های مختلفی را به طور منظم و تصادفی به کار گیرند، این امر می‌تواند نیاز به به‌روزرسانی پیکربندی‌های امنیتی در CM-2(2) را کاهش دهد. بنابراین، اضافه کردن و حذف کردن کنترل‌های امنیتی با توجه به نیازهای سازمان و سیستم‌های اطلاعاتی آن در زمینه امنیت اطلاعات انجام می‌شود، و تنها خود کنترل‌های حذف یا اضافه‌شده در این میان تأثیرگذار نیستند.

نکاتی برای پیاده‌سازی بهتر

در فرایند تغییر و اصلاح کنترل‌های امنیتی، سازمان‌ها به برخی پیوندهای بسیار مهم بین کنترل‌های امنیتی و کنترل‌های پیشرفته مختلف توجه می‌کنند. این پیوندها در فرایند انتخاب کنترل‌های امنیتی و کنترل‌های پیشرفته نیز مد نظر قرار می‌گیرند، اما در مرحله تهیه پوشش‌ها از اهمیت ویژه‌ای برخوردارند (این امر در بخش ۳,۳ و پیوست خ تشریح شده است). در برخی موارد، این پیوندها به گونه‌ای هستند که اضافه کردن یک کنترل امنیتی یا کنترل پیشرفته، بدون اضافه کردن یک کنترل امنیتی یا کنترل پیشرفته دیگر بی معنی خواهد بود. تمامی کنترل‌های امنیتی و کنترل‌های پیشرفته به همراه یکدیگر هستند که یک قابلیت امنیتی را ایجاد می‌کنند. برخی پیوندها واضح و آشکار هستند، که به عنوان مثال می‌توان به پیوند بین کنترل پیشرفته دسترسی اجباری ((AC-3(3)) و ویژگی‌های امنیتی (AC-16) اشاره کرد. اما برخی پیوندها ممکن است چندان آشکار نباشند. این امر به ویژه در مورد پیوند بین کنترل‌های مربوط به عملکرد امنیتی و کنترل‌های مربوط به ضمانت امنیتی مصداق دارد، که در پیوست ث تشریح شده است. به عنوان مثال، پیاده‌سازی کنترل امنیتی AC-3(3) بدون پیاده‌سازی پایش مرجع (AC-25) چندان معنادار نخواهد بود. بهتر است سازمان‌ها توجه ویژه‌ای به بخش «کنترل‌های مربوطه» در قسمت «راهنمایی‌های تکمیلی» داشته باشند تا بتوانند این پیوندها را شناسایی کنند.

سایر ملاحظات

تصمیمات سازمان‌ها در زمینه تغییر و اصلاح کنترل‌های امنیتی، در خلأ اتخاذ نمی‌شوند. این تصمیمات کاملاً مبتنی بر ملاحظات مربوط به امنیت اطلاعات هستند. اما سازمان‌ها باید توجه داشته باشند که تصمیمات مذکور به سایر عوامل مخاطره معمول سازمانی نیز بستگی دارند. عوامل مخاطره مانند هزینه، زمان‌بندی و عملکرد، در تمامی تصمیمات مربوط به پیاده‌سازی کنترل‌های امنیتی در سیستم‌های اطلاعاتی و محیط‌های کاری در نظر گرفته می‌شوند. به عنوان مثال، در سیستم‌های کنترلی و محیط‌های نظامی که در آن‌ها پای زندگی افراد در میان است، پیاده‌سازی کنترل‌های امنیتی بر اساس الزامات عملیاتی انجام می‌شود. در مورد سیستم‌های کنترل ترافیک هوایی و کنسول‌های مورد استفاده برای این کار، نیاز به بررسی بلادرنگ کنسول‌ها نسبت به نیاز امنیتی

قفل نشست یا AC-11 اهمیت بیشتری دارد. به اختصار، فرایند انتخاب کنترل‌های امنیتی (شامل فعالیت‌های تغییر و اصلاح کنترل‌های امنیتی که در بخش ۳,۲ تشریح شده است) باید به همراه فرایند مدیریت مخاطرات انجام شود که در شماره ویژه NIST 800-39 تشریح شده است.

در پایان، سازمان‌ها عامل مقیاس‌پذیری را در فرایند انتخاب کنترل‌های امنیتی در نظر می‌گیرند. به عبارت دیگر، مقیاس‌پذیری کنترل‌ها بر اساس میزان و حیطه پیاده‌سازی آن‌ها تعیین می‌شود. مقیاس‌پذیری بر اساس اسناد FIPS 199 و FIPS 200 مشخص می‌شود. به عنوان مثال، طرح‌های اضطراری مربوط به سیستم‌های اطلاعاتی با سطح تأثیر زیاد، ممکن است شامل جزئیات زیادی در زمینه چگونگی پیاده‌سازی بوده و بنابراین بیش از حد طویل باشند. در مقابل، ممکن است طرح‌های اضطراری مربوط به سیستم‌های اطلاعاتی با سطح تأثیر کم شامل جزئیات چندانی نباشند و بیش از حد کوتاه به حساب آیند. سازمان‌ها در هنگام پیاده‌سازی کنترل‌های امنیتی در سیستم‌های اطلاعاتی سازمانی، احتیاط لازم را به عمل می‌آورند و ملاحظات مربوط به مقیاس‌پذیری در محیط‌های عملیاتی خاص را در نظر می‌گیرند. تعیین کنترل‌های امنیتی بر اساس سطح تأثیر سبب می‌شود که رویکردی مقرون به صرفه و مبتنی بر مخاطرات سازمانی برای پیاده‌سازی کنترل‌های امنیتی به کار گرفته شود. بدین ترتیب، مشخص می‌شود که برای کاهش مخاطرات تا سطح مطلوب به چه منابعی نیاز است، و در ادامه تنها همان منابع به کار گرفته می‌شوند تا صرفه‌جویی لازم به عمل آید.

نکاتی برای پیاده‌سازی بهتر

ثبت سوابق مربوط به فرایند انتخاب کنترل‌های امنیتی و وضعیت این کنترل‌ها، می‌تواند در قالب چند سند یا طرح امنیتی انجام شود. اگر از چند سند استفاده شود، سازمان‌ها می‌توانند به منابع اصلی ارجاع دهند و از کپی کردن دوباره اطلاعات پرهیز نمایند. بدین ترتیب، تهیه اسناد مذکور به زمان و منابع کمتری نیاز خواهد داشت. علاوه بر این، آگاهی امنیتی بالاتر می‌رود و قابلیت‌های سیستم‌های اطلاعاتی بهتر درک می‌شوند. این امر سبب می‌شود که استفاده از اطلاعات امنیتی در سیستم‌های اطلاعاتی سازمان به گونه‌ای بهتر و کارامدتر انجام شود.

۳-۵- سیستم‌های جدید و سیستم‌های بازمانده از قبل

فرایند انتخاب کنترل‌های امنیتی که در این بخش تشریح شده است را می‌توان از دو چشم‌انداز مختلف در سیستم‌های اطلاعاتی سازمان اجرا کرد: (۱) سیستم‌های جدید؛ و (۲) سیستم‌های بازمانده از قبل. در مورد سیستم‌های جدید، فرایند انتخاب کنترل‌های امنیتی از چشم‌انداز «تعریف الزامات» انجام می‌شود، زیرا سیستم از قبل وجود نداشته است و سازمان باید دسته‌بندی امنیتی اولیه را انجام دهد. کنترل‌های امنیتی مورد اشاره در طرح‌های امنیتی، به عنوان ویژگی‌های امنیتی در نظر گرفته می‌شوند و انتظار می‌رود که در مراحل توسعه و پیاده‌سازی، در سیستم‌های اطلاعاتی به کار گرفته شوند. اما در مورد سیستم‌های بازمانده از قبل، و در هنگامی که سازمان‌ها انتظار تغییرات زیادی را در سیستم‌ها داشته باشند (مثلاً در صورت به‌روزرسانی‌ها، تغییرات، یا برون‌سپاری‌های گسترده)، از چشم‌انداز «تحلیل کمبودها» استفاده می‌شود.از آنجا که این سیستم‌های اطلاعاتی در سازمان موجود هستند، سازمان‌ها پیشتر مراحل فرایند دسته‌بندی امنیتی و انتخاب کنترل‌های امنیتی را انجام داده‌اند، طرح‌های امنیتی را تهیه کرده‌اند و در زمینه پیاده‌سازی کنترل‌های امنیتی در سیستم‌های اطلاعاتی تصمیم‌گیری نموده‌اند. بنابراین، می‌توان تحلیل کمبودها را بدین ترتیب انجام داد:

- نخست دسته‌بندی امنیتی و سطح تأثیر سیستم‌های اطلاعاتی را بر اساس انواع اطلاعاتی که در حال پردازش، ذخیره شدن یا انتقال هستند، تأیید یا به‌روز کنید.
- در مرحله دوم، طرح امنیتی فعلی و کنترل‌های امنیتی را بازبینی کنید. در این فرایند باید تغییرات صورت‌گرفته در دسته‌بندی امنیتی سیستم‌های اطلاعاتی و سطح تأثیر آن‌ها، و همچنین تغییرات رخ‌داده در سازمان، مأموریت و فرایند کسب‌وکار، سیستم، یا محیط کاری را مد نظر قرار دهید. مخاطرات را مجدداً بررسی کنید و طرح امنیتی را بازبینی نمایید. تمامی کنترل‌هایی که ممکن است لازم باشند را ثبت و مستندسازی کنید تا اطمینان حاصل نمایید که مخاطرات پیش روی عملیات سازمانی، سرمایه‌های سازمانی، افراد، سایر سازمان‌ها و مردم، در سطح قابل‌قبولی قرار خواهند داشت.
- در مرحله سوم، کنترل‌های امنیتی مستندسازی‌شده در طرح امنیتی جدید را پیاده کنید، کنترل‌هایی را که پیاده‌سازی نشده‌اند در طرح عملیاتی مستند کنید، و بقیه مراحل چارچوب مدیریت مخاطره را به طور معمول انجام دهید.

تحلیل کمبودها برای تأمین‌کنندگان خدمات خارجی

تحلیل کمبودها در مورد تأمین‌کنندگان خدمات خارجی نیز به کار گرفته می‌شود. چنان که در بخش ۲,۵ گفته شد، سازمان‌ها هر روز بیشتر از قبل برای تأمین خدمات سیستم‌های اطلاعاتی خود به تأمین‌کنندگان خارجی وابسته می‌شوند. سازمان‌ها می‌توانند با استفاده از مراحلی که پیشتر در مورد تحلیل کمبودها گفته شد،

تأمین‌کنندگان خدمات خارجی را ملزم کنند که دسته‌بندی امنیتی و انتخاب کنترل‌های امنیتی را بر اساس مراحل چارچوب مدیریت مخاطره انجام دهند. اطلاعات حاصله می‌تواند سازمان‌ها را یاری کند تا تعیین کنند تأمین‌کنندگان خدمات خارجی کدام کنترل‌های امنیتی را در اختیار دارند و کدام کنترل‌ها را باید تهیه کنند. در صورتی که نقصی در زمینه کنترل‌های امنیتی وجود داشته باشد، مسئولیت مخاطرات غیر قابل قبول ناشی از پیاده‌سازی آن‌ها بر عهده مسئولین صدور مجوز خواهد بود. در این شرایط، سازمان‌ها می‌توانند با انجام مراحل زیر، مخاطرات را تا سطح قابل قبول کاهش دهند:

- استفاده از بندهای موجود در قراردادها تا تأمین‌کنندگان خدمات خارجی را ملزم کنند که الزامات امنیتی دیگری که سازمان در نظر گرفته است را نیز رعایت کنند؛
- درخواست از تأمین‌کنندگان مذکور برای فراهم آوردن کنترل‌های امنیتی مورد نیاز، در صورتی که بندهای لازم در قراردادها وجود نداشته باشد؛
- اجازه دادن به تأمین‌کنندگان مذکور برای استفاده از کنترل‌های جبرانی؛ یا
- به کار گرفتن اقدامات دیگری در سیستم‌های اطلاعاتی سازمانی برای کاهش مخاطرات[۱۳۲]، در صورتی که قراردادی وجود نداشته باشد یا این که بندهای لازم برای تأمین سطح مورد نیاز امنیت در قراردادها وجود نداشته باشد.

نکاتی برای پیاده‌سازی بهتر

بسیاری از سازمان‌ها از سیستم‌های اطلاعاتی پیچیده‌ای استفاده می‌کنند، که معمولاً به آن‌ها "سیستمی متشکل از سیستم‌ها» گفته می‌شود. در مورد این نوع از سیستم‌های اطلاعاتی، معماری سازمان نقش مهمی در انتخاب کنترل‌های امنیتی ایفا می‌کند. برای غلبه بر مشکلات ناشی از به‌کارگیری سیستم‌های پیچیده، سازمان‌ها می‌توانند سیستم‌های مذکور را به مجموعه‌ای از چند سیستم ساده‌تر تفکیک کنند و دسته‌بندی امنیتی FIPS 199 و سطح تأثیر FIPS 200 را در مورد هر یک از آن‌ها به کار گیرند. در نظر گرفتن سطوح تأثیر مختلف برای هر یک از این سیستم‌های ساده، سطح تأثیر کلی سیستم اطلاعاتی را تغییر نمی‌دهد، بلکه به هر یک از سیستم‌ها اجازه می‌دهد که کنترل‌های امنیتی متناسب با سطح تأثیر خود را به کار گیرند و همگی آن‌ها مجبور به پیاده‌سازی کنترل‌های امنیتی با سطح تأثیر زیاد نباشند. البته سازمان‌ها نمی‌توانند هر یک از

[۱۳۲] به عنوان مثال، سازمان‌ها می‌*توانند خط*مشی‌ها، روش‌های اجرایی و/یا کنترل‌های جبرانی را برای کاهش ریسک‌های شناسایی‌شده در جریان تحلیل کمبودها تهیه کنند و به کار گیرند.

سیستم‌ها را به عنوان یک موجودیت کاملاً مجزا و مستقل در نظر بگیرند، زیرا این سیستم‌ها دارای پیوند و رابطه درونی هستند.

سازمان‌ها با استفاده از معماری‌های امنیتی، اقدام به تخصیص کنترل‌های امنیتی به هر یک از سیستم‌ها می‌کنند و بدین ترتیب، ارتباطات را در مرزهای اصلی درون سیستم کنترل و پایش می‌نمایند و کنترل‌هایی را نیز برای کل سیستم در نظر می‌گیرند. سازمان‌ها همچنین به این نکته نیز توجه دارند که سیستم‌های فرعی یکسان، آسیب‌پذیری‌های یکسانی دارند که سبب می‌شود سازمان از یک نقطه ضعف واحد بارها خسارت ببیند. سازمان‌ها تلاش می‌کنند تا این تکرارها را کاهش دهند، زیرا خسارت ناشی از یک سیستم فرعی می‌تواند بسیاری از سیستم‌های فرعی دیگر را نیز به صورت همزمان تحت تأثیر قرار دهد.

پیوست‌ها (صفحات ۱۵۱ تا ۴۰۱)

پیوست ث

ضمانت و قابلیت اعتماد

شاخص‌های اعتماد به سیستم‌های اطلاعاتی

ضمانت‌های امنیتی از مسائل مهم در تعیین قابلیت اعتماد سیستم‌های اطلاعاتی به شمار می‌آیند. ضمانت‌های امنیتی نشان می‌دهند که تا چه حد می‌توان اعتماد داشت که کارکردها، ویژگی‌ها، اقدامات، خط‌مشی‌ها، رویه‌ها، سازوکارها و معماری امنیتی سازمان، خط‌مشی‌های امنیتی تعیین‌شده را به اجرا می‌گذارند[۱۳۳]. هدف از این پیوست به شرح زیر است:

- ترغیب سازمان‌ها برای رعایت الزامات ضمانتی در تأمین و تدارکات سیستم‌های اطلاعاتی، مؤلفه‌های سیستم‌ها و خدمات؛
- ترغیب تولیدکنندگان سخت‌افزار، نرم‌افزار و ثابت‌افزار برای استفاده از فرایندهای توسعه‌ای که منجر به افزایش قابلیت اعتماد سیستم‌ها و محصولات IT می‌شوند؛
- ترغیب سازمان‌ها برای شناسایی، انتخاب و استفاده از محصولات IT با سطح ضمانتی مناسب و استفاده از سیستم‌های ایمن و شیوه‌های مهندسی امن در فرایند چرخه عمر توسعه سیستم؛
- کاهش ریسک امنیت اطلاعات با استفاده از محصولات IT مطمئن‌تر در سیستم‌های اطلاعاتی اصلی یا مؤلفه‌های آن‌ها؛ و
- ترغیب توسعه‌دهندگان و سازمان‌ها برای جمع‌آوری مستمر شواهد ضمانتی که نشان‌دهنده قابلیت اعتماد سیستم‌های اطلاعاتی باشند.

حداقل الزامات امنیتی مربوط به اطلاعات و سیستم‌های اطلاعاتی فدرال، در سند FIPS 200 تشریح شده‌اند. برای رعایت این الزامات باید کنترل‌های امنیتی با سطح تأثیر کم، متوسط و زیاد را از مجموعه‌های پایه

---

[۱۳۳] **بخش ۲-۶** مفهوم ضمانت امنیتی و قابلیت اعتماد را شرح می‌دهد و بیان می‌کند که این دو مفهوم چه ارتباطی با یکدیگر دارند. یک مدل قابلیت اعتماد در شکل **۳ نشان داده‌شده است**.

لیست‌شده در پیوست ت انتخاب، اصلاح و پیاده‌سازی کرد[۱۳۴]. این مجموعه‌های پایه همچنین شامل کنترل‌های ضمانتی برای حداقل الزامات مربوط به اطلاعات و سیستم‌های اطلاعاتی فدرال هستند[۱۳۵]. با این حال، از آنجا که فضای تهدیدات تغییر کرده و تهدیدات مستمر پیشرفته (APT) چالش‌های بیشتری را در پیش روی دارایی‌ها و عملیات سازمان، افراد، سایر سازمان‌ها و ملت قرار داده‌اند، ممکن است سازمان‌ها تصمیم بگیرند از برخی کنترل‌های ضمانتی لیست‌شده در پیوست ج نیز استفاده کنند. این کنترل‌های اضافی را می‌توان بر اساس راهنمایی‌های اصلاحی تشریح‌شده در بخش ۳-۲ انتخاب کرد. سازمان‌ها همچنین می‌توانند پوشش‌هایی با سطح ضمانت بالا را برای مأموریت‌ها و کارکردهای کسب‌وکار، محیط‌های عملیاتی خاص و/یا فناوری‌های اطلاعاتی تهیه کنند (بخش ۳-۳ از پیوست خ را ملاحظه کنید). در صورت رعایت الزامات کنترل‌های ضمانتی، سازمان‌ها می‌توانند کنترل‌های جبرانی را پیشنهاد دهند یا میزان مخاطره بالاتری را در زمینه قابلیت‌های امنیتی واقعی خود بپذیرند.

نگاهی جدید به ضمانت‌های امنیتی

هرچند که نسخه‌های قبلی نشریه ویژه ۵۳-۸۰۰ به حداقل الزامات ضمانتی پرداخته‌اند، اما تمرکز آن‌ها بیشتر بر الزامات سطح بالاتر و انتزاعی‌تر مجموعه‌های پایه با سطح تأثیر کم، متوسط و زیاد بوده است. در این نسخه رویکرد کاملاً متفاوتی به کار گرفته شده و کنترل‌های ضمانت امنیتی خاصی در پیوست ج ارائه شده‌اند که سازمان‌ها می‌توانند بر اساس دسته‌بندی امنیتی سیستم‌های اطلاعاتی خود از آن‌ها استفاده نمایند. بدین ترتیب، الازمات ضمانتی مذکور *عملی‌تر* خواهند بود و موقعیت‌هایی را برای افزایش سطح ضمانت بر اساس نیازهای کسب‌وکار و مأموریت سازمان، تهدیدات فعلی و تهدیدات مورد انتظار، محیط‌های عملیاتی منحصربه‌فرد و کاربرد فناوری‌های جدید، در اختیار سازمان قرار می‌دهند. جداول ساده ارائه‌شده در این بخش (جداول ث-۱، ث-۲ و ث-۳) به سازمان کمک می‌کنند تا کنترل‌های ضمانتی مناسب را به راحتی پیدا کنند و کنترل‌های لازم برای رعایت حداقل الزامات را تعریف نمایند. کنترل‌های ضمانتی اختیاری در جدول ث-۴، ویژگی‌های قابل استفاده در فرایندهای تملیک با توسعه‌دهندگان سیستم‌های اطلاعاتی، مؤلفه‌های این سیستم‌ها و خدمات سیستم‌های اطلاعاتی را شرح می‌دهند. این کنترل‌ها به روش‌ها، شیوه‌ها، طراحی‌ها و معماری‌ها می‌پردازند و اصول مهندسی

---

[۱۳۴] **دستورالعمل** CNSS 1253 مجموعه‌های پایه کنترل‌های امنیتی را برای سیستم‌های امنیتی ملی شرح می‌دهد. بنابراین، کنترل‌های ضمانتی در مجموعه‌های پایه مربوط به سیستم‌های امنیت ملی ممکن است با کنترل‌های تعیین‌شده در **جدول ث-۱ و ث-۳** تفاوت داشته باشند.

[۱۳۵] نمی‌**توان** به سادگی تعیین کرد که یک مجموعه پایه کنترل‌های امنیتی از پیوست ت، ضمانت مورد نیاز برای تمام فناوری‌ها، کاربران، **پلتفرم**‌ها و سازمان‌ها را تأمین می‌کند یا خیر. به عنوان مثال، هرچند که استفاده از روش‌های رسمی ممکن است در یک محصول بین دامنه‌ای **مناسب باشد، اما** در یک سیستم کنترل ترافیک هوایی پیچیده یا یک سرور وب متعلق به وزارت امنیت داخلی، باید از شیوه‌های ضمانتی متفاوتی استفاده نمود. با این حال، مجموعه‌های پایه موجود به شکلی طراحی شده‌اند که حداقل ضمانت‌های مورد انتظار تمام فناوری‌ها، کاربران، پلتفرم‌ها **وسازمان**‌ها را دارا هستند.

امنیتی برای ارتقای کیفیت نرم‌افزار، سخت‌افزار و ثابت‌افزار مورد استفاده در سیستم‌های اطلاعاتی سازمان و زیرساخت‌های اصلی را شرح می‌دهند. تخصیص کنترل‌های ضمانتی نشان‌دهنده سطح اهمیت بالاتر آن‌ها نیست. دستیابی به سطح امنیت مناسب در سیستم‌های اطلاعاتی، نیازمند به‌کارگیری ترکیب صحیحی از کنترل‌های امنیتی ضمانتی و عملکردی است. سازمان‌ها تنها با درک اهمیت مفهوم ضمانت و تعیین ضمانتی یا عملکردی بودن کنترل‌ها است که می‌توانند بهترین ترکیب کنترل‌ها را برای حفاظت از دارایی‌ها و عملیات سازمان، افراد، سایر سازمان‌ها و ملت انتخاب نمایند.

در بخش‌های بعد، کنترل‌های ضمانتی موجود در هر یک از مجموعه‌های پایه کنترل‌های امنیتی پیوست ت تشریح شده‌اند. بر اساس ویژگی‌های کلی هر کنترل می‌توان گفت که کنترل مذکور از دسته کنترل‌های ضمانتی است یا عملکردی. به طور کلی، کنترل‌های ضمانتی کنترل‌هایی هستند که: (۱) فرایندها، رویه‌ها، شیوه‌ها یا روش‌هایی را برای طراحی و توسعه سیستم‌های اطلاعاتی و مؤلفه‌های آن‌ها (یعنی سخت‌افزارها، نرم‌افزارها و ثابت‌افزارها) تعریف می‌کنند؛ (۲) فرایندهای عملیاتی پشتیبانی را ارائه می‌کنند که از آن جمله می‌توان به ارتقای کیفیت فرایندها، مؤلفه‌ها و سیستم‌ها اشاره کرد؛ (۳) شواهد امنیتی را برای فعالیت‌های عملیاتی و توسعه‌ای تهیه می‌کنند؛ (۴) مخاطره یا اثربخشی کنترل‌های امنیتی را تعیین می‌کنند؛ یا (۵) دانش، تخصص و مهارت‌های کارکنان را ارتقا می‌هند.

حتی در صورتی که کنترل‌های امنیتی برخی ویژگی‌های عملکردی داشته باشند (مانند SI-4 یا پایش سیستم‌های اطلاعاتی)، ممکن است به عنوان کنترل ضمانتی در نظر گرفته شوند. در هنگام تشریح کنترل‌های ضمانتی در مجموعه‌های پایه، تمایز بین ضمانت و عملکرد دارای اهمیت چندانی نخواهد بود. این امر تا حدی بدین دلیل است که کنترل‌های امنیتی مجموعه‌های پایه پس از اعمال فرایندهای اصلاحی تبدیل به بخشی از طرح امنیتی سیستم‌های اطلاعاتی و سازمان‌ها می‌شوند[۱۳۶]. با این حال، هنگامی که سازمان‌ها می‌خواهند کنترل‌های امنیتی اضافه‌ای را انتخاب کنند و سطح ضمانت یا اعتماد بالاتری را در عملکرد امنیتی و قابلیت‌های امنیتی خود فراهم آورند، بر اهمیت این تمایز افزوده می‌شود.

حداقل الزامات ضمانتی – سیستم‌های با سطح تأثیر کم

[۱۳۶] به سازمان‌ها توصیه می‌شود که کنترل‌های ضمانتی مجموعه‌های پایه را در فرایند اصلاح (از جمله در جریان توسعه پوشش‌ها) به دقت بررسی کنند، تا اطمینان حاصل شود که کنترل‌ها به صورت ناخواسته حذف نشده‌اند، زیرا این امر می‌تواند منجر به پایین آمدن قابلیت اعتماد عملکردهای امنیتی مورد نیاز برای حفاظت از مأموریت و کسب‌وکار سازمان شود.

الزامات ضمانتی: سازمان بر اساس الزامات امنیتی، خط‌مشی‌های امنیتی و قابلیت‌های امنیتی مورد نیاز خود، تا حد اندکی انتظار دارد که عملکرد امنیتی کامل، سازگار و صحیحی داشته باشد.

راهنمایی‌های تکمیلی: برای تأمین ضمانت و عملکرد امنیتی سیستم‌های با سطح تأثیر کم، از کنترل‌های امنیتی مجموعه‌های اصلاحی با سطح تأثیر کم که در پیوست ت به آن‌ها اشاره شده است، استفاده می‌شود. الزامات ضمانتی برای این سیستم‌ها و مؤلفه‌های آن‌ها را می‌توان با استفاده از خدمات و محصولات تجاری موجود در بازار (COTS) برآورده نمود. به دلیل محدود بودن قدرت عملکرد مورد انتظار سیستم‌های با سطح تأثیر کم، شواهد امنیتی کمترین عمق و پوشش را دارند[۱۳۷] و انتظار نمی‌رود که فراتر از عمق و پوشش ارائه‌شده توسط فروشندگان و تولیدکنندگان خدمات و محصولات تجاری موجود در بازار باشند. در کنار عمق و پوشش، از نتایج بررسی کنترل‌های امنیتی و پایش مستمر سیستم‌های اطلاعاتی سازمان و محیط‌های عملیاتی آن‌ها نیز استفاده می‌شود. در مورد عملکردهایی به جز عملکردهای فناورانه، تأکید بر اعتماد محدود به کامل بودن، صحت و سازگاری عمکردهای امنیتی عملیاتی و/یا رویه‌ای است (مانند خط‌مشی‌ها، رویه‌ها، امنیتی فیزیکی و امنیت کارکنان). الزامات ضمانتی تعیین‌شده در قالب کنترل‌های ضمانتی عملیاتی و توسعه‌ای سیستم‌های با سطح تأثیر کم، در جدول ث-۱ لیست شده‌اند. سازمان‌ها می‌توانند از طریق فرایندهای اصلاحی (شامل ارزشیابی مخاطرات سازمانی)، کنترل‌های ضمانتی یا کنترل‌های پیشرفته دیگری را نیز به این مجموعه اضافه کنند.

جدول ث-۱: کنترل‌های ضمانتی برای سیستم‌های با سطح تأثیر کم[۱۳۸]

شناسه	کنترل‌ها	شناسه	کنترل‌ها
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-3, AT-4	PE	PE-1, PE-6, PE-8
AU	AU-1, AU-6	PL	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-4, CM-8	RA	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	SA	SA-1, SA-2, SA-3, SA-4, SA-4(10), SA-5, SA-9
IA	IA-1	SC	SC-1, SC-39
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-5

[۱۳۷] نشریه ویژه شماره ۵۳-۸۰۰الف سازمان NIST اطلاعات بیشتری را درباره عمق و پوشش در فرایند ارزشیابی کنترل‌های امنیتی ارائه می‌نماید.

[۱۳۸] کنترل‌های ضمانتی مورد اشاره در جدول ث-۱ زیرمجموعه‌ای از کنترل‌های امنیتی تشریح‌شده در مجموعه‌های پایه کنترل‌های امنیتی برای سیستم‌های با سطح تأثیر کم در پیوست ت هستند. پیاده‌سازی کنترل‌های ضمانتی مورد اشاره در جدول ث-۱ (از جمله شواهد امنیتی مربوط به عمق و پوشش که در نشریه ویژه شماره ۵۳-۸۰۰الف سازمان NIST به آن‌ها اشاره شده است)، تضمین خواهد نمود که حداقل الزامات ضمانتی برای سیستم‌های با سطح تأثیر کم مورد اشاره در سند FIPS 200 رعایت شده‌اند.

MA	MA-1		

حداقل الزامات ضمانتی – سیستم‌های با سطح تأثیر متوسط

الزامات ضمانتی: سازمان بر اساس الزامات امنیتی، خط‌مشی‌های امنیتی و قابلیت‌های امنیتی مورد نیاز خود، تا حد متوسطی انتظار دارد که عملکرد امنیتی کامل، سازگار و صحیحی داشته باشد.

راهنمایی‌های تکمیلی: برای تأمین ضمانت و عملکرد امنیتی سیستم‌های با سطح تأثیر متوسط، از کنترل‌های امنیتی مجموعه‌های اصلاحی با سطح تأثیر متوسط که در پیوست ت به آن‌ها اشاره شده است، استفاده می‌شود. الزامات ضمانتی برای این سیستم‌ها و مؤلفه‌های آن‌ها را می‌توان با استفاده از این موارد برآورده نمود: (۱) خدمات و محصولات تجاری موجود در بازار (COTS) با سازوکارهای قوی‌تر و قابلیت‌های بیشتر از سیستم‌های با سطح تأثیر کم؛ (۲) برخی اصلاحات و توسعه‌های خاص؛ (۳) استفاده از تنظیمات پیکربندی امن‌تر؛ و (۴) انجام ارزشیابی بیشتر در زمینه قابلیت‌های پیاده‌سازی‌شده. به دلیل متعادل بودن قدرت عملکرد مورد انتظار سیستم‌های با سطح تأثیر متوسط، شواهد امنیتی نسبت به سیستم‌های با سطح تأثیر کم عمق و پوشش بیشتری دارند[۱۳۹]، اما کماکان انتظار نمی‌رود که فراتر از عمق و پوشش ارائه‌شده توسط فروشندگان و تولیدکنندگان خدمات و محصولات تجاری موجود در بازار باشند. در کنار عمق و پوشش، از نتایج بررسی کنترل‌های امنیتی و پایش مستمر سیستم‌های اطلاعاتی سازمان و محیط‌های عملیاتی آن‌ها نیز استفاده می‌شود. در مورد عملکردهایی به جز عملکردهای فناورانه، تأکید بر اعتماد متوسط به کامل بودن، صحت و سازگاری عمکردهای امنیتی عملیاتی و/یا رویه‌ای است (مانند خط‌مشی‌ها، رویه‌ها، امنیتی فیزیکی و امنیت کارکنان). الزامات ضمانتی تعیین‌شده در قالب کنترل‌های ضمانتی عملیاتی و توسعه‌ای سیستم‌های با سطح تأثیر متوسط، در جدول ث-۲ لیست شده‌اند. سازمان‌ها می‌توانند از طریق فرایندهای اصلاحی (شامل ارزشیابی مخاطرات سازمانی)، کنترل‌های ضمانتی یا کنترل‌های پیشرفته دیگری را نیز به این مجموعه اضافه کنند.

جدول ث-۲: کنترل‌های ضمانتی برای سیستم‌های با سطح تأثیر متوسط[۱۴۰]

---

[۱۳۹] نشریه ویژه شماره ۵۳-۸۰۰ف سازمان NIST اطلاعات بیشتری را درباره عمق و پوشش در فرایند ارزشیابی کنترل‌های امنیتی ارائه می‌نماید.

[۱۴۰] کنترل‌های ضمانتی مورد اشاره در جدول ث-۲ زیرمجموعه‌ای از کنترل‌های امنیتی تشریح‌شده در مجموعه‌های پایه کنترل‌های امنیتی برای سیستم‌های با سطح تأثیر متوسط در پیوست ت هستند. پیاده‌سازی کنترل‌های ضمانتی مورد اشاره در جدول ث-۲ (از جمله شواهد امنیتی مربوط به عمق و پوشش که در نشریه ویژه شماره ۵۳-۸۰۰ف سازمان NIST به آن‌ها اشاره شده است)، تضمین خواهد نمود که حداقل الزامات ضمانتی برای سیستم‌های با سطح تأثیر متوسط مورد اشاره در سند FIPS 200 رعایت شده‌اند. مواردی که با فونت بولد مشخص شده‌اند، نشان‌دهنده آن دسته

شناسه	کنترل‌ها	شناسه	کنترل‌ها
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-2(2), AT-3, AT-4	PE	PE-1, PE-6, PE-6(1), PE-8
AU	AU-1, AU-6, AU-6(1), AU-6(3), (AU-7, AU-7(1	PL	PL-1, PL-2, PL-2(3), PL-4, PL-4(1), PL-8
CA	CA-1, CA-2, CA-2(1), CA-3, CA-5, CA-6, CA-7, CA-7(1), CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-2(1), CM-2(3), CM-2(7), CM-3, CM-3(2), CM-4, (CM-8, CM-8(1), CM-8(3), CM-8(5	RA	RA-1, RA-3, RA-5, RA-5(1), RA-5(2), (RA-5(5
CP	(CP-1, CP-3, CP-4, CP-4(1	SA	SA-1, SA-2, SA-3, SA-4, SA-4(1), SA-4(2), SA-4(9), SA-4(10), SA-5, SA-8, SA-9, SA-9(2), SA-10, SA-11
IA	IA-1	SC	SC-1, SC-2, SC-39
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-4(2), SI-4(4), SI-4(5), SI-5, SI-7, SI-7(1), SI-7(7), SI-10, SI-16
MA	MA-1		

حداقل الزامات ضمانتی – سیستم‌های با سطح تأثیر زیاد

الزامات ضمانتی: سازمان بر اساس الزامات امنیتی، خط‌مشی‌های امنیتی و قابلیت‌های امنیتی مورد نیاز خود، تا حد زیادی انتظار دارد که عملکرد امنیتی کامل، سازگار و صحیحی داشته باشد.

راهنمایی‌های تکمیلی: برای تأمین ضمانت و عملکرد امنیتی سیستم‌های با سطح تأثیر زیاد، از کنترل‌های امنیتی مجموعه‌های اصلاحی با سطح تأثیر زیاد که در پیوست ت به آن‌ها اشاره شده است، استفاده می‌شود. الزامات ضمانتی برای این سیستم‌ها و مؤلفه‌های آن‌ها را می‌توان با استفاده از این موارد برآورده نمود: (۱) COTSهای پیشرفته‌تر با سازوکارهای قوی‌تر و قابلیت‌های بیشتر؛ (۲) برخی اصلاحات و توسعه‌های خاص؛ و (۳) انجام ارزشیابی بیشتر در زمینه قابلیت‌های پیاده‌سازی‌شده. به دلیل بالا بودن قدرت عملکرد مورد انتظار سیستم‌های با سطح تأثیر زیاد، شواهد امنیتی نسبت به سیستم‌های با سطح تأثیر متوسط عمق و پوشش بیشتری دارند[۱۴۱]. هرچند انتظار نمی‌رود که این شواهد فراتر از عمق و پوشش ارائه‌شده توسط فروشندگان و تولیدکنندگان خدمات و محصولات تجاری موجود در بازار باشند، اما ممکن است نیاز به ارزشیابی بیشتر برای

از کنترل‌های ضمانتی هستند که به مجموعه‌های پایه با سطح تأثیر کم اضافه شده‌اند تا ضمانت بیشتری را در مجموعه‌های پایه با سطح تأثیر متوسط فراهم آورند.

[۱۴۱] نشریه ویژه شماره ۵۳- ۸۰۰الف سازمان NIST اطلاعات بیشتری را درباره عمق و پوشش در فرایند ارزشیابی کنترل‌های امنیتی ارائه می‌نماید.

تأمین ضمانت باشد. در مورد عملکردهایی به جز عملکردهای فناورانه، اعتماد زیادی به کامل بودن، صحت و سازگاری عمکردهای امنیتی عملیاتی و/یا رویه‌ای (مانند خط‌مشی‌ها، رویه‌ها، امنیتی فیزیکی و امنیت کارکنان) وجود دارد. الزامات ضمانتی تعیین‌شده در قالب کنترل‌های ضمانتی عملیاتی و توسعه‌ای سیستم‌های با سطح تأثیر زیاد، در جدول ث-۳ لیست شده‌اند. سازمان‌ها می‌توانند از طریق فرایندهای اصلاحی (شامل ارزشیابی مخاطرات سازمانی)، کنترل‌های ضمانتی یا کنترل‌های پیشرفته دیگری را نیز به این مجموعه اضافه کنند.

جدول ث- ۳: کنترل‌های ضمانتی برای سیستم‌های با سطح تأثیر زیاد[۱۴۲]

شناسه	کنترل‌ها	شناسه	کنترل‌ها
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-2(2), AT-3, AT-4	PE	PE-1, PE-6, PE-6(1), PE-6(4), PE-8
AU	AU-1, AU-6, AU-6(1), AU-6(3), (AU-6(5), AU-6(6), AU-7, AU-7(1), AU-10	PL	PL-1, PL-2, PL-2(3), PL-4, PL-4(1), PL-8
CA	CA-1, CA-2, CA-2(1), CA-2(2), CA-3, CA-5, CA-6, CA-7, CA-7(1), CA-8, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-2(1), CM-2(2), CM-2(3), CM-3(1), CM-2(7), CM-3, CM-3(2), CM-4, CM-4(1), CM-8, CM-8(1), CM-8(2), CM-8(3), (CM-8(4), CM-8(5	RA	RA-1, RA-3, RA-5, RA-5(1), RA-5(2), (RA-5(4), RA-5(5
CP	CP-1, CP-3, CP-3(1), CP-4, CP-4(1), CP-4(2)	SA	SA-1, SA-2, SA-3, SA-4, SA-4(1), SA-4(2), SA-4(9), SA-4(10), SA-5, SA-8, SA-9, SA-9(2), SA-10, SA-11, SA-12, SA-15, SA-16, SA-17
IA	IA-1	SC	SC-1, SC-2, SC-3, SC-7(18), SC-7(21), SC-24, SC-39
IR	IR-1, IR-2, IR-2(1), IR-2(2), IR-5, IR-5(1)	SI	SI-1, SI-4, SI-4(2), SI-4(4), SI-4(5), SI-5, SI-7, SI-7(1), SI-7(2), SI-7(5), SI-7(7), SI-7(14), SI-10, SI-16
MA	MA-1		

[۱۴۲] کنترل‌های ضمانتی مورد اشاره در جدول ث-۳ زیرمجموعه‌ای از کنترل‌های امنیتی تشریح‌شده در مجموعه‌های پایه کنترل‌های امنیتی برای سیستم‌های با سطح تأثیر زیاد در پیوست ت هستند. پیاده‌سازی کنترل‌های ضمانتی مورد اشاره در جدول ث-۳ (از جمله شواهد امنیتی مربوط به عمق و پوشش که در نشریه ویژه شماره ۸۰۰-۵۳ **الف سازمان** NIST به آن‌ها اشاره شده است)، تضمین خواهد نمود که حداقل الزامات ضمانتی برای سیستم‌های با سطح تأثیر زیاد مورد اشاره در **سند** FIPS 200 رعایت شده‌اند. مواردی که با فونت بولد مشخص شده**اند**، **نشان**دهنده آن دسته از کنترل‌های ضمانتی هستند که به مجموعه‌های پایه با سطح تأثیر متوسط اضافه شده‌اند تا ضمانت بیشتری را در مجموعه‌های پایه با سطح تأثیر زیاد فراهم آورند.

کنترل‌های امنیتی برای دستیابی به ضمانت بیشتر

کنترل‌های ضمانتی اختصاص‌یافته به مجموعه‌های پایه با سطح تأثیر کم، متوسط و زیاد در بخش‌های قبل، بیان‌گر حداقل الزامات ضمانتی هستند. ممکن است سازمان‌ها تصمیم بگیرند که سطح ضمانت را در سیستم‌های اطلاعاتی خود افزایش دهند و به این ترتیب به قابلیت اعتماد سیستم‌های خود نیز بیفزایند. بدین منظور، برخی کنترل‌های ضمانتی به کنترل‌های مجموعه‌های پایه افزوده می‌شوند تا هم قدرت عملکرد امنیتی و هم قابلیت اطمینان عملکردها افزایش یابد. در این صورت، عملکردها در مقابل نفوذ، سرقت و دورزده‌شدن مقاوم خواهند شد. بدین ترتیب، مهاجمان نمی‌توانند محرمانگی، یکپارچگی و آماده‌به‌کار بودن سیستم‌های اطلاعاتی و مؤلفه‌های مربوطه را به سادگی به خطر اندازند.

از آنجا که ممکن است محصولات IT با سطح ضمانت بالا پرهزینه‌تر باشند و تأمین آن‌ها دشوارتر باشد، برخی سازمان‌ها سیستم‌های اطلاعاتی خود را به زیرسیستم‌هایی بخش‌بندی می‌کنند تا مؤلفه‌های حساس را جدا نمایند و سطح ضمانت مجموعه محدودتری از منابع اطلاعاتی را ارتقا دهند. سازمان‌هایی که نمی‌توانند محصولات IT با سطح ضمانت بالا را تأمین کنند، باید حفاظت عملیاتی و رویه‌ای بیشتری را به کار گیرند تا از موفقیت مأموریت و کسب‌وکار خود اطمینان حاصل نمایند. به عنوان مثال، آن‌ها باید مأموریت‌ها و فرایندهای اصلی کسب‌وکار را مهندسی مجدد کنند و از آسیب‌پذیری آن‌ها در برابر تهدیدات پیشرفته بکاهند. جدول ث-۴ فعالیت‌های عملیاتی و توسعه‌ای بیشتری را برای ارتقای سطح ضمانت به سازمان‌ها پیشنهاد می‌نماید. لیست کنترل‌های ضمانتی، لیست جامع و کاملی نیست. ممکن است سازمان‌ها در جریان فرایند اصلاحی خود، کنترل‌های امنیتی دیگری را نیز به عنوان کنترل‌های ضمانتی تعیین کنند و به جدول ث-۴ بیفزایند.

جدول ث-۴: کنترل‌های امنیتی برای ارتقای سطح ضمانت[۱۴۳]

شناسه	کنترل‌ها	شناسه	کنترل‌ها
AC	AC-25	MP	کنترل دیگری وجود ندارد
AT	(AT-2(1), AT-3 (all enhancements	PE	(PE-6(2), PE-6(3
AU	AU-6(4), AU-6(7), AU-6(8), AU-	PL	PL-8 (all enhancements), PL-9

[۱۴۳] کنترل‌های ضمانتی **مورد اشاره در جدول ث-۴ نشان**دهنده کنترل‌های امنیتی دیگری هستند که برای دستیابی به سطح ضمانت بیشتر به آن‌ها نیاز است (یعنی کنترل‌های مورد نیاز برای فراتر رفتن از سطح حداقل ضمانت تأمین‌شده توسط کنترل‌های ضمانتی لیست**شده در جداول ث-۱، ث-۲ و ث-۳**). در صورتی که یک کنترل ضمانتی به یک مجموعه پایه تخصیص داده شده باشد (یعنی در جداول ث-۱، ث-۲ و ث-۳ لیست شده باشد) اما تمامی کنترل های پیشرفته آن در جدول ث-۴ لیست شده باشند، با عبارت all enhancements به آن اشاره شده است. اگر یک کنترل ضمانتی به همراه تمامی کنترل‌های پیشرفته آن به مجموعه‌های پایه تخصیص داده نشده باشند، با عبارت plus enhancements به آن اشاره شده است. در صورتی که کنترل‌های ضمانتی پیشرفته از یک کنترل خاص به یکی از مجموعه‌های پایه تخصیص داده شده باشند، کنترل‌های پیشرفته **انتخاب**نشده به صورت تفکیکی در جدول ث-۴ لیست**شده‌اند**.

		6(9), AU-6(10), AU-10 (all enhancements), AU-11(1), AU-13 (plus enhancements), AU-14 (plus enhancements)	
PS-6(2), PS-6(3)	PS	CA-2(3), CA-5(1), CA-7(3), CA-8 (all enhancements), CA-9(1)	CA
RA-5(3), RA-5(6), RA-5(8), RA-5(10), RA-6	RA	CM-2(6), CM-4(2), CM-8(6), CM-8(7), CM-8(8), CM-8(9)	CM
SA-4(3), SA-4(5), SA-4(6), SA-4(7), SA-4(8), SA-9(1), SA-9(3), SA-9(4), SA-9(5), SA-10 (all enhancements), SA-11 (all enhancements), SA-12 (all enhancements), SA-13, SA-14, SA-15 (all enhancements), SA-17 (all enhancements), SA-18 (plus enhancements), SA-19 (plus enhancements), SA-20, SA-21 (plus enhancement), SA-22 (plus enhancement)	SA	CP-3(2), CP-4(3), CP-4(4), CP-12	CP
SC-2(1), SC-3 (all enhancements), SC-6, SC-7(22), SC-11 (plus enhancement), SC-29 (plus enhancement), SC-30 (plus enhancements), SC-31 (plus enhancements), SC-32, SC-34 (plus enhancements), SC-36 (plus enhancement), SC-37 (plus enhancement), SC-38, SC-39 (all enhancements)	SC	کنترل دیگری وجود ندارد	IA
SI-4(1), SI-4(3), SI-4(7), SI-4(9), SI-4(10), SI-4(11), SI-4(12), SI-4(13), SI-4(14), SI-4(15), SI-4(16), SI-4(17), SI-4(18), SI-4(19), SI-4(20), SI-4(21), SI-4(22), SI-4(23), SI-4(24), SI-7(3), SI-7(6), SI-7(8), SI-7(9), SI-7(10), SI-7(11), SI-7(12), SI-7(13), SI-7(15), SI-7(16), SI-10 (all enhancements), SI-13 (plus enhancements), SI-14 (plus enhancement), SI-15, SI-17	SI	IR-3(1)	IR
		کنترل دیگری وجود ندارد	MA

پیوست ج

کاتالوگ کنترل‌های امنیتی

کنترل‌های امنیتی، کنترل‌های پیشرفته، و راهنمایی‌های تکمیلی

کاتالوگ کنترل‌های امنیتی تشریح‌شده در پیوست حاضر، حیطه گسترده‌ای از ابزارهای امنیتی و روش‌های مقابله با تهدیدات را به سازمان‌ها و سیستم‌های اطلاعاتی ارائه می‌کند[۱۴۴]. کنترل‌های امنیتی به گونه‌ای طراحی شده‌اند که مطابق با دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال باشند[۱۴۵]. سازماندهی کاتالوگ کنترل‌های امنیتی، ساختار کنترل‌های امنیتی، و مفهوم تخصیص دادن کنترل‌های امنیتی و کنترل‌های پیشرفته به مجموعه‌های اولیه تشریح‌شده در پیوست ت، در فصل دوم توضیح داده شده‌اند. کنترل‌های امنیتی مورد اشاره در کاتالوگ، به استثنای چند مورد از آن‌ها، به گونه‌ای طراحی شده‌اند که مستقل از خط‌مشی و فناوری باشند. این امر بدین معنی است که کنترل‌های امنیتی و کنترل‌های پیشرفته، بر ابزارهای اصلی لازم برای حفاظت از اطلاعات در حین پردازش، ذخیره‌سازی و انتقال، تمرکز دارند. بنابراین، اشاره به فناوری‌ها، گروهای ذینفع، محیط‌های عملیاتی، مأموریت‌ها و فرایندهای کسب‌وکار خاص، خارج از دامنه شمول این سند قرار می‌گیرد. این موارد، در فصل سوم و پیوست خ پوشش داده شده‌اند.

در مواردی که برخی فناوری‌ها در کنترل‌های امنیتی مورد اشاره قرار گرفته‌اند (مانند دستگاه‌های همراه، PKI، فناوری بی‌سیم و VOIP)، به سازمان‌ها توصیه شده است که اهداف امنیتی مقتضی را (به جز الزامات ذکرشده) تعیین نمایند. بسیاری از ابزارهای حفاظتی و امنیتی مورد نیاز، از سایر کنترل‌های امنیتی مورد اشاره در کاتالوگ (که در ابتدای فرایند توسعه پوشش‌ها[۱۴۶] و طرح‌های امنیتی، به مجموعه‌های اولیه اختصاص داده شده‌اند) گرفته می‌شوند. علاوه بر توسعه پوشش‌ها و طرح‌های امنیتی، اسناد NIST و گزارشات مربوطه نیز ممکن است راهنمایی‌هایی را ارائه کنند و توصیه‌هایی را در زمینه کنترل‌های امنیتی مناسب برای فناوری‌ها و

---

[۱۴۴] نسخه آنلاین کاتالوگ کنترل‌های امنیتی را می‌توانید در این آدرس اینترنتی مشاهده کنید: http://web.nvd.nist.gov/view/800-53/home.

[۱۴۵] مطابقت با این استانداردها به این معنی است که سازمان‌ها باید حداکثر تلاش خود را برای تأمین امنیت اطلاعات و مدیریت مخاطرات انجام دهند. بدین منظور، سازمان‌ها باید تمام اطلاعات مربوط به مدیریت مخاطرات را با توجه به راهنمایی‌های ارائه‌شده در اسناد NIST به کار گیرند؛ به گونه‌ای که کنترل‌های امنیتی انتخاب‌شده در طرح‌های امنیت سازمان، متناسب با مأموریت‌ها و الزامات سازمانی باشند. برای توسعه دادن، اجرایی کردن و حفظ و نگهداری ابزارهای امنیتی و ابزارهای مقابله با تهدیدات، سازمان‌ها باید از ابزارهای امنیتی و روش‌های مناسب استفاده نمایند، تا در نهایت بتوانند تهدیدات موجود در مقابل سرمایه‌ها و فرایندهای سازمانی، افراد، سایر سازمان‌ها و ملت را از پیش رو بردارند. با استفاده از فناوری‌ها، رویه‌ها و فرایندهای مؤثر مقابله با تهدیدات، می‌توان اطمینان حاصل نمود که سازمان‌ها و سیستم‌های اطلاعاتی فدرال، قدرت کافی برای پشتیبانی از مسئولیت‌های فدرال، زیرساخت‌های مهم، و استمرار حکومت را دارا هستند.

[146] overlays

کاربردهای خاص (مانند شبکه‌های برق هوشمند، حوزه بهداشت و درمان، سیستم‌های کنترل صنعتی، و دستگاه‌های همراه) مطرح نمایند.

استفاده از یک کاتالوگ کنترل امنیتی مستقل از فناوری و خط‌مشی، مزایای زیر را به همراه دارد:

- سازمان‌ها را ترغیب می‌کند تا صرف نظر از فناوری‌های اطلاعاتی مورد استفاده در سیستم‌های اطلاعاتی سازمان، بر قابلیت‌های امنیتی مورد نیاز برای موفقیت مأموریت‌ها و فرایندهای کسب‌وکار و همچنین بر حفاظت از اطلاعات تمرکز نمایند؛
- سازمان‌ها را ترغیب می‌کند تا کنترل‌های امنیتی را بررسی کنند و تعیین نمایند که کدام یک متناسب با فناوری‌ها، محیط‌های عملیاتی، مأموریت‌ها و فرایندهای کسب‌وکار، و گروه‌های ذینفع هستند؛ و
- سازمان‌ها را ترغیب می‌کند تا خط‌مشی‌های امنیتی را به عنوان بخشی از فرایند اصلاح و شخصی‌سازی کنترل‌های امنیتی و پارامترهای آن‌ها توسعه دهند.

به عنوان مثال، سازمان‌هایی که از گوشی‌های هوشمند، تبلت‌ها یا سایر دستگاه‌های همراه استفاده می‌کنند، فرایند اصلاح و تعدیل خود را با این فرض آغاز می‌نمایند که تمام کنترل‌های امنیتی و کنترل‌های پیشرفته مورد اشاره در مجموعه اولیه مربوطه (با تأثیر کم، متوسط یا زیاد) مورد نیاز هستند. ممکن است در این فرایند، برخی از کنترل‌های امنیتی به دلایل مختلف حذف شوند. به عنوان مثال، ممکن است فناوری مورد استفاده، قابلیت پشتیبانی از آن‌ها را نداشته باشد. اما حذف کردن کنترل‌های امنیتی بدون درک اثرات منفی این کار بر مأموریت‌ها و فرایندهای کسب‌وکار، می‌تواند مخاطرات امنیتی سیستم را تا حد زیادی افزایش دهد. به همین دلیل، لازم است که تحلیل‌های کافی پیش از حذف کنترل‌های امنیتی صورت گیرند. این تحلیل‌ها برای اتخاذ تصمیمات مناسب در زمینه مخاطرات (مانند انتخاب کنترل‌های جبرانی مناسب در هنگام استفاده از فناوری‌ها و دستگاه‌های همراه نوظهور)، ضروری هستند. تعیین و تبیین دقیق طرح‌های امنیتی با استفاده از پوشش‌ها و راهنمایی‌های اصلاحی، و همچنین استفاده از مجموعه جامعی از کنترل‌های امنیتی مستقل از فناوری و خط‌مشی، سبب توسعه طرح‌های مقرون به صرفه و مخاطره‌محور در زمینه امنیت اطلاعات می‌شود. این طرح‌ها را می‌توان در هر بخش، برای هر فناوری، و در هر محیط عملیاتی توسعه داد.

انتظار می‌رود که کنترل‌های امنیتی مورد اشاره در این کاتالوگ، به مرور زمان یا با کنار گذاشته شدن، بازبینی و اضافه شدن کنترل‌ها، تغییر کنند. به منظور حفظ ثبات و پایداری طرح‌های امنیتی و ابزارهای خودکارسازی تشریح‌شده در NIST 800-53، کنترل‌های امنیتی پس از کنار گذاشته شدن یک یا چند مورد از کنترل‌ها، مجددا شماره‌گذاری نمی‌شوند و شماره‌های پیشین خود را حفظ می‌کنند. حتی شماره و مشخصات کنترل‌های

حذف‌شده نیز به منظور حفظ سوابق، نگهداری می‌شوند. کنترل‌های امنیتی ممکن است به دلایل مختلف کنار گذاشته شوند. به عنوان مثال، قابلیت امنیتی یک کنترل ممکن است در قالب یک کنترل امنیتی دیگر ارائه شود، قابلیت امنیتی یک کنترل ممکن است دیگر مورد نیاز نباشد، یا این که ممکن است دیگر نیازی به استفاده از یک کنترل امنیتی نباشد.

در برخی موارد ممکن است تکرارهایی در الزامات مربوط به کنترل‌های امنیتی یا کنترل‌های پیشرفته این کاتالوگ وجود داشته باشد. این تکرارها به منظور تأکید بر الزامات امنیتی از چشم‌انداز چند کنترل امنیتی یا کنترل پیشرفته مختلف است. به عنوان مثال، الزام استفاده از روش‌های قدرتمند برای شناسایی و احراز هویت در هنگام انجام فعالیت‌های از راه دور، در خانوده MA در حیطه خاص تعمیر و نگهداری سیستم‌های سازمانی تشریح شده است. اما این الزامات در خانواده عمومی‌تر IA نیز مطرح شده‌اند. هر چند ممکن است این الزامات تکراری و غیر ضروری به نظر برسند، اما در واقع یکدیگر را تأیید می‌کنند و سازمان‌ها هم نیازی به انجام فعالیت‌های جدید برای رعایت آن‌ها ندارند.

نکاتی برای پیاده‌سازی بهتر

کنترل‌های امنیتی و کنترل‌های پیشرفته جدید، به صورت پیوسته و با استفاده از اطلاعات کاربردی به دست آمده در زمینه آسیب‌پذیری‌ها و تهدیدات ملی، و همچین بر اساس اطلاعات مربوط به تدابیر، شیوه‌ها و رویه‌های مهاجمان، توسعه داده می‌شوند. در فرایندهای بازبینی، تغییرات پیشنهادی در کنترل‌های امنیتی و مجموعه‌های اولیه، با هدف افزایش ثبات کاتالوگ کنترل‌های امنیتی و با توجه به فناوری‌های اطلاعاتی، روش‌های حمله، آسیب‌پذیری‌ها و تهدیدات جدید، به دقت سنجیده می‌شوند. هدف کلی این فرایند، افزایش سطح امنیت اطلاعات به مرور زمان است. در صورتی که به یک قابلیت امنیتی خاص نیاز باشد که در کنترل‌های امنیتی موجود در پیوست‌های ج و چ پوشش داده نشده است، سازمان‌ها می‌توانند کنترل‌های امنیتی جدیدی را توسعه دهند.

اختصاص کنترل‌های امنیتی به دسته‌های مختلف

ترجیحات مدیریتی، عملیاتی، و فنی

از آن جا که بسیاری از کنترل‌های امنیتی مورد اشاره در خانواده کنترل‌های امنیتی پیوست ج، شامل ترکیبات مختلفی از ویژگی‌های مدیریتی، عملیاتی و فنی هستند، این کنترل‌های امنیتی به دسته خاصی اختصاص داده نشده‌اند. با این حال، سازمان‌ها می‌توانند کنترل‌های امنیتی یا کنترل‌های پیشرفته را به دسته‌های خاصی اختصاص دهند. ممکن است این کار، سازمان‌ها را یاری کند تا کنترل‌های امنیتی را بهتر گروه‌بندی کنند یا به طور مؤثرتری به آن‌ها ارجاع دهند. این کار همچنین می‌تواند سازمان‌ها را کمک کند تا کنترل‌های امنیتی و کنترل‌های پیشرفته را به سیستم‌ها و نقش‌های روبرو اختصاص دهند: (۱) سیستم‌های اطلاعاتی یا طرفین مسئول (مثلا به عنوان کنترل‌های معمول یا کنترل‌های هیبریدی)؛ (۲) نقش‌های خاص؛ و/یا (۳) برخی مؤلفه‌های خاص یک سیستم. به عنوان مثال، ممکن است سازمان‌ها تصمیم بگیرند که مسئولیت کنترل‌های سیستمی که در دسته مدیریتی قرار داده‌اند با مالک سیستم اطلاعاتی است، مسئولیت کنترل‌هایی که در دسته عملیاتی قرار داده‌اند با مدیر امنیت سیستم اطلاعاتی (ISSO) است، و مسئولیت کنترل‌هایی که در دسته فنی قرار داده‌اند با یک یا چند راهبر سیستم است. این مثال صرفا برای نشان دادن مزایای بالقوه اختصاص دادن کنترل‌های امنیتی و کنترل‌های پیشرفته به دسته‌های خاص است، و به معنی پیشنهاد دادن چیزی به سازمان‌ها یا الزام آن‌ها به انجام کاری نیست.

نکته احتیاطی

توسعه سیستم‌ها، مؤلفه‌ها و خدمات

با افزایش تأکید بر لزوم به‌کارگیری سیستم‌های اطلاعاتی امن و ارتقای امنیت در زنجیره تأمین، لازم است که سازمان‌ها الزمات سیستم‌های اطلاعاتی خود را با وضوح و دقت تشریح کنند تا بتوانند ارتباط مناسب را با صنعت فناوری اطلاعات برقرار نمایند و سیستم‌ها، مؤلفه‌ها و خدمات مورد نیاز برای انجام موفقیت‌آمیز مأموریت‌ها و فرایندهای کسب‌وکار خود را فراهم آورند. برای حصول اطمینان از وجود این قابلیت در سازمان‌ها، سند NIST 800-53 مجموعه‌ای از کنترل‌های امنیتی را در قالب خانواده اکتساب خدمات و سیستم‌ها (یعنی خانواده SA) گردآوری کرده است. این خانواده، الزامات مربوط به توسعه سیستم‌های اطلاعاتی، محصولات فناوری اطلاعات، و خدمات سیستم‌های اطلاعاتی را شرح می‌دهد. بنابراین، بسیاری از کنترل‌های مورد اشاره در خانواده SA در

واقع برای توسعه‌دهندگان این سیستم‌ها، مؤلفه‌ها و خدمات ارائه شده‌اند. سازمان‌ها باید توجه داشته باشند که دامنه شمول کنترل‌های امنیتی خانواده SA شامل توسعه تمام سیستم‌ها، مؤلفه‌ها و خدمات، و تمامی توسعه‌دهندگان مربوطه است، خواه این توسعه‌دهندگان جزو کارکنان سازمان یا افرادی خارج از سازمان باشند. کنترل‌های مربوطه عبارتند از SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20 و SA-21.

کلیات این کاتالوگ

کنترل‌های امنیتی و کنترل‌های پیشرفته مورد اشاره در پیوست‌های ج و چ، به طور کلی مستقل از خط‌مشی و فناوری هستند. سازمان‌ها به دو شکل می‌توانند اطلاعاتی را درباره کنترل‌های امنیتی و کنترل‌های پیشرفته ارائه نمایند:

- تشریح دقیق نحوه پیاده‌سازی کنترل‌های امنیتی (مثلا مسائل مربوط به پلت‌فرم مورد استفاده) در طرح امنیتی سیستم اطلاعاتی یا طرح برنامه امنیتی سازمان؛ و
- تعیین مقادیر برای متغیرهای مختلف کنترل‌های امنیتی در عبارت‌های انتخاب و اختصاص.

عبارت‌های انتخاب و اختصاص، این امکان را به سازمان می‌دهند تا کنترل‌های امنیتی و کنترل‌های پیشرفته را بر اساس الزامات امنیتی خود یا الزامات نشأت‌گرفته از دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال، تعدیل و شخصی‌سازی کند. مقادیری که توسط سازمان برای پارامترهای مختلف در عبارت‌های انتخاب و اختصاص در نظر گرفته می‌شوند، در تمام کنترل‌های پیشرفته مربوط به کنترل امنیتی مورد نظر نیز اعمال خواهند شد. کنترل‌های پیشرفته، قابلیت‌های امنیتی کنترل اصلی را تقویت می‌کنند، اما نمی‌توانند جایگزین عبارت‌های اختصاص و انتخاب شوند. عبارت‌های اختصاص کنترل‌های امنیتی و کنترل‌های پیشرفته، شامل مقادیر حداقل و حداکثر نیستند (مثلا آزمون کردن طرح‌های آمادگی برای رویدادهای آینده، *حداقل سالی یک بار*). سازمان‌ها باید چنین اطلاعاتی را از دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال به دست آورند. وجود نداشتن مقادیر حداقل و حداکثر در کنترل‌های امنیتی و کنترل‌های پیشرفته، به معنی عدم نیاز به رعایت الزامات تشریح‌شده در اسناد کنترلی اصلی نیست.

نخستین کنترل امنیتی هر خانواده (یعنی کنترلی که با شماره ۱ مشخص شده است)، در بر دارنده الزامات مربوط به رویه‌ها و خط‌مشی‌های خاصی است که برای پیاده‌سازی مؤثر سایر کنترل‌های امنیتی آن خانواده ضروری هستند. بنابراین، نیازی نیست که همه کنترل‌های امنیتی و کنترل‌های پیشرفته به این رویه‌ها و خط‌مشی‌ها اشاره نمایند. بخش راهنمایی‌های تکمیلی کنترل‌های امنیتی و کنترل‌های پیشرفته، در بر دارنده هیچ الزامی نیستند و به اسناد FIPS و NIST نیز ارجاع نمی‌دهند. اما اسناد NIST، در بخش «مراجع» هر کنترل امنیتی آمده‌اند.

برای پشتیبانی از پروژه کارگروه مشترک[۱۴۷] و به منظور توسعه یک چارچوب یکپارچه برای سیستم‌های اطلاعات دولت فدرال، کنترل‌های امنیتی و کنترل‌های پیشرفته سیستم‌های اطلاعاتی ملی نیز در این پیوست آمده‌اند. گنجانده شدن این کنترل‌های امنیتی و کنترل‌های پیشرفته، الزامی را برای سازمان‌هایی که از سیستم‌های اطلاعاتی ملی استفاده می‌کنند، ایجاد نمی‌نماید. سازمان‌ها می‌توانند در صورت تأیید مقامات فدرال، به صورت داوطلبانه از این کنترل‌های امنیتی و کنترل‌های پیشرفته استفاده کنند. علاوه بر این، اولویت‌بندی‌ها و مجموعه‌های اولیه کنترل‌های امنیتی تشریح‌شده در پیوست ت و پیوست ج، در مورد تمام سیستم‌های امنیتی غیر ملی نیز اعمال می‌شوند، مگر این که مقامات فدرال ذی‌صلاح به گونه‌ای دیگر تصمیم‌گیری کرده باشند.

استفاده از کاتالوگ

سازمان‌ها، کنترل‌های امنیتی[۱۴۸] و سیستم‌های اطلاعاتی فدرال و محیط‌های عملیاتی آن‌ها را بر اساس FIPS 199، FIPS 200، NIST 800-37 و NIST 800-39 به کار می‌گیرند. بر اساس FIPS 199، دسته‌بندی امنیتی اطلاعات و سیستم‌های اطلاعاتی فدرال، نخستین گام فرایند RMF به شمار می‌آید[۱۴۹]. در ادامه، سازمان‌ها مجموعه اولیه کنترل‌های امنیتی خود را بر اساس الزامات تشریح‌شده در FIPS 200 انتخاب می‌کنند. پیوست ت، سه مجموعه اولیه کنترل‌های امنیتی و سطح تأثیر سیستم‌های اطلاعاتی مربوطه را، چنان که در فرایند دسته‌بندی امنیتی گفته شده است، تشریح می‌کند[۱۵۰]. پس از انتخاب مجموعه اولیه کنترل‌های امنیتی،

---

[147] joint task force

[۱۴۸] کنترل‌های امنیتی **مورد اشاره در** NIST 800-53 به صورت آنلاین نیز موجود هستند و می‌**توان** آن‌ها را در فرمت‌های مختلف، از این آدرس اینترنتی دانلود نمود: http://web.nvd.nist.gov/view/800-53/home

[۱۴۹] **سند** CNSS 1253، راهنمایی‌هایی را در زمینه «دسته‌بندی امنیتی» سیستم‌های امنیت ملی ارائه می‌کند.

[۱۵۰] **سند** CNSS 1253، راهنمایی‌هایی را در زمینه «مجموعه‌های اولیه کنترل‌های امنیتی» سیستم‌های امنیت ملی، و الزامات مربوط به این سیستم‌ها را ارائه می‌کند.

سازمان‌ها به ترتیب روبرو اقدام به تعدیل و اصلاح آن‌ها می‌نمایند: (۱) شناسایی و تخصیص کنترل‌های معمول؛ (۲) اعمال ملاحظات در نظر گرفته شده؛ (۳) انتخاب کنترل‌های جبرانی در صورت نیاز؛ (۴) تعیین مقادیر پارامترها در عبارات انتخاب و اختصاص؛ (۵) تکمیل مجموعه‌های اولیه کنترل‌های امنیتی با استفاده از کنترل‌های امنیتی و کنترل‌های پیشرفته مورد اشاره در کاتالوگ کنترل‌های امنیتی؛ و (۶) ارائه اطلاعات تکمیلی برای پیاده‌سازی کنترل‌ها. سازمان‌ها همچنین می‌توانند از فرایندهای اصلاحی اولیه و مفهوم پوشش استفاده کنند که در بخش ۳,۲ و پیوست خ شماره ویژه ۳۰-۸۰۰ تشریح شده است. بدین ترتیب، سازمان‌ها می‌توانند فرایند انتخاب کنترل‌های امنیتی را به نحو بهتری اجرا کنند[۱۵۱].

نکته احتیاطی

استفاده از رمزنگاری

در صورتی که بر اساس انتخاب کنترل‌های امنیتی در پیوست ج، تشخیص داده شود که برای حفاظت از اطلاعات باید آن‌ها را رمزگذاری نمود، و این کار توسط سیستم‌های اطلاعاتی سازمان انجام شود، سازوکارهای رمزنگاری مورد استفاده باید متناسب با دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال باشند. روش‌های مورد استفاده شامل روش‌های رمزنگاری مورد تأیید NSA برای حفاظت از اطلاعات محرمانه، روش‌های رمزنگاری مورد تأیید FIPS برای حفاظت از اطلاعات غیر محرمانه، و فرایندها و فناوری‌های مدیریتی مورد تأیید NSA و FIPS است. کنترل‌های امنیتی SC-12 و SC-13، اطلاعات ویژه‌ای را در مورد سازوکارهای رمزنگاری مناسب ارائه می‌کنند و قدرت این سازوکارها را بیان می‌نمایند.

[۱۵۱] کنترل‌های امنیتی و کنترل‌های پیشرفته دیگری نیز در کاتالوگ هستند که در مجموعه‌های اولیه مورد استفاده قرار نگرفته‌اند. این کنترل‌های امنیتی و کنترل‌های پیشرفته در اختیار سازمان‌ها قرار دارند و می‌**توان با استفاده از آن‌**ها در فرایندهای اصلاحی، به سطح حفاظتی مورد نیاز بر اساس بررسی مخاطرات سازمانی دست یافت.

خانواده: کنترل دسترسی

AC-1: خط‌مشی و رویه‌های کنترل دسترسی

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۱. خط‌مشی شناسایی و احراز هویت شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و
۲. رویه‌های تسهیل پیاده‌سازی خط‌مشی شناسایی و احراز هویت و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۱. خط‌مشی شناسایی و احراز هویت؛ و
۲. رویه‌های شناسایی و احراز هویت.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده IA را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: شماره‌های ویژه NIST 800-12, 800-100.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AC-1 اولویت پایین	AC-1 اولویت متوسط	AC-1 اولویت بالا

AC-2: مدیریت حساب کاربری

کنترل: سازمان:

الف. انواع مختلف حساب‌های کاربری سیستم‌های اطلاعاتی را به منظور پشتیبانی از فرایندهای کسب‌وکار سازمان، شناسایی و انتخاب می‌کند: [اختصاص: انواع حساب‌های کاربری سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان]؛

ب. مدیران حساب‌های کاربری را برای مدیریت حساب‌های کاربری سیستم‌های اطلاعاتی منصوب می‌نماید؛

پ. شرایط مربوط به عضویت در گروه‌ها و نقش‌ها را تعیین می‌کند؛

ت. کاربران مجاز سیستم اطلاعاتی، عضویت در گروه و نقش، مجوز دسترسی (یعنی امتیازات ویژه) و سایر ویژگی‌ها را (در صورت نیاز) برای هر یک از حساب‌های کاربری مشخص می‌کند؛

ث. در صورت درخواست افراد برای ایجاد یک حساب کاربری در سیستم‌های اطلاعاتی، از آن‌ها می‌خواهد که مجوز [اختصاص: کارکنان و نقش‌های تعیین‌شده توسط سازمان] را ارائه کنند؛

ج. حساب‌های کاربری سیستم‌های اطلاعاتی را بر اساس [شرایط و رویه‌های تعیین‌شده توسط سازمان] ایجاد، فعال، اصلاح، غیر فعال، و حذف می‌کند؛

چ. نحوه استفاده از حساب‌های کاربری سیستم‌های اطلاعاتی را پایش می‌کند؛

ح. موارد زیر را به مدیران حساب‌های کاربری اطلاع می‌دهد:

۱. هنگامی که دیگر به حساب‌ها نیازی نباشد

۲. هنگامی که مجوز کاربران به پایان رسیده یا منتقل شده باشد

۳. هنگامی که کاربرد یا اطلاعات مربوط به سیستم‌های اطلاعاتی تغییر کنند

خ. مجوز دسترسی به سیستم‌های اطلاعاتی را بر اساس موارد زیر صادر می‌نماید:

۱. مجوز دسترسی معتبر

۲. استفاده صحیح و هدفمند از سیستم

۳. ویژگی‌های دیگر تعیین‌شده توسط سازمان یا مبتنی بر مأموریت‌ها و فرایندهای کسب‌وکار

د. حساب‌های کاربری را بازبینی می‌کند تا اطمینان حاصل نماید که مطابق الزامات مدیریتی [اختصاص: در بازه زمانی تعیین‌شده توسط سازمان] هستند؛

ذ. هنگامی که برخی افراد از گروه کنار بروند، فرایندی را برای صدور مجدد اطلاعات حساب‌های کاربری مشترک ایجاد می‌نماید.

راهنمایی‌های تکمیلی: حساب‌های کاربری سیستم‌های اطلاعاتی، انواع مختلفی از جمله شخصی، مشترک، گروهی، سیستمی، مهمان / ناشناس، اضطراری، توسعه‌دهنده / تولیدکننده / فروشنده، موقتی، و خدماتی را شامل می‌شوند. برخی از الزامات مدیریتی حساب‌های کاربری که در بالا لیست شده‌اند، توسط سیستم‌های اطلاعاتی سازمان قابل پیاده‌سازی هستند. شناسایی کاربران مجاز سیستم‌های اطلاعاتی و تعیین امتیازات ویژه دسترسی، بر اساس الزامات مورد اشاره در این کنترل امنیتی و سایر کنترل‌های موجود در طرح امنیتی صورت می‌گیرد. کاربراتی که به امتیازات ویژه راهبری در حساب‌های کاربری سیستم‌های اطلاعاتی نیاز دارند، ابزارهای حفاظتی اضافه‌ای را نیز از کارکنان مربوطه (مانند مالک سیستم، مالک مأموریت و کسب‌وکار، یا مدیر ارشد امنیت اطلاعات) دریافت می‌کنند. سازمان‌ها می‌توانند امتیازات ویژ دسترسی و سایر ویژگی‌ها را بر اساس حساب کاربری، نوع حساب، یا ترکیبی از هر دو مورد تعیین نمایند. سایر ویژگی‌های مورد نیاز برای دسترسی، مواردی از جمله محدودیت ساعت در روز، روز در هفته، و نقطه مبدأ را شامل می‌شوند. برای تعیین این ویژگی‌ها، سازمان‌ها به مواردی از جمله الزامات سیستم (مانند برنامه زمان‌بندی تعمیر و نگهداری، و به‌روزرسانی‌های سیستم)، و الزامات مربوط به مأموریت‌ها و فرایندهای کسب‌وکار (مانند تفاوت‌های زمانی، الزامات مشتری، و الزامات دسترسی از راه دور) توجه می‌کنند. عدم توجه به این موارد، می‌تواند سبب از دسترس خارج شدن سیستم‌های اطلاعاتی گردد. حساب‌های موقتی و اضطراری، حساب‌هایی هستند که برای استفاده کوتاه‌مدت در نظر گرفته شده‌اند. هنگامی که نیاز به حساب‌های کوتاه‌مدت بدون فعال‌سازی آنی باشد، سازمان‌ها از حساب‌های موقتی برای فعال‌سازی حساب‌های کوتاه‌مدت مذکور استفاده می‌کنند. حساب‌های اضطراری نیز در مواقع بحران

و در صورت نیاز به فعال‌سازی سریع مورد استفاده قرار می‌گیرند. بنابراین، فعال‌سازی حساب‌های اضطراری ممکن است مقدم بر صدور مجوز حساب‌های معمولی باشد. حساب‌های موقتی و اضطراری را نباید با حساب‌هایی که به صورت محدود به کار گرفته می‌شوند (مانند حساب‌های ورود محلی مورد استفاده برای وظایف خاص تعیین‌شده توسط سازمان، یا مورد استفاده در شرایطی که منابع شبکه از دسترس خارج شده‌اند)، اشتباه گرفت. این حساب‌ها فعال باقی می‌مانند و شامل غیر فعال شدن خودکار یا انقضای تاریخ استفاده نمی‌شوند. شرایط غیر فعال شدن حساب‌ها، مواردی از این دست را شامل می‌گردند: (الف) در صورتی که دیگر نیازی به حساب‌های مشترک، گروهی، اضطراری یا موقتی نباشد؛ (ب) هنگامی که برخی افراد کنار رفته یا منتقل شده باشند. ممکن است برای استفاده از برخی حساب‌های کاربری سیستم‌های اطلاعاتی، نیاز به آموزش وجود داشته باشد. کنترل‌های مربوطه: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

کنترل‌های پیشرفته:

(۱) مدیریت حساب کاربری / مدیریت خودکار حساب‌های سیستم

سازمان، سازوکارهای خودکار را برای پشتیبانی از مدیریت حساب‌های سیستم اطلاعاتی، مورد استفاده قرار می‌دهد.

راهنمایی‌های تکمیلی: استفاده از سازوکارهای خودکار، مواردی از این دست را در بر می‌گیرد: استفاده از ایمیل یا پیام کوتاه متنی برای اطلاع‌رسانی خودکار به مدیران حساب‌ها در هنگامی که برخی افراد کنار رفته یا منتقل شده باشند؛ استفاده از سیستم اطلاعاتی برای پایش نحوه استفاده از حساب؛ و استفاده از اطلاع‌رسانی تلفنی برای گزارش دادن موارد غیر معمول استفاده از حسب‌ها.

(۲) مدیریت حساب کاربری / حساب‌های اضطراری

سیستم اطلاعاتی، حساب‌های اضطراری و موقتی را به طور خودکار پس از [اختصاص: زمان تعیین‌شده توسط سازمان برای هر حساب]، [انتخاب: غیر فعال می‌کند، حذف می‌کند].

راهنمایی‌های تکمیلی: این کنترل پیشرفته، لازم می‌دارد که پس از اتمام یک مدت زمان از پیش تعریف شده (و نه به صلاحدید راهبر سیستم)، حساب‌های اضطراری و موقتی به طور خودکار حذف شوند.

(۳) مدیریت حساب کاربری / غیر فعال کردن حساب‌های بلااستفاده

سیستم اطلاعاتی، حساب‌های بلااستفاده را به طور خودکار پس از [اختصاص: زمان تعیین‌شده توسط سازمان برای هر حساب] غیر فعال می‌کند.

(۴) مدیریت حساب کاربری / اقدامات ممیزی خودکار

سیستم اطلاعاتی، فرایند ممیزی را به طور خودکار در مورد ایجاد، تغییر، فعال‌سازی، غیرفعال‌سازی، و حذف حساب‌های کاربری انجام می‌دهد و مراتب را به [اختصاص: نقش‌ها و کارکنان تعیین‌شده توسط سازمان] اطلاع‌رسانی می‌کند.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: AU-2, AU-12.

(۵) مدیریت حساب کاربری / خارج شدن در صورت عدم فعالیت

سازمان از کاربران می‌خواهد تا در صورت [اختصاص: سپری شدن مدت زمان عدم فعالیت یا برقرار بودن شرایط خروج تعیین‌شده توسط سازمان]، از سیستم خارج شوند.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: SC-23.

(۶) مدیریت حساب کاربری / مدیریت پویای امتیازات ویژه

سیستم اطلاعاتی، این قابلیت‌های مدیریت پویای امتیازات ویژه را به اجرا در می‌آورد: [اختصاص: لیست قابلیت‌های مدیریت پویای امتیازات ویژه تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: بر خلاف رویکرد دسترسی مرسوم که در آن از حساب‌های استاتیک سیستم اطلاعاتی و مجموعه از پیش تعیین شده‌ای از امتیازات ویژه کاربری استفاده می‌شود، رویکردهای کنترل دسترسی پویا (مانند معماری‌های خدمت‌محور) مبتنی بر کنترل دسترسی زمان اجرا و مدیریت پویای امتیازات هستند. در حالی که هویت کاربران ممکن است برای مدتی نسبتا طولانی ثابت بمانند، امتیازات ویژه کاربری تغییرات سریع‌تری را بر اساس الزامات مأموریت و فرایندهای کسب‌وکار، و نیازهای عملیاتی سازمان تجربه می‌کنند. مدیریت پویای امتیازات ویژه، مواردی از جمله فسخ آنی امتیازات ویژه کاربران را شامل می‌شود (در مقابل رویکردی که در آن از کاربر خواسته می‌شود تا نشست خود را به اتمام برساند و مجددا آغاز کند تا تغییرات در امتیازات ویژه اعمال شوند). مدیریت پویای امتیازات ویژه همچنین می‌تواند به سازوکارهایی گفته شود که امتیازات ویژه کاربران را بر اساس قوانین پویا تغییر می‌دهند (در مقابل رویکردهایی که در آن‌ها، این امتیازات بر اساس ویرایش پروفایل کاربران تغییر داده می‌شوند). این نوع از مدیریت امتیازات ویژه، مواردی از جمله تغییر خودکار امتیازات ویژه در صورت فعالیت کاربران در خارج از ساعات کاری عادی خود، و یا کار کردن سیستم‌های اطلاعاتی تحت فشار یا در شرایط تعمیر و نگهداری اضطراری را شامل می‌شود. این کنترل پیشرفته همچنین اثرات

فرعی تغییر امتیازات ویژه را شامل می‌شود. به عنوان مثال، می‌توان به تغییرات بالقوه در کلیدهای رمزنگاری مورد استفاده برای برقراری ارتباطات اشاره کرد. مدیریت پویای امتیازات ویژه می‌تواند از الزامات مربوط به انعطاف سیستم‌های اطلاعاتی نیز پشتیبانی نماید. کنترل مربوطه: AC-16.

(۷) مدیریت حساب کاربری / الگوهای مبتنی بر نقش

سازمان:

(الف) حساب‌های کاربری دارای امتیازات ویژه را بر اساس الگوهای دسترسی نقش‌محوری ایجاد و راهبری می‌کند که امتیازات ویژه و دسترسی مجاز به سیستم‌های اطلاعاتی را سازماندهی می‌کنند؛

(ب) فرایند اختصاص نقش‌های دارای امتیازات ویژه را پایش می‌کند؛ و

(پ) هنگامی که این نقش‌های دارای امتیازات ویژه دیگر صحیح نباشند، [اختصاص: اقدامات تعیین‌شده توسط سازمان] را انجام می‌دهد.

راهنمایی‌های تکمیلی: نقش‌های دارای امتیازات ویژه، نقش‌هایی هستند که به افراد اختصاص داده شده‌اند و به آن‌ها اجازه می‌دهند تا اقدامات امنیتی خاصی را انجام دهند (اقداماتی که توسط افراد عادی قابل انجام نیستند). این نقش‌های دارای امتیازات ویژه، مواردی از جمله مدیریت کلید، مدیریت حساب کاربری، راهبری سیستم و شبکه، راهبری پایگاه داده، و راهبری وب را در بر می‌گیرند.

(۸) مدیریت حساب کاربری / ایجاد حساب‌های کاربری به صورت پویا

سیستم اطلاعاتی، [اختصاص: حساب‌های کاربری سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] را به صورت پویا ایجاد می‌کند.

راهنمایی‌های تکمیلی: در رویکردهای پویا برای ایجاد حساب‌های کاربری سیستم‌های اطلاعاتی (مانند آن چه در معماری‌های خدمت‌محور مشاهده می‌شود)، حساب‌های کاربری (هویت‌ها) در زمان اجرا برای موجودیت‌های پیشتر ناشناخته، ایجاد می‌شوند. سازمان‌ها برای ایجاد حساب‌های کاربری سیستم‌های اطلاعاتی، سازوکارها و روابط مبتنی بر اعتمادی را با مقامات مربوطه برقرار می‌کنند تا مجوزها و امتیازات ویژه را تأیید نمایند. کنترل مربوطه: AC-16.

(۹) مدیریت حساب کاربری / محدودیت‌های استفاده از حساب‌های مشترک و گروهی

سازمان تنها اجازه استفاده از آن دسته از حساب‌های گروهی و مشترک را صادر می‌نماید که مطابق با [اختصاص: شرایط تعیین‌شده توسط سازمان برای ایجاد حساب‌های مشترک و گروهی] باشند.

(۱۰) مدیریت حساب کاربری / ابطال اطلاعات حساب‌های مشترک و گروهی

هنگامی که برخی از افراد گروه را ترک کنند، سیستم اطلاعاتی اقدام به ابطال اطلاعات کاربری حساب‌های مشترک و گروهی می‌نماید.

(۱۱) مدیریت حساب کاربری / شرایط استفاده

سیستم اطلاعاتی، [اختصاص: شرایط و/یا نحوه استفاده تعیین‌شده توسط سازمان] را برای [اختصاص: حساب‌های سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] به اجرا در می‌آورد.

راهنمایی‌های تکمیلی: سازمان‌ها می‌توانند شرایط خاصی را برای استفاده از حساب‌های سیستم‌های اطلاعاتی تعیین کنند. به عنوان مثال، می‌توان به محدودیت استفاده در روزهای خاصی از هفته، زمان‌های خاصی از روز، یا محدوده‌های زمانی خاص اشاره کرد.

(۱۲) مدیریت حساب کاربری / پایش حساب‌های کاربری و استفاده‌های غیر معمول

سازمان:

(الف) حساب‌های سیستم‌های اطلاعاتی را پایش می‌کند تا موارد [اختصاص: استفاده‌های غیر معمول تعیین‌شده توسط سازمان] را مشخص نماید؛

(ب) استفاده‌های غیر معمول از حساب‌های سیستم‌های اطلاعاتی را به [اختصاص: کارکنان و نقش‌های تعیین‌شده توسط سازمان] گزارش می‌دهد.

راهنمایی‌های تکمیلی: به عنوان مثالی از استفاده‌های غیر معمول، می‌توان به دسترسی به سیستم‌های اطلاعاتی در ساعات یا از مکان‌هایی اشاره کرد که با الگوی استفاده معمول افراد متناسب نیست. کنترل مربوطه: CA-7.

(۱۳) مدیریت حساب کاربری / غیر فعال کردن حساب‌ها برای افرادی با سطح مخاطره بالا

سازمان، حساب‌های کاربرانی که سطح بالایی از مخاطره را موجب می‌شوند را، در بازه زمانی [اختصاص: مدت زمان تعیین‌شده توسط سازمان] پس از شناسایی مخاطره، غیر فعال می‌نماید.

راهنمایی‌های تکمیلی: افرادی که سطح بالایی از مخاطره را برای سازمان موجب می‌شوند، شامل افرادی هستند که اطلاعات یا شواهد معتبری بر علیه آن‌ها وجود دارد که نشان می‌دهد قصد ایجاد خسارت برای سازمان را داشته‌اند یا این که متخاصمان می‌توانند از طریق آن‌ها، خسارت‌هایی را موجب شوند. منظور از خسارت، اثرات نامطلوب بالقوه بر سرمایه‌های و عملیات سازمان، افراد، سایر سازمان‌ها، و کشور است. همکاری نزدیک بین مقامات مسئول، راهبران سیستم‌های اطلاعاتی، و مدیران منابع انسانی، برای اجرای به‌هنگام این کنترل پیشرفته لازم است. کنترل مربوطه: PS-4.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AC-2 اولویت پایین	AC-2(1)(2)(3)(4) اولویت متوسط	AC-2(1)(2)(3)(4)(5)(11)(12)(13) اولویت بالا	

AC-3: **تحقق دسترسی**

کنترل: سیستم اطلاعاتی، مجوز دسترسی منطقی به منابع سیستم و اطلاعات را بر اساس خط‌مشی‌های کنترلی مربوطه، تأیید می‌کند.

راهنمایی‌های تکمیلی: خط‌مشی‌های کنترل دسترسی (مانند خط‌مشی‌های هویت‌محور، خط‌مشی‌های مبتنی بر نقش، ماتریس‌های کنترل، و رمزنگاری)، دسترسی بین عاملین یا موجودیت‌های فعال (یعنی کاربران یا فرایندهایی که از سوی آن‌ها عمل می‌کنند) و موضوعات یا موجودیت‌های غیر فعال (یعنی دستگاه‌ها، فایل‌ها، سوابق، دامنه‌ها) در سیستم اطلاعاتی را کنترل می‌کنند. علاوه بر تحقق دسترسی مجاز در سطح سیستم اطلاعاتی و توانایی سیستم‌های اطلاعاتی برای میزبانی خدمات و برنامه‌های کاربردی متعدد در پشتیبانی از مأموریت‌ها و فرایندهای کسب‌وکار سازمان، سازوکارهای تحقق دسترسی را می‌توان در سطح خدمت یا برنامه کاربردی نیز برای ارتقای امنیت اطلاعات، مورد استفاده قرار داد. کنترل‌های مربوطه: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.

کنترل‌های پیشرفته:

(۱) تحقق دسترسی / دسترسی محدود به توابع دارای امتیازات ویژه
[حذف شد: به بخش AC-6 منتقل شد].

(۲) تحقق دسترسی / مجوز دوگانه

سیستم اطلاعاتی، از سیستم مججوز دوگانه برای [اختصاص: دستورات ویژه تعیین‌شده توسط سازمان یا سایر اقدامات تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: در سازوکارهای مبتنی بر مجوز دوگانه، لازم است که دو فرد مجاز، دستوری را تأیید کنند تا دستور مذکور به اجرا در آید. در صورتی که نیاز به واکنش سریع و آنی باشد، سازمان‌ها از

سازوکارهای مبتنی بر مجوز دوگانه استفاده نمی‌کنند. مجوز دوگانه گاهی به نام کنترل دونفره نیز شناخته می‌شود. کنترل‌های مربوطه: CP-9, MP-6.

(۳) تحقق دسترسی / کنترل دسترسی اجباری

هنگامی که شرایط زیر برقرار باشند، سیستم اطلاعاتی [اختصاص: خط‌مشی کنترل دسترسی اجباری تعیین‌شده توسط سازمان] را بر همه عاملین و موضوعات ارجحیت می‌دهد:

(الف) خط مشی مورد نظر در محدوده مرزهای سیستم اطلاعاتی، به طور یکنواخت بین تمام عاملین[۱۵۲] و موضوعات[۱۵۳] توزیع شده و لازم‌الاجرا باشد؛

(ب) خط‌مشی مورد نظر، بیان دارد که عاملی با دسترسی عمومی به اطلاعات، از انجام موارد زیر منع شده است:

۱. انتقال اطلاعات به عاملین یا موضوعات غیرمجاز؛

۲. اعطای امتیازات ویژه خود به سایر عاملین؛

۳. تغییر یک یا چند ویژگی امنیتی عاملین، موضوعات، سیستم اطلاعاتی، یا مؤلفه‌های سیستم اطلاعاتی؛

۴. انتخاب ویژگی‌های امنیتی و مقادیر مربوطه بر اساس تغییراتی که اخیرا در موضوعات صورت گرفته است؛ و

۵. تغییر قوانین حاکم بر کنترل دسترسی.

(پ) خط‌مشی مورد نظر، بیان دارد که [اختصاص: امتیازات ویژه تعیین‌شده توسط سازمان (بدین معنی که عاملین مورد نظر، عاملین مورد اعتمادی هستند)] به [اختصاص: عاملین تعیین‌شده توسط سازمان] اعطا شود و محدودیت‌های فوق در مورد آن‌ها اعمال نشود.

راهنمایی‌های تکمیلی: کنترل دسترسی اجباری در این کنترل پیشرفته، معادل کنترل دسترسی غیر احتیاطی است و تنها محدود به برخی کاربران خاص نمی‌شود (مثلا پیاده‌سازی با استفاده از مدل Bell-LaPadula). دسته فوق از خط‌مشی‌های کنترل دسترسی اجباری، اقداماتی را که عاملین می‌توانند با استفاده از اطلاعات انجام دهند، محدود می‌کند و بنابراین، آن‌ها را از انتقال اطلاعات به عاملین و موضوعات غیر مجاز منع می‌کند. این کنترل‌ها همچنین اقداماتی که عاملین در زمینه امتیازات ویژه می‌توانند انجام دهند را نیز محدود می‌کنند؛ بدین معنی که عاملی با امتیازات ویژه، نمی‌تواند این

[152] subjects
[153] objects

امتیازات را به عاملین دیگر منتقل کند. این خط‌مشی به طور یکسان در مورد تمام عاملین و موضوعاتی که سیستم اطلاعاتی روی آن‌ها کنترل دارد، اجرا می‌شود. در غیر این صورت، خط‌مشی کنترل امنیتی قابل دور زدن خواهد بود. این فرایند اجرا معمولا مبتنی بر یک سازوکار سازگار با مفهوم پیش مرجع است (AC-25 را ملاحظه کنید). این خط‌مشی در محدوده مرزهای سیستم اطلاعاتی اجرا می‌شود (یعنی به محض این که اطلاعات از مرزهای سیستم خارج شوند، باید ابزارهای دیگری را به کار گرفت تا از تحقق محدودیت‌های مذکور اطمینان حاصل شود). به عاملین مورد اعتماد فوق، امتیازاتی بر اساس اصل حداقل بودن اختیارات اعطا می‌شود (AC-6 را ملاحظه کنید). تنها امتیازاتی در اختیار عاملین مورد اعتماد قرار می‌گیرد که آن‌ها را در برآورده ساختن نیازهای کسب‌وکار و مأموریت‌های سازمان یاری کند. این کنترل به ویژه هنگامی قابل اجرا است که قوانین خاصی (مانند دستورات اجرایی، رهنمودها، قوانین و مقررات) وجود داشته باشند که خط‌مشی‌هایی را در خصوص دسترسی به اطلاعات حساس و محرمانه شکل دهند و برخی از کاربران سیستم اطلاعاتی، اجازه دسترسی به تمام اطلاعات موجود در آن سیستم را نداشته باشند. این کنترل را می‌توان در کنار AC-3(4) مورد استفاده قرار داد. عاملی که محدودیت‌های این کنترل در موردش برقرار است، می‌تواند تحت محدودیت‌های آزادانه‌تر کنترل AC-3(4) نیز فعالیت کند، اما کنترل حاضر بر کنترل AC-3(4) اولویت دارد. به عنوان مثال، هر چند که کنترل حاضر یک عامل را از انتقال اطلاعات به عامل دیگری که با برچسب حساسیت مختلفی کار می‌کند منع می‌نماید، اما کنترل AC-3(4) به یک عامل اجازه می‌دهد تا اطلاعات را به هر عامل دیگری که با همان برچسب حساسیت کار می‌کند، منتقل نماید. کنترل‌های مربوطه: AC-25, SC-11.

(۴) تحقق دسترسی / کنترل دسترسی احتیاطی

در صورتی که خط‌مشی مورد نظر بیان دارد که یک عامل دارای مجوز دسترسی به اطلاعات، می‌تواند یک یا چند مورد از اقدامات زیر را انجام دهد، سیستم اطلاعاتی [اختصاص: خط‌مشی کنترل دسترسی احتیاطی تعیین‌شده توسط سازمان] را به اجرا در می‌آورد:

(الف) انتقال اطلاعات به عاملین یا موضوعات دیگر؛

(ب) اعطای امتیازات ویژه خود به سایر عاملین؛

(پ) تغییر ویژگی‌های امنیتی عاملین، موضوعات، سیستم اطلاعاتی، یا مؤلفه‌های سیستم اطلاعاتی؛

(ت) تغییر قوانین حاکم بر کنترل دسترسی.

راهنمایی‌های تکمیلی: در صورت اجرای خط‌مشی‌های کنترل دسترسی احتیاطی، عاملین محدودیتی در زمینه کار با اطلاعاتی که مجوز دسترسی به آن را دارند، نخواهند داشت. بنابراین، عاملینی که مجوز

دسترسی به اطلاعات را دارند، می‌توانند اطلاعات را سایر عاملین و موضوعات منتقل کنند. این کنترل را می‌توان در کنار AC-3(3) مورد استفاده قرار داد. عاملی که محدودیت‌های این کنترل در موردش برقرار است، می‌تواند تحت محدودیت‌های آزادانه‌تر کنترل AC-3(3) نیز فعالیت کند. بنابراین، در حالی که کنترل AC-3(3) یک عامل را از انتقال اطلاعات به عامل دیگری که با برچسب حساسیت مختلفی کار می‌کند منع می‌نماید، اما کنترل AC-3(4) به یک عامل اجازه می‌دهد تا اطلاعات را به هر عامل دیگری که با همان برچسب حساسیت کار می‌کند، منتقل نماید. این خط‌مشی در محدوده مرزهای سیستم اطلاعاتی اجرا می‌شود؛ یعنی به محض این که اطلاعات از مرزهای سیستم خارج شوند، باید ابزارهای دیگری را به کار گرفت تا از تحقق محدودیت‌های مذکور اطمینان حاصل شود. در حالی که در فرایندهای قدیمی‌تر کنترل دسترسی احتیاطی، مبتنی بر تأیید هویت به منظور دسترسی هستند، محدودیت مذکور در مورد کنترل حاضر صدق نمی‌کند.

(۵) تحقق دسترسی / اطلاعات امنیتی

سیستم اطلاعاتی، مگر در حالت امن و غیر اجرایی بودن سیستم، از دسترسی به [اختصاص: اطلاعات امنیتی تعیین‌شده توسط سازمان] جلوگیری به عمل می‌آورد.

راهنمایی‌های تکمیلی: منظور از اطلاعات امنیتی، هر گونه اطلاعاتی در سیستم‌های اطلاعاتی است که می‌تواند بر عملکرد خدمات و توابع امنیتی تأثیر بگذارد و سبب عدم اجرای خط‌مشی‌های امنیتی سیستم شود یا تفکیک کدها و داده‌ها را با اخلال مواجه سازد. به عنوان نمونه‌هایی از اطلاعات امنیتی، می‌توان به قوانین فیلترینگ مسیریاب‌ها و فایروال‌ها، اطلاعات مدیریت کلید رمزنگاری، پارامترهای پیکربندی خدمات امنیتی، و لیست‌های کنترل دسترسی اشاره کرد. وضعیت امن اما غیر عملیاتی سیستم هنگامی است که سیستم‌های اطلاعاتی، عملکردهای خود در زمینه انجام مأموریت‌ها و فرایندهای کسب‌وکار را انجام نمی‌دهند (مثلا هنگامی که به منظور تعمیر و نگهداری، رفع عیب، یا راه‌اندازی مجدد، خاموش شده است). کنترل مربوطه: CM-3.

(۶) تحقق دسترسی / حفاظت از اطلاعات سیستم و اطلاعات کاربری

[حذف شد: به بخش‌های MP-4 و SC-28 منتقل شد].

(۷) تحقق دسترسی / کنترل دسترسی مبتنی بر نقش

سیستم اطلاعاتی، یک خط‌مشی کنترل دسترسی مبتنی بر نقش را برای موضوعات و عاملین مختلف اجرا می‌کند، و دسترسی را بر اساس [اختصاص: نقش‌ها و کاربرانی که سازمان برای انجام آن نقش‌ها در نظر گرفته است] کنترل می‌نماید.

راهنمایی‌های تکمیلی: کنترل دسترسی مبتنی بر نقش (RBAC)، نوعی خط‌مشی کنترل دسترسی است که دسترسی به سیستم اطلاعاتی را محدود به کاربران مجاز می‌کند. سازمان‌ها می‌توانند بر اساس امتیازات و وظایف شغلی، و به منظور انجام عملیات لازم در سیستم‌های اطلاعاتی سازمانی، نقش‌هایی را بر اساس وظایف و اختیارات شغلی تعیین کنند. هنگامی که نقش‌های سازمانی به کاربران تخصیص داده شوند، اختیارات و امتیازات مربوط به آن نقش‌ها نیز به آن‌ها تفویض خواهد شد. کنترل دسترسی RBAC، مدیریت این امتیازات و اختیارات را برای سازمان ساده‌تر می‌کند؛ زیرا امتیازات و اختیارات به مستقیماً به هر کابر اختصاص داده نشده‌اند، بلکه از طریق نقش‌های سازمانی به آن‌ها تفویض شده‌اند. RBAC را می‌توان به عنوان یک کنترل دسترسی اجباری یا اختیاری پیاده‌سازی نمود. در مورد سازمان‌هایی که RBAC را به همراه کنترل‌های دسترسی اجباری پیاده‌سازی می‌کنند، موضوعات و مسائل مربوطه در الزامات AC-3(3) تشریح شده‌اند.

(۸) تحقق دسترسی / ابطال مجوز دسترسی

در صورتی که تغییر ویژگی‌های امنیتی عوامل یا موجودیت‌های غیر فعال منجر به ابطال مجوزهای دسترسی شود، سیستم اطلاعاتی این موارد ابطال را بر اساس [اختصاص: قوانین تعیین‌شده توسط سازمان درباره زمان‌بندی ابطال مجوزهای دسترسی] به اجرا در می‌آورد.

راهنمایی‌های تکمیلی: قوانین ابطال مجوز دسترسی به نوع دسترسی ابطال‌شده بستگی دارند. به عنوان مثال، اگر یک عامل (یعنی یک کاربر یا فرایند) از گروهی حذف شود، ممکن است دسترسی در همان لحظه ابطال نشود و این اتفاق زمانی رخ دهد که موجویت غیر فعال (مانند فایل) باز شود یا عامل بار دیگر تلاش کند که به موجودیت مذکور دسترسی پیدا نماید. ابطال بر اساس تغییر برچسب‌های امنیتی ممکن است به صورت آنی اعمال شود. در صورتی که اعمال سریع ابطال لازم باشد و سیستم اطلاعاتی چنین قابلیتی نداشته باشد، سازمان‌ها می‌توانند رویکردهای دیگری را به کار گیرند.

(۹) تحقق دسترسی / انتشار کنترل‌شده اطلاعات

سیستم اطلاعاتی، اطلاعات را در خارج از مرزهای سیستم منتشر نمی‌کند مگر این که:

(الف) [اختصاص: سیستم اطلاعاتی یا مؤلفه تعیین‌شده توسط سازمان] دریافت‌کننده اطلاعات، [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] را فراهم آورد؛ و

(ب) با استفاده از [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان]، تأیید شود که می‌توان اطلاعات را منتشر نمود.

راهنمایی‌های تکمیلی: سیستم‌های اطلاعاتی تنها می‌توانند اطلاعات سازمانی را در محدوده مرزهای تعیین‌شده سیستم حفاظت کنند. برای حصول اطمینان از امن بودن اطلاعات پس از عبور آن‌ها از مرزهای سیستم، باید از ابزارهای ایمنی دیگری استفاده کرد. به عنوان مثالی از خروج اطلاعات از مرزهای سیستم، می‌توان به انتقال اطلاعات به سیستم‌های اطلاعاتی خارجی یا چاپ کردن اطلاعات با استفاده از یکی از چاپگرهای سیستم اشاره کرد. در صورتی که سیستم اطلاعاتی نتواند از کافی بودن قدرت حفاظتی موجودیت‌های خارج از خود اطمینان حاصل کند، سازمان بررسی می‌کند که آیا سیستم‌های اطلاعاتی خارجی دارای قابلیت‌های امنیتی کافی هستند یا خیر. ابزارهای مورد استفاده برای تعیین کافی بودن قدرت امنیتی سیستم‌های اطلاعاتی خارجی عبارتند از انجام بازرسی‌ها و آزمون‌های دوره‌ای، امضای موافقت‌نامه بین سازمان و همتایان آن و فرایندهای دیگری از این دست. لازم نیست که موجودیت‌های خارجی برای حفاظت از اطلاعات دریافتی از همان ابزارهایی استفاده کنند که سازمان آن‌ها را به کار می‌گیرد، اما باید سطح حفاظت کافی را از اطلاعات به عمل آورند. این کنترل پیشرفته، سیستم‌های اطلاعاتی را ملزم می‌کند که از با استفاده از ابزارهای رویه‌ای و فنی، اطلاعات را پیش از ارسال آن‌ها به سیستم‌های اطلاعاتی دیگر تأیید کنند. به عنوان مثال، اگر مجموعه‌ای از اطلاعات توسط یک سیستم اطلاعاتی به سیستم اطلاعاتی دیگری فرستاده شوند که تحت کنترل سازمان دیگری است، با استفاده از ابزارهای فنی بررسی می‌شود که ویژگی‌های امنیتی اطلاعات ارسال‌شده متناسب با سیستم دریافت‌کننده باشد. اگر اطلاعات توسط سیستم اطلاعاتی به یک چاپگر تحت کنترل سازمان فرستاده شوند، می‌توان با استفاده از ابزارهای رویه‌ای اطمینان حاصل کرد که تنها افراد مجاز به این چاپگر دسترسی دارند. این کنترل پیشرفته به ویژه در شرایطی قابل اعمال است که خط‌مشی‌هایی در زمینه دسترسی به اطلاعات وجود داشته باشند و این خط‌مشی‌ها حیطه‌ای فراتر از یک سیستم اطلاعاتی یا سازمان خاص را در بر گیرند.

(۱۰) تحقق دسترسی / باطل کردن ممیزی‌شده سازوکارهای کنترل دسترسی

سازمان، فرایند باطل کردن ممیزی‌شده سازوکارهای کنترل دسترسی خودکار را [اختصاص: با شرایط تعیین‌شده توسط سازمان] پیاده‌سازی می‌نماید.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: AU-2, AU-6.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AC-3 اولویت پایین	AC-3 اولویت متوسط	AC-3 اولویت بالا

AC-4: برقراری جریان اطلاعات

کنترل: سیستم اطلاعاتی، مجوزهای لازم برای کنترل جریان اطلاعات درون سیستم و بین سیستم‌های به‌هم‌پیوسته را بر اساس [اختصاص: خط‌مشی‌های تعیین‌شده توسط سازمان در زمینه کنترل جریان اطلاعات] صادر می‌نماید.

راهنمایی‌های تکمیلی: کنترل جریان اطلاعات، تعیین می‌کند که اطلاعات در کدام مسیرها درون یک سیستم اطلاعاتی و بین سیستم‌های به‌هم‌پیوسته می‌تواند جریان داشته باشد. این الزام به افرادی که مجوز دسترسی به اطلاعات را دارند و همچنین به دسترسی‌های بعدی به اطلاعات توجهی ندارد. محدودیت‌های کنترل جریان اطلاعات، مواردی از این دست را در بر می‌گیرند: مسدود کردن ترافیک خارجی که ادعا می‌کند از درون سازمان نشأت گرفته است، محدود کردن درخواست‌های وب که از سرور پراکسی وب داخلی نیستند، و محدود کردن انتقال اطلاعات بین سازمان‌ها بر اساس محتوا و ساختار داده‌ها. انتقال اطلاعات بین سیستم‌های اطلاعاتی مختلفی که دامنه‌های امنیتی و خط‌مشی‌های امنیتی متفاوت دارند، ممکن است منجر به نقض خط‌مشی‌های یک یا چند دامنه شود. در چنین شرایطی، مباشران و مالکان اطلاعات، راهنمایی‌هایی را در نقاط اجرایی بین سیستم‌های به‌هم‌پیوسته ارائه می‌کنند. هنگامی که سازمان‌ها ناچار به اجرای خط‌مشی‌های امنیتی خاصی هستند، روش‌های معماری ویژه‌ای را به کار می‌گیرند. برخی روش‌های مورد استفاده عبارتند از: (۱) جلوگیری از انتقال اطلاعات بین سیستم‌های اطلاعاتی به‌هم‌پیوسته (صرفاً صدور مجوز دسترسی)، (۲) به‌کارگیری سازوکارهای سخت‌افزاری برای برقراری جریان یک‌طرفه اطلاعات، و (۳) به‌کارگیری سازوکارهای بازبینی مورد اعتماد برای اختصاص مجدد ویژگی‌ها و برچسب‌های امنیتی.

سازمان‌ها معمولاً برای کنترل جریان اطلاعات بین مبادی و مقاصد تعیین‌شده (مانند شبکه‌ها، افراد و دستگاه‌ها) درون سیستم‌های اطلاعاتی و بین سیستم‌های به‌هم‌پیوسته، از خط‌مشی‌های کنترل جریان اطلاعات و سازوکارهای اجرایی استفاده می‌کنند. کنترل جریان بر اساس ویژگی‌های اطلاعات و/یا مسیر اطلاعاتی انجام می‌شود. اجرای این فرایند مثلاً در دستگاه‌های حفاظت مرزی (مانند گیت‌وی‌ها، مسیریاب‌ها، حفاظ‌ها، تونل‌های رمزگذاری یا فایروال‌ها) اتفاق می‌افتد که مجموعه قوانین یا پیکربندی‌هایی را به کار می‌گیرند که خدمات

سیستم اطلاعاتی را محدود می‌کنند، قابلیت فیلترینگ بسته را بر اساس اطلاعات سربرگ ارائه می‌نمایند، یا قابلیت فیلترینگ بسته را بر اساس محتوای پیام ارائه می‌کنند (مثلاً پیاده‌سازی قابلیت جستجوی کلیدواژه‌ها یا استفاده از ویژگی‌های اسناد). سازمان‌ها همچنین قابلیت اعتماد سازوکارهای فیلترینگ/بازرسی (مانند مؤلفه‌های سخت‌افزاری، ثابت‌افزاری و نرم‌افزاری) که اهمیتی حیاتی در پیاده‌سازی جریان اطلاعات دارند را نیز در نظر می‌گیرند. کنترل‌های پیشرفته ۳ تا ۲۲ به روش‌هایی می‌پردازند که تمرکز آن‌ها بر یک یا چند شیوه فیلترینگ پیشرفته، تحلیل ژرف، و سازوکارهای قدرتمندتر جریان اطلاعات است که در محصولات بین‌دامنه‌ای به کار گرفته می‌شوند (مانند حفاظ‌های با سطح تضمین بالا). این قابلیت‌ها معمولاً در محصولات IT موجود در بازار دیده نمی‌شوند. کنترل‌های مربوطه: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

کنترل‌های پیشرفته:

(۱) برقراری جریان اطلاعات / ویژگی‌های امنیتی اشیا

سیستم اطلاعاتی برای پیاده‌سازی [اختصاص: خط‌مشی‌های تعیین‌شده توسط سازمان در زمینه کنترل جریان اطلاعات] به عنوان مبنای تصمیمات کنترل جریان، از [اختصاص: ویژگی‌های امنیتی تعیین‌شده توسط سازمان] مربوط به [اختصاص: اشیای مبدأ، مقصد و اطلاعات تعیین‌شده توسط سازمان] استفده می‌کند.

راهنمایی‌های تکمیلی: سازوکارهای برقراری جریان اطلاعات، ویژگی‌های امنیتی اطلاعات (محتوای داده‌ها و ساختار داده‌ها) و اشیای مبدأ و مقصد را مقایسه می‌کنند و در صورتی که سازوکارها با یک جریان اطلاعاتی مواجه شوند که به مجوز آن‌ها توسط خط‌مشی‌های جریان اطلاعات صادر نشده است، پاسخ مقتضی را ارائه نمایند (مثلاً مسدود کردن، قرنطینه کردن یا نمایش هشدار برای راهبر). به عنوان مثال، یک شی اطلاعاتی که برچسب «مخفی» بر آن خورده است، می‌تواند به یک شی مقصد با برچسب «مخفی» جریان پیدا کند، اما یک شی اطلاعاتی با برچسب «فوق مخفی» نمی‌تواند به یک شی مقصد با برچسب «مخفی» برود. ویژگی‌های امنیتی می‌توانند شامل آدرس‌های مبدأ و مقصد مورد استفاده در فایروال‌های فیلترینگ ترافیک نیز باشند. از طریق برقراری جریان با استفاده از ویژگی‌های امنیتی آشکار، می‌توان افشای انواع خاصی از اطلاعات را کنترل کرد. کنترل مربوطه: AC-16.

(۲) برقراری جریان اطلاعات / دامنه‌های پردازشی

سیستم اطلاعاتی از دامنه‌های پردازشی محافظت‌شده برای پیاده‌سازی [اختصاص: خط‌مشی‌های تعیین‌شده توسط سازمان در زمینه کنترل جریان اطلاعات] و به عنوان مبنایی برای اتخاذ تصمیمات مربوط به کنترل جریان استفاده می‌کند.

راهنمایی‌های تکمیلی: درون سیستم‌های اطلاعاتی، دامنه‌های پردازشی محافظت‌شده به فضاهای پردازشی اطلاق می‌شود که با سایر فضاهای پردازشی تعامل کنترل‌شده دارند و در نتیجه، امکان کنترل جریان اطلاعات بین این فضاها و انتقال جریان اطلاعات به/از اشیای داده/اطلاعات را فراهم می‌آورند. یک دامنه پردازشی محافظت‌شده مثلاً از طریق پیاده‌سازی قوانین مربوط به نوع و دامنه ایجاد می‌شود. در فرایند پیاده‌سازی قوانین مربوط به نوع و دامنه، فرایندهای سیستم‌های اطلاعاتی به دامنه‌ها تخصیص داده می‌شوند؛ اطلاعات بر اساس نوع شناسایی می‌شوند؛ و جریان‌های اطلاعاتی بر اساس دسترسی‌های مجاز به اطلاعات، سیگنال‌دهی‌های مجاز بین دامنه‌ها، و انتقال‌های مجاز به سایر دامنه‌ها کنترل می‌گردند.

(۳) برقراری جریان اطلاعات / کنترل پویای جریان اطلاعات

سیستم اطلاعاتی، کنترل پویای جریان اطلاعات را بر اساس [اختصاص: خط‌مشی‌های تعیین‌شده توسط سازمان] انجام می‌دهد.

راهنمایی‌های تکمیلی: خط‌مشی‌های سازمان در زمینه کنترل پویای جریان اطلاعات مواردی از جمله اجازه دادن یا اجازه ندادن به جریان اطلاعات بر اساس شرایط در حال تغییر یا ملاحظات عملیاتی/مأموریتی را در بر می‌گیرد. به عنوان مثال‌هایی از شرایط در حال تغییر، می‌توان به تغییر در سطح تحمل مخاطرات سازمان به دلیل تغییر در اضطرار نیازهای کسب‌وکار و مأموریت، تغییر در محیط تهدیدات، و حذف رخدادهایی که به طور بالقوه زیان‌آور هستند اشاره کرد. کنترل مربوطه: SI-4.

(۴) برقراری جریان اطلاعات / بررسی محتوایی اطلاعات رمزگذاری‌شده

سیستم اطلاعاتی از طریق [انتخاب (یک یا چند مورد): رمزگشایی اطلاعات، مسدود کردن جریان اطلاعات رمزگذاری‌شده، اتمام نشست‌های ارتباطی که به دنبال انتقال اطلاعات رمزگذاری‌شده هستند، [اختصاص: روش‌ها یا رویه‌های تعیین‌شده توسط سازمان]] مانع از دور زده شدن سازکارهای بررسی محتوا توسط اطلاعات رمزگذاری‌شده می‌شود.

راهنمایی‌های تکمیلی: کنترل مربوطه: SI-4.

(۵) برقراری جریان اطلاعات / انواع داده تعبیه‌شده

سیستم اطلاعاتی [اختصاص: محدودیت‌های تعیین‌شده توسط سازمان] را روی انواع داده تعبیه‌شده اعمال می‌کند.

راهنمایی‌های تکمیلی: وجود انواع داده تعبیه‌شده در بین سایر انواع داده‌ها می‌تواند سبب کاهش اثربخشی کنترل جریان شود. روش‌های تعبیه کردن نوع داده عبارتند از گنجاندن فایل‌های اجرایی به عنوان شی در فایل‌های پردازشگر کلمه، گنجاندن مراجع یا اطلاعات توصیفی در فایل‌های رسانه‌ای، یا انواع داده‌های فشرده‌شده یا بایگانی‌شده که ممکن است شامل چند نوع داده تعبیه‌شده باشند. محدودیت‌های تعبیه کردن داده‌ها با توجه به سطح تعبیه تعیین می‌شوند و مانع سطوحی از تعبیه می‌شوند که ورای قابلیت‌های ابزارهای بازرسی هستند.

(۶) برقراری جریان اطلاعات / فراداده

سیستم اطلاعاتی، کنترل جریان اطلاعاتی را بر اساس [اختصاص: فراداده تعیین‌شده توسط سازمان] انجام می‌دهد.

راهنمایی‌های تکمیلی: فراداده اطلاعاتی است که برای تشریح ویژگی‌های داده‌ها به کار گرفته می‌شود. فراداده می‌تواند شامل فراداده ساختاری باشد که ساختارهای داده‌ها را توصیف می‌کند (مانند قالب، سینتاکس یا معناشناسی داده‌ها)، یا به شکل فراداده توصیفی باشد که محتوای داده‌ها را توصیف می‌نماید (مانند سن، مکان و شماره تلفن). برقراری جریان‌های مجاز اطلاعات بر اساس فراداده، امکان کنترل ساده‌تر و مؤثرتر جریان‌های اطلاعاتی را فراهم می‌آورد. سازمان‌ها قابلیت اعتماد فراداده را با توجه به دقت داده‌ها (یعنی دانستن این که مقادیر فراداده، با توجه به داده‌ها، درست هستند)، یکپارچگی داده‌ها (یعنی جلوگیری از تغییرات غیر مجاز در تگ‌های فراداده)، و پایبندی فراداده به بار داده‌ها (یعنی حصول اطمینان از روش‌های پایبندی قدرتمند با سطح تضمین مناسب) تعیین می‌نمایند.

کنترل‌های مربوطه: AC-16, SI-7.

(۷) برقراری جریان اطلاعات / سازوکارهای جریان یک‌طرفه

سیستم اطلاعاتی، [اختصاص: جریان‌های اطلاعاتی یک‌طرفه تعیین‌شده توسط سازمان] را با استفاده از سازوکارهای سخت‌افزاری برقرار می‌سازد.

(۸) برقراری جریان اطلاعات / فیلترهای خط‌مشی امنیتی

سیستم اطلاعاتی، کنترل جریان اطلاعاتی را با استفاده از [اختصاص: فیلترهای خط‌مشی امنیتی تعیین‌شده توسط سازمان] به عنوان مبنایی برای تصمیمات کنترل [اختصاص: جریان‌های اطلاعاتی تعیین‌شده توسط سازمان] انجام می‌دهد.

راهنمایی‌های تکمیلی: عملکرد فیلترهای خط‌مشی امنیتی تعیین‌شده توسط سازمان می‌تواند بر اساس محتوا و ساختار داده‌ها باشد. به عنوان مثال، فیلترهای خط‌مشی امنیتی مبتنی بر ساختارهای داده‌ها می‌توانند حداکثر طول فایل، حداکثر اندازه فیلد، و نوع فایل‌ها و داده‌ها را مبنای کار خود قرار دهند (برای داده‌های ساختارمند و غیر ساختارمند). فیلترهای خط‌مشی امنیتی مبتنی بر محتوای داده‌ها نیز ممکن است کلمات خاص (مانند فیلترهای کلمات کثیف/تمیز)، شماره یا محدوده مقادیر داده‌ها، و محتوای پنهان را جستجو کنند. داده‌های ساختارمند، امکان تفسیر محتوای داده توسط برنامه کاربردی را فراهم می‌آورند. داده‌های غیر ساختارمند معمولاً به اطلاعات دیجیتالی اطلاق می‌شود که ساختار خاصی ندارند یا ساختار آن‌ها به گونه‌ای است که امکان توسعه قوانینی برای تعیین حساسیت ویژه آن‌ها را فراهم نمی‌کند. داده‌های غیر ساختارمند شامل این موارد هستند: (۱) اشیای بیت‌مپ که به طور ذاتی مبتنی بر زبان نیستند (یعنی تصاویر، ویدئوها یا فایل‌های صوتی)؛ و (۲) اشیای بافتی که مبتنی بر زبان‌های نوشته‌شده یا چاپ‌شده هستند (مانند اسناد پردازش کلمه موجود در بازار، صفحات گسترده یا ایمیل‌ها). سازمان‌ها می‌توانند برای دستیابی به اهداف کنترل جریان اطلاعات، از بیش از یک فیلتر خط‌مشی امنیتی استفاده کنند (مثلاً استفاده از لیست کلمات تمیز در کنار لیست کلمات کثیف می‌تواند احتمال تأیید نادرست را کاهش دهد).

(۹) برقراری جریان اطلاعات / بازبینی انسانی

سیستم اطلاعاتی، بازبینی انسانی [اختصاص: جریان‌های اطلاعاتی تعیین‌شده توسط سازمان] را در این شرایط در دستور کار قرار می‌دهد: [اختصاص: شرایط تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: سازمان‌ها در تمام شرایطی که اتخاذ خودکار تصمیمات کنترل جریان اطلاعات امکان‌پذیر باشد، فیلترهای خط‌مشی امنیتی را تعریف می‌کنند. در صورتی که اتخاذ خودکار این تصمیمات امکان‌پذیر نباشد، ممکن است از بازبینی انسانی به جای فیلترینگ خط‌مشی امنیتی خودکار، یا به عنوان مکمل آن، استفاده شود. بازبینی انسانی ممکن است در شرایط دیگر نیز در صورت صلاحدید سازمان به کار گرفته شود.

(۱۰) برقراری جریان اطلاعات / فعال کردن و غیر فعال کردن فیلترهای خط‌مشی امنیتی

سیستم اطلاعاتی قابلیت فعال و غیر فعال کردن [اختصاص: فیلترهای خط‌مشی امنیتی تعیین‌شده توسط سازمان] را در شرایط روبرو برای راهبران دارای اختیارات ویژه فراهم می‌آورد: [اختصاص: شرایط تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: به عنوان مثال، سیستم اطلاعاتی می‌تواند به راهبران اجازه دهد که فیلترهای خط‌مشی امنیتی را برای پذیرفتن انواع مجاز داده‌ها فعال کنند.

(۱۱) برقراری جریان اطلاعات / پیکربندی فیلترهای خط‌مشی امنیتی

سیستم اطلاعاتی قابلیت پیکربندی [اختصاص: فیلترهای خط‌مشی امنیتی تعیین‌شده توسط سازمان] را جهت پشتیبانی از خط‌مشی‌های امنیتی مختلف برای راهبران دارای اختیارات ویژه فراهم می‌آورد.

راهنمایی‌های تکمیلی: به عنوان مثال، راهبران می‌توانند برای بازتاب دادن تغییرات در خط‌مشی‌های امنیتی، لیست «کلمات کثیف» که توسط سازوکارهای خط‌مشی امنیتی بر اساس تعاریف ارائه‌شده توسط سازمان بررسی می‌شوند را تغییر دهند.

(۱۲) برقراری جریان اطلاعات / شناسه‌های نوع داده

در هنگام انتقال اطلاعات بین دامنه‌های امنیتی مختلف، سیستم اطلاعاتی به منظور تأیید داده‌های ضروری برای اتخاذ تصمیمات مربوط به جریان اطلاعات، از [اختصاص: شناسه‌های نوع داده تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: به عنوان مثال‌هایی از شناسه‌های نوع داده‌ها می‌توان به نام فایل، نوع فایل، توکن یا امضای فایل، و چند توکن و امضای درونی همزمان برای فایل اشاره کرد. ممکن است سیستم‌های اطلاعاتی تنها در صورتی اجازه انتقال داده‌ها را بدهند که با فرمت‌های مشخص‌شده در زمینه نوع داده سازگاری داشته باشند.

(۱۳) برقراری جریان اطلاعات / تجزیه به مؤلفه‌های فرعی مبتنی بر خط‌مشی‌ها

در هنگام انتقال اطلاعات بین دامنه‌های امنیتی مختلف، سیستم اطلاعاتی به منظور ارائه اطلاعات به سازوکارهای اجرای خط‌مشی‌ها، آن‌ها را به [اختصاص: مؤلفه‌های فرعی خط‌مشی‌محور تعیین‌شده توسط سازمان] تجزیه می‌کند.

راهنمایی‌های تکمیلی: سازوکارهای اجرای خط‌مشی‌ها به منظور تسهیل جریان اطلاعات پیش از انتقال این اطلاعات به دامنه‌های امنیتی مختلف، اقدام به پیاده‌سازی قوانین فیلترینگ، بازرسی، و/یا پاک‌سازی روی مؤلفه‌های فرعی مبتنی بر خط‌مشی‌ها می‌کنند. تجزیه فایل‌های انتقالی، تصمیم‌گیری در خصوص مبدأ، مقصد، گواهی‌ها، دسته‌بندی، پیوست‌ها و سایر وجه تمایزهای امنیتی را تسهیل می‌کند.

(۱۴) برقراری جریان اطلاعات / محدودیت‌های فیلتر خط‌مشی امنیتی

در هنگام انتقال اطلاعات بین دامنه‌های امنیتی مختلف، سیستم اطلاعاتی [اختصاص: فیلترهای خط‌مشی امنیتی تعیین‌شده توسط سازمان] را پیاده‌سازی می‌کند که نیازمند فرمت‌های کاملاً عددی هستند که محتوا و ساختار داده‌ها را محدود کند.

راهنمایی‌های تکمیلی: محدودیت محتوا و ساختار داده‌ها باعث می‌شود که محتوای به طور بالقوه مخرب در تراکنش‌های بین دامنه‌ها کاهش یابد. فیلترهای خط‌مشی امنیتی از طریق روش‌هایی مانند محدود کردن اندازه فایل و طول فیلد، ساختارهای داده‌ها را محدود می‌نمایند. فیلترهای خط‌مشی محتوای داده‌ها نیز روش‌هایی از این دست را شامل می‌شوند: (۱) رمزگذاری فرمت‌های مربوط به مجموعه کاراکترها، (۲) محدود کردن فیلدهای داده‌های کاراکتری به کاراکترهای الفبایی-عددی، (۳) ممنوع کردن استفاده از کاراکترهای ویژه، و (۴) تأیید ساختار الگوها.

(۱۵) برقراری جریان اطلاعات / ردیابی اطلاعات تأییدنشده

در هنگام انتقال اطلاعات بین دامنه‌های امنیتی مختلف، سیستم اطلاعاتی اقدام به بررسی اطلاعات می‌کند تا وجود [اختصاص: اطلاعات تأییدنشده تعیین‌شده توسط سازمان] را ردیابی کند و بر اساس [اختصاص: خط‌مشی‌های امنیتی تعیین‌شده توسط سازمان]، از انتقال آن‌ها جلوگیری به عمل آورد.

راهنمایی‌های تکمیلی: برای ردیابی اطلاعات تأییدنشده از روش‌های مختلفی استفاده می‌شود. به عنوان مثال، تمام اطلاعاتی که قرار است منتقل شوند، بررسی می‌گردند تا کدهای مخرب و کلمات کثیف احتمالی موجود در آن‌ها یافته شوند. کنترل مربوطه: SI-3.

(۱۶) برقراری جریان اطلاعات / انتقال اطلاعات در سیستم‌های به‌هم‌پیوسته

[حذف شد: به بخش AC-4 منتقل شد].

(۱۷) برقراری جریان اطلاعات / احراز هویت دامنه

سیستم اطلاعاتی برای انتقال اطلاعات، نقاط مبدأ و مقصد را به طور منحصربه‌فرد بر اساس [انتخاب (یک یا چند مورد): سازمان، سیستم، برنامه کاربردی، شخص] شناسایی و احراز هویت می‌کند.

راهنمایی‌های تکمیلی: اِسناد، یکی از مؤلفه‌های اصلی مفهوم امنیت عملیات است. توانایی شناسایی نقاط مبدأ و مقصد جریان اطلاعات در سیستم‌های اطلاعاتی، امکان بازسازی جرم‌شناسانه رویدادها در صورت نیاز را فراهم می‌آورد و با استناد موارد نقش خط‌مشی‌ها به افراد و سازمان‌های خاص، همگان را به رعایت قانون ترغیب می‌کند. برای احراز هویت موفقیت‌آمیز دامنه، باید سیستم‌ها، سازمان‌ها و افراد دخیل در فرایند آماده‌سازی، ارسال، دریافت یا توزیع اطلاعات را با استفاده از برچسب‌های سیستم اطلاعاتی از یکدیگر متمایز نمود.

(۱۸) برقراری جریان اطلاعات / پیونددهی ویژگی‌های امنیتی

سیستم اطلاعاتی برای تسهیل اجرای خط‌مشی‌های جریان اطلاعات، ویژگی‌های امنیتی را با استفاده از [اختصاص: شیوه‌های پیونددهی تعیین‌شده توسط سازمان] به اطلاعات پیوند می‌دهد.

راهنمایی‌های تکمیلی: شیوه‌های پیونددهی مورد استفاده سیستم‌های اطلاعاتی، بر قدرت پیونددهی ویژگی‌های امنیتی تأثیر می‌گذارند. قدرت پیونددهی و ضمانت‌های مربوط به شیوه‌های پیونددهی، نقش مهمی در اعتماد سازمان‌ها به فرایند برقراری جریان اطلاعات دارند. شیوه‌های پیونددهی بر تعداد و شدت بازبینی‌های مورد نیاز توسط سازمان نیز تأثیر می‌گذارند. کنترل‌های مربوطه: AC-16, SC-16.

(۱۹) برقراری جریان اطلاعات / تأیید فراداده

در هنگام انتقال اطلاعات بین دامنه‌های امنیتی مختلف، سیستم اطلاعاتی برای فراداده‌ها نیز از همان روش‌های فیلترینگ خط‌مشی امنیتی استفاده می‌کند که برای داده‌های انتقالی به کار گرفته است.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، تأیید فراداده و داده‌هایی که فراداده به آن‌ها اعمال می‌شود را لازم می‌دارد. برخی سازمان‌ها بین فراداده و داده‌های انتقالی (یعنی داده‌هایی که فراداده به آن‌ها پیوند داده شده است) تمایز قایل می‌شوند. برخی سازمان‌های دیگر نیز چنین تمایزی قایل نمی‌شوند و فراداده و داده‌هایی که فراداده به آن‌ها اعمال می‌شود را بخشی از داده‌های انتقالی به شمار می‌آورند. فیلترینگ و بازرسی روی تمامی اطلاعات (شامل فراداده و داده‌هایی که فراداده به آن‌ها اعمال می‌شود) اعمال می‌گردد.

(۲۰) برقراری جریان اطلاعات / روش‌های تأییدشده

سازمان برای کنترل جریان [اختصاص: اطلاعات تعیین‌شده توسط سازمان] در دامنه‌های امنیتی، از [اختصاص: روش‌های تعیین‌شده توسط سازمان در پیکربندی‌های تأییدشده] استفاده می‌کند.

راهنمایی‌های تکمیلی: سازمان‌ها پیکربندی‌ها و روش‌های تأییدشده در راهنمایی‌ها و خط‌مشی‌های بین دامنه‌ای را بر اساس انواع جریان‌های اطلاعاتی بین مرزهای دسته‌بندی، تعریف می‌کنند. دفتر مدیریت یکپارچه بین دامنه‌ای (UCDMO) لیست مرجع روش‌های تأییدشده بین دامنه‌ای را ارائه می‌نماید.

(۲۱) برقراری جریان اطلاعات / تفکیک فیزیکی و منطقی جریان‌های اطلاعاتی

سیستم اطلاعاتی برای [اختصاص: تفکیک ضروری بر اساس نوع اطلاعات]، جریان‌های اطلاعاتی را با استفاده از [اختصاص: شیوه‌ها و سازوکارهای تعیین‌شده توسط سازمان] تفکیک می‌نماید.

راهنمایی‌های تکمیلی: سازمان می‌تواند با تفکیک جریان‌های اطلاعاتی بر اساس نوع اطمینان حاصل نماید که اطلاعات در حال انتقال داده شدن با هم مخلوط نمی‌شوند. سازمان همچنین می‌تواند برای

کنترل جریان از مسیرهای انتقالی استفاده کند که استفاده از آن‌ها پیشتر امکان‌پذیر نبوده است. بدین ترتیب، سازمان می‌تواند به شکل بهتری از اطلاعات محافظت نماید. انواع قابل تفکیک اطلاعات مواردی از جمله ترافیک ارتباطی ورودی و خروجی، درخواست‌ها و پاسخ‌های خدمات، و اطلاعات دسته‌های امنیتی مختلف را در بر می‌گیرند.

(۲۲) برقراری جریان اطلاعات / دسترسی صِرف

سیستم اطلاعاتی امکان دسترسی از یک دستگاه به پلت‌فرم‌های پردازشی، برنامه‌های کاربردی یا داده‌های موجود روی چند دامنه امنیتی مختلف فراهم می‌آورد و در عین حال، از برقراری جریان اطلاعات بین دامنه‌های امنیتی مختلف جلوگیری می‌نماید.

راهنمایی‌های تکمیلی: به عنوان مثال، سیستم اطلاعاتی دسکتاپی را در اختیار کاربران قرار می‌دهد تا بدون ارائه سازوکارهایی جهت انتقال اطلاعات بین دامنه‌های امنیتی مختلف، امکان دسترسی به هر دامنه امنیتی متصل را برای آن‌ها فراهم آورد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، اولویت پایین	AC-4 اولویت متوسط	AC-4 اولویت بالا

AC-5: **تفکیک وظایف**

کنترل: سازمان:

الف. [اختصاص: وظایف فردی تعیین‌شده توسط سازمان] را تفکیک می‌کند؛

ب. تفکیک وظایف افراد را مستندسازی می‌کند؛ و

پ. مجوزهای دسترسی به سیستم اطلاعاتی برای پشتیبانی از تفکیک وظایف را مستندسازی می‌کند.

راهنمایی‌های تکمیلی: هدف از تفکیک وظایف، جلوگیری از سوء استفاده احتمالی از اختیارات مجاز و کاهش خطر فعالیت‌های بدخواهانه بدون تبانی است. تفکیک وظایف، مواردی از این دست را در بر می‌گیرد: (۱) تقسیم کارکردهای مأموریت و پشتیبانی سیستم اطلاعاتی بین نقش‌ها و/یا افراد مختلف؛ (۲) اجرای کارکردهای

پشتیبانی سیستم اطلاعاتی توسط افراد مختلف (مانند مدیریت سیستم، برنامه‌ریزی، مدیریت پیکربندی، آزمون و تضمین کیفیت، و امنیت شبکه)؛ و (۳) حصول اطمینان از این که کارکنان امنیتی مسئول راهبری کارکردهای کنترل دسترسی، کارکردهای ممیزی را راهبری نمی‌کنند. کنترل‌های مربوطه: AC-3, AC-6, PE-3, PE-4, PS-2.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، اولویت پایین	AC-5 اولویت متوسط	AC-5 اولویت بالا

AC-6: **حداقل بودن اختیارات**

کنترل: سازمان اصل حداقل بودن اختیارات را در دستور کار قرار می‌دهد و تنها امکان دسترسی‌هایی را به کاربران (یا فرایندهایی که فعالیت‌هایی را از طرف آن‌ها انجام می‌دهند) می‌دهد که برای انجام وظایف آن‌ها بر اساس مأموریت و کارکردهای کسب‌وکار سازمان ضروری باشد.

راهنمایی‌های تکمیلی: سازمان‌ها از اصل حداقل بودن اختیارات برای برخی از سیستم‌های اطلاعاتی و وظایف خاص استفاده می‌کنند. اصل حداقل بودن اختیارات همچنین در مورد فرایندهای سیستم اطلاعاتی نیز پیاده‌سازی می‌شود تا اطمینان حاصل گردد که سطح اختیارات این فرانیدها، بیش از نیاز آن‌ها برای انجام مأموریت‌ها و فرایندهای کسب‌وکار سازمان نیست. سازمان‌ها در صورت لزوم اقدام به ایجاد حساب‌های سیتسم اطلاعاتی، فرایندها و نقش‌های اضافی می‌کنند، تا بتوانند اصل حداقل بودن اختیارات را پیاده‌سازی نمایند. سازمان‌ها همچنین اصل حداقل بودن اختیارات را در مورد توسعه، پیاده‌سازی و فعالیت سیستم‌های اطلاعاتی نیز به کار می‌گیرند. کنترل‌های مربوطه: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

کنترل‌های پیشرفته:

(۱) حداقل بودن اختیارات / صدور مجوز دسترسی به توابع امنیتی

سازمان مجوز دسترسی به [اختصاص: توابع امنیتی تعیین‌شده توسط سازمان (پیاده‌سازی‌شده در سخت‌افزارها، نرم‌افزارها و ثابت‌افزارها) و اطلاعات امنیتی تعیین‌شده توسط سازمان] را صادر می‌نماید.

راهنمایی‌های تکمیلی: به عنوان مثال‌هایی از توابع امنیتی، می‌توان به ایجاد حساب‌های سیستم، پیکربندی مجوزهای دسترسی (یعنی مجوزها و اختیارات)، تنظیم رویدادهایی که باید ممیزی شوند، و تنظیم پارامترهای تشخیص ورود غیر مجاز اشاره کرد. اطلاعات امنیتی نیز مواردی از جمله قوانین فیلترینگ برای مسیریاب‌ها و فایروال‌ها، اطلاعات مدیریت کلید رمزنگاری، پارامترهای پیکربندی خدمات امنیتی و لیست‌های کنترل دسترسی را در بر می‌گیرند. کارکنانی که به آن‌ها مجوز داده می‌شود، افرادی مانند راهبران امنیتی، راهبران شبکه و سیستم، مسئولان امنیت سیستم، کارکنان تعمیر و نگهداری سیستم، برنامه‌نویسان سیستم و سایر کاربران دارای اختیارات ویژه هستند. کنترل‌های مربوطه: AC-17, AC-18, AC-19.

(۲) حداقل بودن اختیارات / دسترسی به توابع غیر امنیتی بدون نیاز به اختیار ویژه

سازمان از کاربران نقش‌ها یا حساب‌های سیستم اطلاعاتی با دسترسی به [اختصاص: توابع امنیتی یا اطلاعات امنیتی تعیین‌شده توسط سازمان] می‌خواهد که در هنگام دسترسی به توابع غیر امنیتی، از نقش‌ها یا حساب‌های بدون نیاز به اختیار ویژه استفاده کنند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته میزان دسترسی به اطلاعات در هنگام انجام عملیاتی از درون نقش‌ها یا حساب‌های دارای اختیار ویژه را محدود می‌کند. به این دلیل به نقش‌ها اشاره شده است که گاهی اوقات سازمان‌ها از خط‌مشی‌های کنترل دسترسی مبتنی بر نقش استفاده می‌کنند یا این که تغییر نقش سبب تغییر در مجوز دسترسی می‌شود. کنترل مربوطه: PL-4.

(۳) حداقل بودن اختیارات / دسترسی شبکه به دستورات ویژه

سازمان مجوز دسترسی شبکه به [اختصاص: دستورات ویژه تعیین‌شده توسط سازمان] را تنها برای [اختصاص: نیازهای عملیاتی تعیین‌شده توسط سازمان] صادر می‌کند و منطق این دسترسی را در طرح امنیتی سیستم اطلاعاتی مستندسازی می‌نماید.

راهنمایی‌های تکمیلی: دسترسی شبکه به هر نوع دسترسی از طریق اتصال شبکه به جای اتصال محلی (یعنی حضور فیزیکی کاربر در دستگاه) گفته می‌شود. کنترل مربوطه: AC-17.

(۴) حداقل بودن اختیارات / دامنه‌های پردازشی مجزا

سیستم اطلاعاتی با ارائه دامنه‌های پردازشی مجزا، امکان تخصیص دقیق‌تر اختیارات کاربری را فراهم می‌آورد.

راهنمایی‌های تکمیلی: به منظور ارائه دامنه‌های پردازشی مجزا جهت تخصیص دقیق‌تر اختیارات کاربری، می‌توان چنین اقداماتی را انجام داد: (۱) استفاده از شیوه‌های مجازی‌سازی برای ارائه اختیارات بیشتر درون یک ماشین مجازی و در عین حال، محدود کردن اختیارات به سایر ماشین‌های مجازی یا ماشین‌های واقعی مربوطه؛ (۲) استفاده از سازوکارهای تفکیک دامنه سخت‌افزاری و/یا نرم‌افزاری؛ و (۳) استفاده از دامنه‌های فیزیکی مجزا. کنترل‌های مربوطه: AC-4, SC-3, SC-30, SC-32.

(۵) حداقل بودن اختیارات / حساب‌های ویژه

سازمان امکان دسترسی به حساب‌های ویژه روی سیستم اطلاعاتی را تنها برای [اختصاص: کارکنان یا نقش‌های تعیین‌شده توسط سازمان] فراهم می‌آورد.

راهنمایی‌های تکمیلی: حساب‌های ویژه در سیستم‌عامل‌های موجود در بازار، معمولاً حساب‌های راهبری سیستم نامیده می‌شوند. محدود کردن امکان دسترسی به حساب‌های ویژه به نقش‌ها و کارکنان خاص باعث می‌شود که کاربران عادی نتوانند به توابع و اطلاعات ویژه دسترسی داشته باشند. ممکن است سازمان‌ها در اجرای این کنترل پیشرفته، بین اختیارات حساب‌های محلی و حساب‌های دامنه تمایز قایل شوند، مشروط بر این که توانایی کنترل پیکربندی پارامترهای امنیتی اصلی سیستم‌های اطلاعاتی یا کاهش مخاطرات به هر روش دیگر را داشته باشند. کنترل مربوطه: CM-6.

(۶) حداقل بودن اختیارات / دسترسی ویژه توسط کاربران غیر سازمانی

سازمان از دسترسی ویژه به سیستم‌های اطلاعاتی توسط کاربران غیر سازمانی جلوگیری به عمل می‌آورد.

راهنمایی‌های تکمیلی: کنترل مربوطه: IA-8.

(۷) حداقل بودن اختیارات / بازبینی اختیارات ویژه کاربری

سازمان:

(الف) [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان]، اختیارات تخصیص‌داده‌شده به [اختصاص: دسته‌های کاربران یا نقش‌های تعیین‌شده توسط سازمان] را بازبینی می‌کند تا نیاز به وجود آن‌ها را تأیید نماید؛ و

(ب) در صورت لزوم، اختیارات ویژه را مجدداً تخصیص می‌دهد یا آن‌ها را حذف می‌کند، به گونه‌ای که به درستی بازتاب‌دهنده نیازهای کسب‌وکار و مأموریت سازمان باشند.

راهنمایی‌های تکمیلی: نیاز به برخی اختیارات ویژه کاربری ممکن است به مرور زمان و بسته به تغییرات توابع کسب‌وکار و مأموریت سازمان، محیط عملیاتی، فناوری‌ها و تهدیدات، تغییر نماید. بنابراین، باید

این اختیارات را به صورت دوره‌ای بازبینی کرد تا مشخص شود که آیا کماکان به آن‌ها نیاز هست یا خیر. اگر نتوان این نیاز را تأیید کرد، سازمان اقدامات اصلاحی مقتضی را در دستور کار قرار خواهد داد. کنترل مربوطه: CA-7.

(۸) حداقل بودن اختیارات / سطوح اختیارات ویژه برای اجرای کد

در صورتی که کاربر سطح اختیار ویژه لازم برای اجرای یک [اختصاص: نرم‌افزار تعیین‌شده توسط سازمان] را نداشته باشد، سیستم اطلاعاتی از اجرای نرم‌افزار مذکور جلوگیری می‌کند.

راهنمایی‌های تکمیلی: در برخی شرایط خاص، لازم است نرم‌افزارها یا برنامه‌های کاربردی که نیازمند سطوح بالاتر اختیارات ویژه هستند، اجرا شوند تا برخی توابع ضروری به اجرا در آیند. اگر کاربران از سطح اختیار لازم برای اجرای این نرم‌افزارها یا برنامه‌های کاربردی برخوردار نباشند، به طور غیر مستقیم سطح اختیار بالاتری به آن‌ها تخصیص داده می‌شود.

(۹) حداقل بودن اختیارات / استفاده ممیزی از توابع ویژه

سیستم اطلاعاتی، اجرای توابع ویژه را ممیزی می‌نماید.

راهنمایی‌های تکمیلی: سوء استفاده عامدانه یا غیر عامدانه از توابع ویژه توسط کاربران مجاز یا موجودیت‌های غیر مجاز خارجی که حساب‌های سیستم اطلاعاتی را در معرض خطر قرار داده‌اند، یکی از دغده‌های جدی و مستمر سازمان‌ها است و می‌تواند اثرات نامطلوب زیادی بر آن‌ها داشته باشد. ممیزی استفاده از توابع ویژه، یکی از راه‌های ردیابی این موارد سوء استفاده است. بدین ترتیب، خطر تهدیدات داخلی و تهدیدات مستمر پیشرفته (APT) کاهش می‌یابد. کنترل مربوطه: AU-2.

(۱۰) حداقل بودن اختیارات / جلوگیری از اجرا شدن توابع ویژه توسط کاربران غیر ویژه

سیستم اطلاعاتی از اجرا شدن توابع ویژه (مانند غیر فعال کردن، دور زدن یا تغییر دادن ابزارهای امنیتی پیاده‌سازی‌شده) توسط کاربران غیر ویژه جلوگیری می‌نماید.

راهنمایی‌های تکمیلی: توابع ویژه مواردی از جمله ایجاد حساب‌های سیستم اطلاعاتی، بررسی یکپارچگی سیستم، یا راهبری کردن فعالیت‌های مدیریت کلید رمزنگاری را در بر می‌گیرند. کاربران غیر ویژه به افرادی گفته می‌شود که اختیارات لازم را ندارند. دور زدن سازوکارهای تشخیص یا جلوگیری از ورود غیر مجاز یا سازوکارهای مقابله با کدهای مخرب، مثال‌هایی از توابع ویژه هستند که کاربران غیر ویژه حق اجرای آن‌ها را ندارند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، اولویت پایین	AC-6(1)(2)(5)(9)(10) اولویت متوسط	AC-6(1)(2)(3)(5)(9)(10) اولویت بالا

AC-7: تلاش‌های ورود ناموفق

کنترل: سیستم اطلاعاتی:

الف. محدودیت [اختصاص: تعداد تعیین‌شده توسط سازمان] تلاش ورود ناموفق متوالی توسط کاربر را [اختصاص: مدت زمان تعیین‌شده توسط سازمان] تعیین و اجرا می‌کند؛ و

ب. پس از اتمام محدودیت تلاش‌های ناموفق، به صورت خودکار [انتخاب: گره/حساب را برای [اختصاص: مدت زمان تعیین‌شده توسط سازمان] قفل می‌کند؛ گره/حساب را قفل می‌کند تا زمانی که راهبر آن را باز کند؛ تلاش بعدی برای ورود به سیستم را بر اساس [اختصاص: الگوریتم تأخیر تعیین‌شده توسط سازمان] به تأخیر می‌اندازد].

راهنمایی‌های تکمیلی: صرف نظر از این که تلاش ورود از طریق یک اتصال محلی یا شبکه انجام شده باشد، کنترل تکمیلی حاضر برقرار خواهد بود. به دلیل احتمال DoS، قفل شدن خودکار توسط سیستم اطلاعاتی معمولاً حالت موقتی دارد و پس از گذشت زمانی که ز پیش توسط سازمان تعیین شده است، سیستم از حالت قفل خارج می‌شود. اگر از یک الگوریتم تأخیر استفاده شود، ممکن است سازمان بر اساس قابلیت‌های مؤلفه‌های مختلف سیستم اطلاعاتی، از الگوریتم‌های متفاوتی برای آن‌ها استفاده کند. واکنش به تلاش‌های ورود ناموفق ممکن است در سطح سیستم‌عامل یا در سطح برنامه کاربردی پیاده‌سازی شود. کنترل‌های مربوطه: AC-2, AC-9, AC-14, IA-5.

کنترل‌های پیشرفته:

(۱) تلاش‌های ورود ناموفق / قفل شدن خودکار حساب
[حذف شد: به بخش AC-7 منتقل شد].

(۲) تلاش‌های ورود ناموفق / پاک کردن دستگاه همراه

سیستم اطلاعاتی پس از [اختصاص: تعداد تعیین‌شده توسط سازمان] تلاش ورود ناموفق، اطلاعات را بر اساس [اختصاص: شیوه‌ها و الزامات پاکسازی تعیین‌شده توسط سازمان] از [اختصاص: دستگاه‌های همراه تعیین‌شده توسط سازمان] پاک می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته تنها برای دستگاه‌های همراهی است که کاربر باید به آن‌ها وارد شود (مانند دستیارهای دیجیتال شخصی، گوشی‌های هوشمند و تبلت‌ها). ورود به دستگاه همراه صورت می‌گیرد، نه به یک حساب موجود روی آن. بنابراین، هر بار ورود موفق به هر یک از حساب‌های روی دستگاه همراه، سبب ریست شدن شمارنده ورودهای ناموفق به صفر می‌شود. سازمان در هنگام تعیین اطلاعاتی که باید پاک شوند، دقت زیادی به عمل می‌آورد، زیرا در غیر این صورت ممکن است اطلاعات بیش از حد پاک شوند و دستگاه کارایی خود را از دست بدهد. اگر اطلاعات موجود روی دستگاه با استفاده از سازوکارهای رمزگذاری قدرتمند محافظت شده باشند و سطح این حفاظت کافی باشد، ممکن است نیازی به پاک کردن اطلاعات نباشد. کنترل‌های مربوطه: AC-19, MP-5, MP-6, SC-13.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AC-7 اولویت پایین	AC-7 اولویت متوسط	AC-7 اولویت بالا

AC-8: نوتیفیکیشن استفاده از سیستم

کنترل: سیستم اطلاعاتی:

الف. پیش از اعطای مجوز دسترسی به سیستم، [اختصاص: بنر یا پیام نوتیفیکیشن استفاده از سیستم، تعیین‌شده توسط سازمان] را برای کاربران نمایش می‌دهد. این بنر یا پیام، اطلاعیه‌های امنیتی و حریم خصوصی را بر اساس دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال در اختیار کاربران قرار می‌دهد و بیان می‌کند که:

۱. کاربران به سیستم اطلاعاتی دولت آمریکا دسترسی پیدا کرده‌اند؛
۲. استفاده از سیستم اطلاعاتی ممکن است پایش، ثبت و ممیزی شود؛

۳. استفاده غیر مجاز از سیستم اطلاعاتی ممنوع است و با جرایم مدنی و کیفری مواجه خواهد شد؛ و
۴. استفاده از سیستم اطلاعاتی بدین معنی است که کاربر رضایت خود را در خصوص پایش و ثبت اعلام کرده است؛

ب. بنر یا پیام نوتیفیکیشن را روی صفحه نمایش نگه می‌دارد، تا زمانی که کاربر شرایط استفاده را تأیید کند و اقدامی را برای ورود به سیستم اطلاعاتی یا دسترسی به آن انجام دهد؛ و

پ. در مورد سیستم‌های با دسترسی عمومی:

۱. پیش از اعطای مجوز دسترسی بیشتر، اطلاعات استفاده از سیستم را با [اختصاص: شرایط تعیین‌شده توسط سازمان] نمیش می‌دهد؛
۲. در صورت وجود، موارد ارجاع به قوانین پایش، ثبت یا ممیزی که سازگار با مسائل حریم خصوصی سیستم هستند را نشان می‌دهد؛ و
۳. استفاده‌های مجاز از سیستم را شرح می‌دهد.

راهنمایی‌های تکمیلی: نوتیفیکیشن‌های استفاده از سیستم را می‌توان با استفاده از پیام‌ها یا بنرهایی پیش از ورود افراد به سیستم اطلاعاتی نمایش داد. این نوتیفیکیشن‌ها تنها برای دسترسی از طریق واسط‌های ورود با کاربر انسانی استفاده می‌شوند و در صورت وجود نداشتن این واسط‌های انسانی، ضروری نخواهند بود. بسته به نیازهای سازمان و توزیع جمعیت‌شناختی کاربران سیستم اطلاعاتی، ممکن است بنرها و پیام‌های نوتیفیکیشن به زبان‌های مختلفی نمایش داده شوند. سازمان‌ها به منظور بازبینی قانونی و تأیید محتوای بنرهای هشدار، با دفتر مشاور کل مشورت می‌کنند.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AC-8 اولویت پایین	AC-8 اولویت متوسط	AC-8 اولویت بالا

AC-9: نوتیفیکیشن ورود (دسترسی) در گذشته

کنترل: سیستم اطلاعاتی پس از ورود (دسترسی) موفق کاربر به سیستم، زمان و تاریخ ورود (دسترسی) قبلی را به وی اطلاع می‌دهد.

راهنمایی‌های تکمیلی: این کنترل مربوط به ورود به سیستم‌های اطلاعاتی از طریق واسط‌های کاربر انسانی و آن دسته از موارد ورود به سیستم است که در انواع دیگر معماری (مانند معماری خدمت‌محور) رخ می‌دهند. کنترل‌های مربوطه: AC-7, PL-4.

کنترل‌های پیشرفته:

(۱) نوتیفیکیشن ورود در گذشته / ورودهای ناموفق

سیستم اطلاعاتی پس از ورود/دسترسی موفق کاربر به سیستم، به وی اطلاع می‌دهد که پس از آخرین ورود/دسترسی موفق، چند تلاش ناموفق برای ورود/دسترسی به سیستم صورت گرفته است.

(۲) نوتیفیکیشن ورود در گذشته / ورود موفق / ناموفق

سیستم اطلاعاتی به کاربر اطلاع می‌دهد که [اختصاص: در بازه زمانی تعیین‌شده توسط سازمان] چند [انتخاب: ورود/دسترسی موفق؛ تلاش ناموفق برای ورود/دسترسی؛ هر دو مورد] صورت گرفته است.

(۳) نوتیفیکیشن ورود در گذشته / نوتیفیکیشن تغییرات حساب

سیستم اطلاعاتی به کاربر اطلاع می‌دهد که [اختصاص: در بازه زمانی تعیین‌شده توسط سازمان] چه تغییراتی در [اختصاص: پارامترها/ویژگی‌های امنیتی حساب کاربر، بر اساس تعریف سازمان] صورت گرفته است.

(۴) نوتیفیکیشن ورود در گذشته / سایر اطلاعات ورود

سیستم اطلاعاتی پس از ورود/دسترسی موفق کاربر به سیستم، این اطلاعات را به وی اطلاع می‌دهد: [اختصاص: اطلاعات تعیین‌شده توسط سازمان که باید علاوه بر زمان و تاریخ آخرین ورود (دسترسی)، برای کاربر نمایش داده شوند].

راهنمایی‌های تکمیلی: این کنترل پیشرفته به سازمان‌ها اجازه می‌دهد تا اطلاعات دیگری که باید برای کاربر نمایش داده شوند را تعیین نمایند. به عنوان مثالی از این اطلاعات، می‌توان به مکان ورود قبلی اشاره کرد. مکان کاربر بر اساس اطلاعاتی ارائه می‌شود که سیستم اطلاعاتی می‌تواند به آن دست یابد. به عنوان مثال، می‌توان از آدرس IP که ورود از طریق آن صورت گرفته است، شناسه دستگاه، یا نوتیفیکیشن ورود محلی نام برد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

AC-10: کنترل نشست‌های همزمان

کنترل: سیستم اطلاعاتی تعداد نشست‌های همزمان برای هر [اختصاص: حساب و/یا نوع حساب تعیین‌شده توسط سازمان] را به [اختصاص: تعداد تعیین‌شده توسط سازمان] محدود می‌کند.

راهنمایی‌های تکمیلی: ممکن است سازمان‌ها حداکثر تعداد نشست‌های همزمان برای حساب‌های سیستم اطلاعاتی را به صورت جهانی بر اساس نوع حساب (مانند کاربر ویژه، کاربر غیر ویژه، دامنه، برنامه کاربردی خاص)، حساب، یا ترکیبی از این دو تعیین کنند. به عنوان مثال، ممکن است سازمان تعداد نشست‌های همزمان برای راهبران سیستم یا افرادی که در دامنه‌های دارای حساسیت خاص یا برنامه‌های کاربردی دارای مأموریت حساس کار می‌کنند را محدود کند. این کنترل به نشست‌های همزمان برای حساب‌های سیستم اطلاعاتی می‌پردازد و در خصوص نشست‌های همزمان توسط یک کاربر واحد از طریق چند حساب سیستم مصداق ندارد.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	AC-10 اولویت بالا

AC-11: قفل کردن نشست

کنترل: سیستم اطلاعاتی:

الف. با قفل کردن نشست پس از [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] عدم فعالیت یا در صورت دریافت درخواست از کاربر، از دسترسی بیشتر به سیستم جلوگیری می‌کند؛ و

ب. نشست را در حالت قفل نگه می‌دارد، تا زمانی که کاربر با استفاده از هویت شناخته‌شده و رویه‌های احراز هویت، مجدداً وارد سیستم شود و به آن دسترسی پیدا نماید.

راهنمایی‌های تکمیلی: قفل کردن نشست یک اقدام موقتی است که در صورت غیر فعال بودن کاربر و دور شدن موقتی از سیستم اطلاعاتی بدون خارج شدن از آن انجام می‌شود. قفل کردن نشست در صورتی انجام می‌شود که فعالیت‌های سیستم را بتوان شناسایی کرد. این امر معمولاً در سطح سیستم‌عامل صورت می‌گیرد، اما می‌تواند در سطح برنامه کاربردی نیز رخ دهد. قفل کردن نشست جایگزین مناسبی برای خارج شدن از سیستم اطلاعاتی نیست (مثلاً اگر سازمان از کاربران بخواهد که در پایان روز کاری از سیستم خارج شوند). کنترل مربوطه: AC-7.

کنترل‌های پیشرفته:

(۱) قفل کردن نشست / نمایش تصاویر برای مخفی کردن الگوها

سیستم اطلاعاتی با قفل کردن نشست از طریق نمایش تصاویر قابل مشاهده توسط عموم، اطلاعاتی را که قبلاً قابل مشاهده بوده‌اند مخفی می‌کند.

راهنمایی‌های تکمیلی: تصاویر قابل مشاهده توسط عموم می‌توانند تصاویر استاتیک یا دینامیک باشند. به عنوان مثال، می‌توان به الگوهای مورد استفاده به عنوان اسکرین سیور، تصاویر عکاسی، صفحات تک‌رنگ، ساعت، نشانگر عمر باتری، یا یک صفحه سفید اشاره کرد. هیچ یک از تصاویر مورد استفاده حاوی اطلاعات مهم و حساس نیستند.

مراجع: تفهیم‌نامه OMB 06-16.

اولویت و تخصیص به مجموعه‌های پایه:

P3	انتخاب نشده، اولویت پایین	AC-11(1) اولویت متوسط	AC-11(1) اولویت بالا

AC-12: **اتمام نشست**

کنترل: سیستم اطلاعاتی پس از [اختصاص: شرایط و رویدادهایی که بنا به تعیین سازمان، باعث قطع شدن نشست می‌شوند]، نشست کاربری را به طور خودکار به اتمام می‌رساند.

راهنمایی‌های تکمیلی: در مقابل بخش SC-10 که به اتمام اتصالات شبکه مربوط به نشست‌های ارتباطی می‌پردازد، این کنترل اتمام نشست‌های منطقی آغازشده توسط کاربر را بررسی می‌کند. یک نشست منطقی (برای دسترسی از راه دور، دسترسی شبکه و دسترسی محلی) هنگامی آغاز می‌شود که یک کاربر (یا فرایندی که از سوی وی عمل می‌کند)، به یک سیستم اطلاعاتی سازمان دسترسی پیدا کند. این نشست کاربری را می‌توان بدون اتمام نشست شبکه به اتمام رساند (و بنابراین می‌توان دسترسی کاربر را نیز اتمام داد). اتمام نشست باعث اتمام همه فرایندهای مربوط به نشست منطقی کاربر می‌شود، به جز فرایندهایی که کاربر (یعنی مالک نشست) آن‌ها را به طور خاص به گونه‌ای ایجاد کرده است که پس از اتمام نشست نیز ادامه یابند. شرایط و رویدادهایی که سبب اتمام خودکار نشست می‌شوند عبارتند از غیر فعال بودن کاربر برای مدت زمان تعیین‌شده توسط سازمان، پاسخ‌های هدفمند به انواع خاصی از حوادث، محدویت کاربرد سیستم اطلاعاتی در زمان‌هایی از روز و موار دیگری از این دست. کنترل‌های مربوطه: SC-10, SC-23.

کنترل‌های پیشرفته:

(۱) اتمام نشست / خروج کاربر از سیستم و نمایش پیام

سیستم اطلاعاتی:

(الف) هنگامی که از احراز هویت برای دسترسی به [اختصاص: منابع اطلاعاتی تعیین‌شده توسط سازمان] استفاده شود، امکان خروج از نشست‌های ارتباطی آغازشده توسط کاربر را فراهم می‌آورد؛ و

(ب) پیام‌های خروج را به کاربر نشان می‌دهد که دال بر اتمام نشست‌های ارتباطی احرازهویت‌شده است.

راهنمایی‌های تکمیلی: منابع اطلاعاتی که کاربران از طریق احراز هویت به آن‌ها دسترسی پیدا می‌کنند عبارتند از مواردی همچون وب‌سایت‌ها و خدمات وب حفاظت‌شده توسط گذرواژه، پایگاه‌های داده و ایستگاه‌های کاری محلی. پیام‌های خروج مربوط به دسترسی به صفحات وی را می‌توان مثلاً پس از اتمام نشست‌های احرازهویت‌شده نمایش داد. اما در مورد برخی انواع نشست‌های تعاملی از جمله نشست‌های پروتکل انتقال فایل (FTP)، سیستم‌های اطلاعاتی معمولاً پیام خروج را به عنوان آخرین پیام پیش از اتمام نشست‌ها نمایش می‌دهند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب نشده، اولویت پایین	AC-12 اولویت متوسط	AC-12 اولویت بالا

AC-13: **نظارت و بازبینی – کنترل دسترسی**

[حذف شد: به بخش‌های AC-2 و AU-6 منتقل شد].

AC-14: **اقدامات مجاز بدون نیاز به شناسایی یا احراز هویت**

کنترل: سازمان:

الف. آن دسته از [اختصاص: اقدامات کاربری تعیین‌شده توسط سازمان] را مشخص می‌کند که کاربر می‌تواند بدون نیاز به شناسایی و احراز هویت بر اساس مأموریت و فرایندهای کسب‌وکار سازمان، آن‌ها را انجام دهد؛ و

ب. اقدامات مجاز بدون نیاز به شناسایی یا احراز هویت را مستندسازی می‌کند و دلایل این امر را در طرح امنیتی سیستم اطلاعاتی ذکر می‌نماید.

راهنمایی‌های تکمیلی: این کنترل شرایطی را بررسی می‌کند که در آن‌ها سازمان مجوز اقداماتی را بدون نیاز به شناسایی یا احراز هویت صادر می‌کند. سازمان‌ها در موارد معدودی این مجوز را صادر می‌کنند که از آن جمله می‌توان به هنگامی اشاره کرد که افراد به وب‌سایت‌های عمومی یا سایر سیستم‌های اطلاعاتی فدرال دسترسی پیدا می‌کنند که دسترسی همگانی به آن‌ها آزاد است، هنگامی که افراد از گوشی‌های تلفن خود برای دریافت تماس استفاده می‌کنند، یا هنگامی که رونوشت‌هایی دریافت می‌شوند. سازمان‌ها همچنین فعالیت‌هایی را تعیین می‌کنند که در شرایط عادی نیازمند شناسایی یا احراز هویت هستند، اما ممکن است در شرایط خاصی این الزام کنار گذاشته شود. دور زدن این الزامات مثلاً از طریق یک سوئیچ فیزیکی قابل خواندن توسط نرم‌افزار انجام می‌شود که دستور به دور زدن فرایند ورود می‌دهد و از آن در برابر استفاده تصادفی یا کنترل‌نشده محافظت می‌شود. این کنترل مربوط به شرایطی است که شناسایی و احراز هویت هنوز انجام نشده‌اند، نه شرایطی که شناسایی و احراز هویت پیشتر صورت گرفته‌اند. ممکن است سازمان به این نتیجه برسد که هیچ اقدامی بدون شناسایی و احراز هویت از سوی کاربر قابل انجام نخواهد بود. در این صورت، در عبارت اختصاص به این امر اشاره خواهد شد که هیچ اقدامی بدون شناسایی و احراز هویت قابل انجام نیست. کنترل‌های مربوطه: CP-2, IA-2.

کنترل‌های پیشرفته: وجود ندارد.

(۱) اقدامات مجاز بدون نیاز به شناسایی یا احراز هویت / کاربردهای ضروری
[حذف شد: به بخش AC-14 منتقل شد].

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	AC-14 اولویت پایین	AC-14 اولویت متوسط	AC-14 اولویت بالا

AC-15: **علامت‌گذاری خودکار**

[حذف شد: به بخش MP-3 منتقل شد].

AC-16: **ویژگی‌های امنیتی**

کنترل: سازمان:

الف. ابزارهای برقراری پیوند بین [اختصاص: انواع ویژگی‌های امنیتی تعیین‌شده توسط سازمان] که دارای [اختصاص: ارزش ویژگی‌های امنیتی تعیین‌شده توسط سازمان] هستند را با اطلاعات موجود در حافظه، اطلاعات مورد استفاده در فرایندها و/یا اطلاعات انتقالی فراهم می‌آورد؛

ب. اطمینان حاصل می‌نماید که پیوند بین ویژگی‌های امنیتی و اطلاعات برقرار و حفظ شده است؛

پ. [اختصاص: ویژگی‌های امنیتی تعیین‌شده توسط سازمان] مجاز را برای [اختصاص: سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] برقرار می‌نماید؛ و

ت. [اختصاص: محدوده‌ها یا ارزش‌های تعیین‌شده توسط سازمان] مجاز را برای هر یک از ویژگی‌های امنیتی برقرارشده تعیین می‌نماید.

راهنمایی‌های تکمیلی: اطلاعات به وسیله ساختارهای داده در سیستم‌های اطلاعاتی نشان داده می‌شوند. ساختارهای داده درونی می‌توانند انواع مختلف موجودیت‌های فعال و غیر فعال را نمایندگی کنند. موجودیت‌های فعال که به آن‌ها «subject» نیز گفته می‌شود، معمولاً مرتبط با افراد، دستگاه‌ها یا فرایندهایی هستند که از سوی آن‌ها عمل می‌کنند. موجودیت‌های غیر فعال که به آن‌ها «object» نیز گفته می‌شود، معمولاً مرتبط با ساختارهای داده مانند سوابق، بافرها، جداول، فایل‌ها و پورت‌های ارتباطی هستند. ویژگی‌های امنیتی که نوعی فراداده هستند، ساختارهایی هستند که شاخصه‌های اصلی موجودیت‌های فعال و غیر فعال در زمینه تأمین امنیت اطلاعات را نمایندگی می‌کنند. این ویژگی‌ها ممکن است مرتبط با موجودیت‌های فعالی باشند که قابلیت ارسال و دریافت اطلاعات، برقراری جریان اطلاعات بین موجودیت‌های غیر فعال مختلف یا تغییر وضعیت سیستم اطلاعاتی را دارند. ویژگی‌های مذکور همچنین ممکن است مرتبط با موجودیت‌های غیر فعالی باشند که دربردارنده اطلاعات هستند یا اطلاعات را دریافت می‌کنند. به ارتباط بین ویژگی‌های امنیتی با موجودیت‌های فعال و غیر فعال «پیوستگی» گفته می‌شود. این ارتباط معمولاً شامل تعیین مقدار و نوع ویژگی‌ها است. هنگامی که ویژگی‌های امنیتی با دادها و اطلاعات پیون می‌یابند، امکان اجرای خط‌مشی‌های امنیت اطلاعات برای کنترل دسترسی و کنترل جریان اطلاعات را از طریق فرایندهای سازمان یا سازوکارها و توابع سیستم اطلاعاتی فراهم می‌آورند. محتوا یا مقادیر اختصاص‌یافته به ویژگی‌های امنیتی می‌تواند به طور مستقیم بر توانایی افراد در دسترسی به اطلاعات سازمان تأثیر بگذارد.

سازمان‌ها می‌توانند انواع ویژگی‌های امنیتی مورد نیاز سیستم‌های اطلاعاتی منتخب برای پشتیبانی از مأموریت و توابع کسب‌وکار را تعیین کنند. به صورت بالقوه می‌توان محدوده گسترده‌ای از مقادیر را به ویژگی‌های امنیتی تخصیص داد. علامت‌گذاری انتشار می‌تواند، به عنوان مثال، فقط برای آمریکا، برای ناتو، یا برای NOFRON باشد (انتشار اطلاعات برای ملیت‌های دیگر مجاز نیست). سازمان‌ها با تعیین محدوده‌ها و مقادیر مجاز ویژگی‌های امنیت، اطمینان حاصل می‌نمایند که محدوده‌ها و مقادیر مورد استفاده معنادار و مربوط هستند. منظور از عبارت «برچسب‌گذاری امنیتی»، پیوند دادن ویژگی‌های امنیتی با موجودیت‌های فعال و غیر فعال نمایندگی‌شده توسط ساختارهای داده درون سیستم‌های اطلاعاتی سازمان است، به طوری که امکان اجرای خط‌مشی‌های امنیت اطلاعات را بر اساس فرایندهای سیستم‌های اطلاعاتی فراهم آورد. برچسب‌های امنیتی مواردی از جمله صدور مجوز دسترسی، حفاظت از چرخه عمر داده‌ها، ملیت، اطلاعات پیمانکار و دسته‌بندی اطلاعات بر اساس الزامات قانونی را در بر می‌گیرند. منظور از عبارت «علامت‌گذاری امنیتی»، پیوند دادن ویژگی‌های امنیتی با موجودیت‌های غیر فعال در یک فرمت قابل خواندن توسط انسان است، به طوری که امکان

اجرای خط‌مشی‌های امنیت اطلاعات را بر اساس فرایندهای سازمانی فراهم آورد. مجموعه پایه کنترل‌های امنیتی AC-16، الزامات پیوند ویژگی‌ها بر اساس مقتضیات کاربر را ارائه می‌کند (علامت‌گذاری). کنترل‌های پیشرفته AC-16 نیز الزامات دیگری را در خصوص پیوند ویژگی‌های مبتنی بر سیستم‌های اطلاعاتی ارائه می‌نمایند (برچسب‌گذاری). به عنوان مثال‌هایی از ویژگی‌های امنیتی می‌توان به سطوح دسته‌بندی (محرمانگی) برای موجودیت‌های غیر فعال و سطوح تأییدیه‌های امنیتی (مجوز دسترسی) برای موجودیت‌های فعال اشاره کرد. به عنوان مثالی از ارزش هر دو نوع ویژگی، می‌توان از «فوق سری» نام برد. کنترل‌های مربوطه: AC-3, AC-4, AC-6, AC-21, AU-2, AU-10, SC-16, MP-3.

کنترل‌های پیشرفته:

(۱) علامت‌گذاری خودکار / پیوند پویای ویژگی‌ها

پس از تولید و ترکیب اطلاعات، سیستم اطلاعاتی ویژگی‌های امنیتی را به صورت پویا و بر اساس [اختصاص: خط‌مشی‌های امنیتی تعیین‌شده توسط سازمان] با [اختصاص: موجودیت‌های فعال و غیر فعال تعیین‌شده توسط سازمان] پیوند می‌دهد.

راهنمایی‌های تکمیلی: پیوند پویای ویژگی‌های امنیتی در مواردی به کار می‌آید که مشخصه‌های امنیتی اطلاعات در طول زمان تغییر کنند. دلایلی از جمله مسائل ناشی از تجمیع اطلاعات (یعنی این که مشخصه‌های امنیتی هر یک از عناصر اطلاعاتی متفاوت از مشخصه‌های امنیتی عناصر ترکیبی باشند)، تغییر مجوزهای دسترسی افراد (یعنی اختیارات ویژه) و تغییر دسته‌بندی امنیتی اطلاعات می‌توانند منجر به تغییر ویژگی‌های امنیتی شوند. کنترل مربوطه: AC-4.

(۲) علامت‌گذاری خودکار / تغییر ارزش ویژگی‌ها توسط افراد مجاز

سیستم اطلاعاتی به افراد مجاز (یا فرایندهایی که از سوی آن‌ها عمل می‌کنند) امکان می‌دهد تا ارزش ویژگی‌های امنیتی پیونددادهشده را تغییر دهند.

راهنمایی‌های تکمیلی: محتوای ارزش‌های تخصیص‌دادهشده به ویژگی‌های امنیتی می‌تواند به طور مستقیم بر قابلیت دسترسی به اطلاعات سازمانی توسط افراد تأثیر بگذارد. از این رو، سیستم‌های اطلاعاتی باید بتوانند امکان ایجاد یا تغییر ویژگی‌های امنیتی را صرفاً به افراد مجاز محدود نمایند. کنترل‌های مربوطه: AC-6, AU-2.

(۳) علامت‌گذاری خودکار / تعمیر و نگهداری پیوندهای ویژگی‌ها توسط سیستم اطلاعاتی

سیستم اطلاعاتی پیوند و یکپارچگی [اختصاص: ویژگی‌های امنیتی تعیین‌شده توسط سازمان] با [اختصاص: موجودیت‌های فعال و غیر فعال تعیین‌شده توسط سازمان] را حفظ می‌کند.

راهنمایی‌های تکمیلی: حفظ پیوستگی و یکپارچگی ویژگی‌های امنیتی با موجودیت‌های فعال و غیر فعال باعث می‌شود که بتوان از پیوند ویژگی‌ها به عنوان مبنای پیاده‌سازی خودکار خط‌مشی‌ها استفاده کرد. منظور از پیاده‌سازی خودکار خط‌مشی‌ها، اتخاذ تصمیم در زمینه کنترل دسترس، کنترل جریان اطلاعات و موارد دیگری از این دست است.

(۴) علامت‌گذاری خودکار / پیوند ویژگی‌های امنیتی با افراد مجاز

سیستم اطلاعاتی، از پیوند [اختصاص: ویژگی‌های امنیتی تعیین‌شده توسط سازمان] با [اختصاص: موجودیت‌های فعال و غیر فعال تعیین‌شده توسط سازمان] توسط افراد مجاز (یا فرایندهایی که از سوی آن‌ها عمل می‌کنند) پشتیبانی می‌نماید.

راهنمایی‌های تکمیلی: پشتیبانی سیستم اطلاعاتی می‌تواند این موارد را در بر گیرد: (۱) درخواست از کاربران برای انتخاب ویژگی‌های امنیتی خاصی که قرار است با موجودیت‌های غیر فعال اطلاعاتی خاص پیوند داده شوند؛ (۲) پیاده‌سازی سازوکارهای خودکار برای دسته‌بندی اطلاعات با ویژگی‌های مناسب بر اساس خط‌مشی‌های تعیین‌شده؛ یا (۳) حصول اطمینان از این که ترکیب ویژگی‌های امنیتی انتخاب‌شده، ترکیبی معتبر است. سازمان‌ها در هنگام تعریف رویدادهای قابل ممیزی، اقدام به تولید، پاک کردن و تغییر ویژگی‌های امنیتی می‌کنند.

(۵) علامت‌گذاری خودکار / نمایش ویژگی‌ها روی دستگاه‌های خروجی

سیستم اطلاعاتی ویژگی‌های امنیتی را به شکل قابل خواندن توسط انسان روی هر یک از موجودیت‌های غیر فعال انتقال‌یافته به دستگاه‌های خروجی نمایش می‌دهد تا [اختصاص: دستورالعمل‌های ویژه تعیین‌شده توسط سازمان در زمینه انتشار، مدیریت و توزیع اطلاعات] را با استفاده از [اختصاص: قراردادهای نام‌گذاری استاندارد و قابل خواندن توسط انسان که به وسیله سازمان تعیین شده‌اند] تعیین نماید.

راهنمایی‌های تکمیلی: خروجی‌های سیستم اطلاعاتی شامل مواردی از جمله کاغذ، صفحه نمایش یا موارد دیگری از این دست هستند. دستگاه‌های خروجی سیستم اطلاعاتی نیز مواردی از جمله چاپگرها و نمایشگرهای ویدئویی در ایستگاه‌های رایانه‌ای، لپتاپ‌ها و دستیارهای دیجیتال شخصی را در بر می‌گیرند.

(۶) علامت‌گذاری خودکار / حفظ و نگهداری پیوند ویژگی‌ها توسط سازمان

سازمان به کارکنان خود اجازه می‌دهد تا بر اساس [اختصاص: خط‌مشی‌های امنیتی تعیین‌شده توسط سازمان]، بین [اختصاص: ویژگی‌های امنیتی تعیین‌شده توسط سازمان] و [اختصاص: موجودیت‌های فعال و غیر فعال تعیین‌شده توسط سازمان] پیوند برقرار کنند و این پیوند را حفظ نمایند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته از کارکنان (نه از سیستم اطلاعاتی) می‌خواهد که پیوند بین ویژگی‌های امنیتی و موجودیت‌های فعال و غیر فعال را حفظ نمایند.

(۷) علامت‌گذاری خودکار / تفسیر سازگار ویژگی‌ها

سازمان تفسیر سازگاری از ویژگی‌های امنیتی منتقل‌شده بین مؤلفه‌های توزیع‌شده سیستم اطلاعاتی ارائه می‌کند.

راهنمایی‌های تکمیلی: به منظور اجرای خط‌مشی‌های امنیتی در مؤلفه‌های مختلف سیستم‌های اطلاعاتی توزیع‌شده (مانند سیستم‌های توزیع‌شده مدیریت پایگاه داده، سیستم‌های مبتنی بر کلاد و معماری‌های خدمت‌گرا)، سازمان اقدام به تفسیر سازگار ویژگی‌های امنیتی می‌کند که در تصمیمات مربوط به تحقق جریان و دسترسی به کار گرفته شده‌اند. سازمان‌ها از طریق موافقت‌نامه‌ها و فرایندها، اطمینان حاصل می‌کنند که تمام مؤلفه‌های توزیع‌شده سیستم اطلاعاتی، ویژگی‌های امنیتی را با تفاسیری سازگار در سیستم‌های تحقق دسترسی/جریان استفاده می‌کنند.

(۸) علامت‌گذاری خودکار / فناوری‌ها و شیوه‌های برقراری پیوند

سیستم اطلاعاتی برای پیوند دادن ویژگی‌های امنیتی با اطلاعات، از [اختصاص: فاوری‌ها و شیوه‌های تعیین‌شده توسط سازمان] با [اختصاص: سطوح تضمین تعیین‌شده توسط سازمان] استفاه می‌کند.

راهنمایی‌های تکمیلی: پیوند بین ویژگی‌های امنیتی و اطلاعات درون سیستم اطلاعاتی از جهت تحقق جریان و تحقق دسترسی از اهمیت بالایی برخوردار است. در کنار برقراری این پیوند، می‌توان از شیوه‌ها و فناوری‌های تضمینی مختلفی استفاده کرد. به عنوان مثال، سیستم‌های اطلاعاتی می‌توانند ویژگی‌های امنیتی را به شیوه رمزنگاری و با استفاده از امضای دیجیتال به اطلاعات پیوند دهند و از کلیدهای رمزنگاری پشتیبان حفاظت‌شده توسط دستگاه‌های سخت‌افزاری نیز استفاده کنند (که مرجع اعتماد سخت‌افزاری نامیده می‌شود).

(۹) علامت‌گذاری خودکار / تخصیص مجدد ویژگی‌های امنیتی

سازمان اطمینان حاصل می‌نماید که تخصیص مجدد ویژگی‌های امنیتی پیوندیافته با اطلاعات، تنها از طریق سازوکارهای اعطای مجدد و با استفاده از [اختصاص: شیوه‌ها یا رویه‌های تعیین‌شده توسط سازمان] صورت می‌گیرد.

راهنمایی‌های تکمیلی: سازمان از سازوکارهای اعطای مجدد استفاده می‌کند تا سطح تضمین مورد نیاز فعالیت‌های تخصیص مجدد را تأمین نماید. برای تسهیل فرایند تأیید نیز سازمان اطمینان حاصل می‌نماید که سازوکارهای اعطای مجدد، تک‌منظوره و دارای عملکرد محدود هستند. از آنجا که تخصیص مجدد ویژگی‌های امنیتی می‌تواند بر اجرای خط‌مشی‌های امنیتی (مانند فرایندهای تحقق دسترسی و تحقق جریان) تأثیر بگذارد، باید از سازوکارهای اعطای مجدد قابل اعتماد استفاده کرد تا از صحت عملکرد آن‌ها اطمینان حاصل شود.

(۱۰) علامت‌گذاری خودکار / پیکربندی ویژگی‌ها توسط افراد مجاز

سیستم اطلاعاتی به افراد مجاز این امکان را می‌دهد که نوع و ارزش ویژگی‌های امنیتی موجود برای برقراری پیوند با موجودیت‌های فعال و غیر فعال را تعریف کنند و تغییر دهند.

راهنمایی‌های تکمیلی: محتوای ارزش‌های تخصیص‌یافته به ویژگی‌های امنیتی می‌تواند مستقیماً بر توانایی افراد برای دسترسی به اطلاعات سازمانی تأثیر بگذارد. بنابراین، سیستم‌های اطلاعاتی باید تنها به افراد مجاز امکان دهند که ویژگی‌های امنیتی را ایجاد کنند و تغییر دهند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

AC-17: دسترسی از راه دور

کنترل: سازمان:

الف. محدودیت‌های کاربرد، الزامات اتصال و پیکربندی و نکات مربوط به پیاده‌سازی هر یک از انواع دسترسی از راه دور را تعیین و مستندسازی می‌کند؛ و

ب. پیش از صدور مجوز چنین اتصالاتی، مجوز دسترسی از راه دور به سیستم اطلاعاتی را صادر می‌کند.

راهنمایی‌های تکمیلی: دسترسی از راه دور یعنی دسترسی به سیستم‌های اطلاعاتی سازمان توسط آن دسته از کاربران (یا فرایندهایی که از سوی آن‌ها عمل می‌کنند) که از طریق شبکه‌های خارجی (مانند اینترنت) ارتباط برقرار کرده‌اند. به عنوان مثال‌هایی از روش‌های دسترسی از راه دور می‌توان به اتصالات dial-up، باند پهن و

بی‌سیم اشاره کرد. سازمان‌ها معمولاً برای ارتقای محرمانگی و یکپارچگی در اتصالات راه دور، از شبکه‌های خصوصی مجازی (VPN) رمزگذاری‌شده استفاده می‌کنند. استفاده از VPNهای رمزگذاری‌شده باعث نمی‌شود که دسترسی از حالت راه دور خارج شود؛ اما هنگامی که این شبکه‌ها در کنار کنترل‌های امنیتی مناسب به کار گرفته شوند، این تضمین را به سازمان می‌دهند که می‌تواند با این اتصالات به عنوان شبکه‌های داخلی رفتار کند. با این حال، اتصالات VPN از شبکه‌های خارج از سازمان می‌گذرند و VPN رمزگذاری‌شده، آماده به کار بودن اتصالات راه دور را ارتقا نمی‌دهد. علاوه بر این، VPNهای با تونل‌های رمزگذاری‌شده می‌توانند بر توانایی سازمان در پایش مناسب ترافیک ارتباطی جهت یافتن کدهای مخرب تأثیر بگذارند. کنترل‌های دسترسی از راه دور در سیستم‌های اطلاعاتی به جز سرورهای عمومی وب یا سیستم‌های طراحی‌شده برای دسترسی عمومی، پیاده‌سازی می‌شوند. این کنترل به مقوله صدور مجوز پیش از اجازه‌دهی برای دسترسی از راه دور می‌پردازد و اشاره‌ای به نوع مجوزها نمی‌نماید. ممکن است سازمان‌ها از موافقت‌نامه‌های امنیتی اتصالات بین سازمانی به عنوان مبنای صدور مجوزهای دسترسی استفاده کنند؛ اما موافقت‌نامه‌های مذکور در این کنترل لازم نیستند. محدودیت‌های دسترسی اتصالات راه دور در بخش AC-3 تشریح شده‌اند. کنترل‌های مربوطه: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

کنترل‌های پیشرفته:

(۱) دسترسی از راه دور / کنترل و پایش خودکار

سیستم اطلاعاتی روش‌های دسترسی از راه دور را کنترل و پایش می‌کند.

راهنمایی‌های تکمیلی: کنترل و پایش خودکار نشست‌های دسترسی از راه دور، به سازمان امکان می‌دهد که حملات سایبری را شناسایی کند. سازمان همچنین با ممیزی فعالیت‌های کاربران راه دور روی مؤلفه‌های مختلف سیستم‌های اطلاعاتی مانند سرورها، ایستگاه‌ها، لپتاپ‌ها، گوشی‌های هوشمند و تبلت‌ها، اطمینان حاصل می‌نماید که خط‌مشی‌های دسترسی از راه دور رعایت شده‌اند. کنترل‌های مربوطه: AU-2, AU-12.

(۲) دسترسی از راه دور / حفاظت از محرمانگی و یکپارچگی با استفاده از رمزگذاری

سیستم اطلاعاتی با استفاده از سازوکارهای رمزنگاری، از محرمانگی و یکپارچگی نشست‌های دسترسی از راه دور محافظت می‌کند.

راهنمایی‌های تکمیلی: قدرت امنیتی سازوکارهای مورد استفاده، بر اساس دسته‌بندی امنیتی اطلاعات تعیین می‌شود. کنترل‌های مربوطه: SC-8, SC-12, SC-13.

(۳) دسترسی از راه دور / نقاط کنترل دسترسی مدیریت‌شده

سیستم اطلاعاتی تمام دسترسی‌های از راه دور را از طریق [اختصاص: تعداد تعیین‌شده توسط سازمان] نقطه کنترل دسترسی مدیریت‌شده هدایت می‌نماید.

راهنمایی‌های تکمیلی: محدود کردن تعداد نقاط کنترل دسترسی از راه دور، احتمال حمله به سازمان را کاهش می‌دهد. سازمان‌ها الزامات مربوط به اتصالات اینترنتی مورد اعتماد (TIC) را برای اتصالات خارجی شبکه‌ها مد نظر قرار می‌دهند. کنترل مربوطه: SC-7.

(۴) دسترسی از راه دور / دسترسی و دستورات ویژه

سازمان:

(الف) مجوز اجرای دستورات ویژه و دسترسی از راه دور به اطلاعات امنیتی را تنها در موارد [اختصاص: نیازهای تعیین‌شده توسط سازمان] صادر می‌کند؛ و

(ب) دلیل این دسترسی را در طرح امنیتی سیستم اطلاعاتی مستندسازی می‌کند.

راهنمایی‌های تکمیلی: کنترل مربوطه: AC-6.

(۵) دسترسی از راه دور / پایش اتصالات غیر مجاز

[حذف شد: به بخش SI-4 منتقل شد].

(۶) دسترسی از راه دور / حفاظت از اطلاعات

سازمان اطمینان حاصل می‌نماید که کاربران از اطلاعات مربوط به سازوکارهای دسترسی از راه دور محافظت می‌کنند و از کاربرد و افشای غیر مجاز آن‌ها جلوگیری به عمل می‌آورند.

راهنمایی‌های تکمیلی: کنترل مربوطه: AT-2, AT-3, PS-6.

(۷) دسترسی از راه دور / حفاظت بیشتر از دسترسی به توابع امنیتی

[حذف شد: به بخش AC-3(10) منتقل شد].

(۸) دسترسی از راه دور / غیر فعال کردن پروتکل‌های غیر امن شبکه

[حذف شد: به بخش CM-7 منتقل شد].

(۹) دسترسی از راه دور / قطع کردن و غیر فعال کردن دسترسی

سازمان قابلیت قطع کردن یا غیر فعال کردن دسترسی از راه دور به سیستم اطلاعاتی را [اختصاص: در بازه زمانی تعیین‌شده توسط سازمان] فراهم می‌آورد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته سازمان‌ها را ملزم می‌کند تا قابلیت قطع کردن سریع دسترسی از راه دور توسط کاربران و/یا غیر فعال کردن این دسترسی را داشته باشند. سرعت قطع کردن

یا غیر فعال کردن، به درجه اهمیت مأموریت‌ها و توابع کسب‌وکار و نیاز به غیر فعال کردن امکان دسترسی از راه دور در حال حاضر یا در آینده بستگی دارد.

مراجع: نشریه‌های ویژه شماره ۸۰۰-۴۶، ۸۰۰-۷۷، ۸۰۰-۱۱۳، ۸۰۰-۱۱۴ و ۸۰۰-۱۲۱ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AC-17 اولویت پایین	AC-17(1)(2)(3)(4) اولویت متوسط	AC-17(1)(2)(3)(4) اولویت بالا

AC-18: دسترسی بی‌سیم

کنترل: سازمان:

الف. محدودیت‌های کاربرد، الزامات اتصال و پیکربندی و نکات مربوط به پیاده‌سازی هر یک از انواع دسترسی بی‌سیم را تعیین و مستندسازی می‌کند؛ و

ب. پیش از صدور مجوز چنین اتصالاتی، مجوز دسترسی بی‌سیم به سیستم اطلاعاتی را صادر می‌کند.

راهنمایی‌های تکمیلی: به عنوان مثال‌هایی از فناوری‌های دسترسی بی‌سیم، می‌توان به مایکروویو، رادیو بسته‌ای (UHF/VHF)، 802.11x و بلوتوث اشاره کرد. شبکه‌های بی‌سیم از پروتکل‌های احراز هویت استفاده می‌کنند. این پروتکل‌ها امکان حفاظت از اطلاعات محرمانه و احراز هویت متقابل را فراهم می‌آورند. کنترل‌های مربوطه: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.

کنترل‌های پیشرفته:

(۱) دسترسی بی‌سیم / احراز هویت و رمزگذاری

سیستم اطلاعاتی با استفاده از احراز هویت [انتخاب (یک یا چند مورد): دستگاه‌ها، کاربران] و رمزگذاری، از دسترسی بی‌سیم محافظت می‌کند.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: SC-8, SC-13.

(۲) دسترسی بی‌سیم / پایش اتصالات غیر مجاز

[حذف شد: به بخش SI-4 منتقل شد].

(۳) دسترسی بی‌سیم / غیر فعال کردن امکان شبکه شدن بی‌سیم

در صورتی که به قابلیت شبکه شدن بی‌سیم مؤلفه‌های سیستم اطلاعاتی نیازی نباشد، سازمان این قابلیت را پیش از برقراری و اجرا، غیر فعال می‌نماید.

راهنمایی‌های تکمیلی: کنترل مربوطه: AC-19.

(۴) دسترسی بی‌سیم / محدود کردن امکان پیکربندی توسط کاربران

سازمان کاربرانی که می‌توانند قابلیت شبکه شدن بی‌سیم را به طور مستقل پیکربندی کنند، شناسایی و برای آن‌ها به صورت آشکار صدور مجوز می‌نماید.

راهنمایی‌های تکمیلی: مجوزهای سازمان در خصوص پیکربندی قابلیت شبکه، تا حدی توسط سازوکارهای تحقق دسترسی مورد استفاده در سیستم‌های اطلاعاتی سازمان اجرا می‌شوند. کنترل‌های مربوطه: AC-3, SC-15.

(۵) دسترسی بی‌سیم / آنتن‌ها و سطوح قدرت انتقال

سازمان آنتن‌های رادیویی را انتخاب می‌کند و سطوح قدرت انتقال را به گونه‌ای تنظیم می‌کند که امکان ارسال سیگنال‌هایی به خارج از مرزهای کنترل‌شده توسط سازمان کاهش یابد.

راهنمایی‌های تکمیلی: سازمان می‌تواند اقداماتی را برای محدود کردن استفاده غیر مجاز از ارتباطات بی‌سیم در خارج از مرزهای کنترل‌شده توسط سازمان انجام دهد که از آن جمله می‌توان به این موارد اشاره کرد: (۱) کاهش قدرت ارسال بی‌سیم به گونه‌ای که امکان ارسال سیگنال‌های قابل استفاده توسط متخاصمان خارج از مرزهای فیزیکی سازمان را کاهش دهد؛ (۲) استفاده از شاخص‌هایی از جمله TEMPEST برای کنترل ارسال‌های بی‌سیم؛ و (۳) استفاده از آنتن‌های جهتی/اشعه‌ای که امکان ایجاد تداخل در سیگنال‌ها توسط گیرنده‌های متفرقه را کاهش می‌دهد. پیش از انجام این اقدامات، سازمان‌ها می‌توانند با انجام تحقیقات دوره‌ای، وضعیت فرکانس رادیویی سیستم‌های اطلاعاتی سازمان و سیستم‌های دیگر فعال در ناحیه مورد نظر را بررسی کنند. کنترل مربوطه: PE-19.

مراجع: نشریه‌های ویژه شماره ۸۰۰-۴۸ و ۸۰۰-۹۴ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AC-18 اولویت پایین	AC-18(1) اولویت متوسط	AC-18(1)(4)(5) اولویت بالا

AC-19: **کنترل دسترسی دستگاه‌های همراه**

کنترل: سازمان:

الف. محدودیت‌های کاربرد، الزامات اتصال و پیکربندی و نکات مربوط به پیاده‌سازی دستگاه‌های همراه کنترل‌شده توسط سازمان را تعیین می‌کند؛ و

ب. اجازه اتصال دستگاه‌های همراه به سیستم‌های اطلاعاتی سازمان را صادر می‌نماید.

راهنمایی‌های تکمیلی: منظور از دستگاه همراه، یک دستگاه محاسباتی است که: (۱) اندازه کوچکی دارد و به راحتی توسط یک فرد قابل حمل است؛ (۲) به گونه‌ای طراحی شده است که بدون اتصال فیزیکی کار کند (یعنی اطلاعات را به صورت بی‌سیم دریافت یا ارسال کند)؛ (۳) دارای حافظه محلی قابل جداسازی یا غیر قابل جداسازی است؛ و (۴) دارای یک منبع توان داخلی است. دستگاه‌های همراه ممکن است دارای قابلیت ارتباط صوتی، حسگرهایی برای جمع‌آوری اطلاعات، و/یا ویژگی‌های تعبیه‌شده‌ای برای همزمان‌سازی داده‌های محلی با مکان‌های دوردست باشند. به عنوان مثال‌هایی از دستگاه‌های همراه می‌توان به گوشی‌های هوشمند، تبلت‌ها و مواردی از این دست اشاره کرد. دستگاه‌های همراه معمولاً متعلق به یک فرد هستند و در مجاورت وی قرار دارند؛ اما میزان این مجاورت بسته به نوع دستگاه و اندازه آن متفاوت خواهد بود. قابلیت پردازش، ذخیره‌سازی و انتقال دستگاه‌های همراه قابل مقایسه با سیستم‌های دسکتاپ است؛ که البته میزان دقیق آن به ماهیت و هدف دستگاه بستگی دارد. به دلیل تنوع دستگاه‌های همراه و ویژگی‌های متفاوت آن‌ها، محدودیت‌های سازمانی مربوط به آن‌ها نیز با هم تفاوت خواهند داشت. به عنوان مثالی از محدودیت‌های کاربرد و راهنمایی‌های پیاده‌سازی دستگاه‌های همراه می‌توان به مدیریت پیکربندی، شناسایی و احراز هویت دستگاه، استفاده از نرم‌افزارهای حفاظتی اجباری (مانند فایروال‌ها و نرم‌افزارهای شناسایی کدهای مخرب)، اسکن کردن دستگاه‌ها برای شناسایی کدهای مخرب، به‌روزرسانی آنتی‌ویروس‌ها، جستجوی بسته‌های به‌روزرسانی مهم، آزمون یکپارچگی سیستم عامل (یا سایر نرم‌افزارهای نصب‌شده) و غیر فعال کردن سخت‌افزارهای غیر ضروری (مانند سخت‌افزارهای مربوط به قابلیت بی‌سیم و مادون قرمز) اشاره کرد. به سازمان‌ها یادآوری می‌شود که ممکن است برای تأمین امنیت دستگاه‌های همراه به نحو مقتضی، نیاز به ابزارهای امنیتی دیگری به جز آنچه در این کنترل ذکر شده است نیز داشته باشند. بسیاری از ابزارهای تضمینی و امنیتی دستگاه‌های همراه در سایر کنترل‌های امنیتی کاتالوگ به عنوان بخشی از مجموعه‌های کنترل پایه ذکر شده‌اند. ممکن است همپوشانی‌هایی نیز بین کنترل‌های امنیتی مورد اشاره در خانواده‌های مختلف وجود داشته باشد. کنترل AC-20 به آن دسته از دستگاه‌های همراه می‌پردازد که توسط سازمان کنترل نمی‌شوند. کنترل‌های مربوطه: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.

کنترل‌های پیشرفته:

(۱) کنترل دسترسی دستگاه‌های همراه / استفاده از حافظه‌های قابل حمل و قابل نوشتن
[حذف شد: به بخش MP-7 منتقل شد].

(۲) کنترل دسترسی دستگاه‌های همراه / استفاده از حافظه‌های قابل حمل شخصی
[حذف شد: به بخش MP-7 منتقل شد].

(۳) کنترل دسترسی دستگاه‌های همراه / استفاده از حافظه‌های قابل حملی که مالک آن‌ها معلوم نیست
[حذف شد: به بخش MP-7 منتقل شد].

(۴) کنترل دسترسی دستگاه‌های همراه / محدودیت‌های مربوط به اطلاعات محرمانه
سازمان:

(الف) استفاده از دستگاه‌های همراه غیر محرمانه در تأسیساتی که سیستم‌های اطلاعاتی آن‌ها مشغول پردازش، ذخیره‌سازی یا انتقال اطلاعات محرمانه هستند را ممنوع می‌کند، مگر این که اجازه این کار به طور ویژه توسط مقامات داده شده باشد؛ و

(ب) در خصوص افراد مجاز به استفاده از دستگاه‌های همراه غیر محرمانه در تأسیساتی که سیستم‌های اطلاعاتی آن‌ها مشغول پردازش، ذخیره‌سازی یا انتقال اطلاعات محرمانه هستند، محدودیت‌های زیر را اعمال می‌نمایند:

(۱) اتصال دستگاه‌های همراه غیر محرمانه به سیستم‌های اطلاعاتی محرمانه ممنوع است؛

(۲) اتصال دستگاه‌های همراه غیر محرمانه به سیستم‌های اطلاعاتی غیر محرمانه نیازمند تأیید مقامات مربوطه است؛

(۳) استفاده از واسط‌های بی‌سیم یا مودم‌های داخلی یا خارجی در دستگاه‌های همراه غیر محرمانه ممنوع است؛ و

(۴) دستگاه‌های همراه غیر محرمانه و اطلاعات ذخیره‌شده روی آن‌ها به طور تصادفی توسط [اختصاص: مقامات امنیتی تعیین‌شده توسط سازمان] بازبینی و بازرسی می‌شوند و اگر اطلاعات محرمانه‌ای مشاهده شود، به خط‌مشی مدیریت حوادث رجوع می‌گردد.

(پ) اتصال دستگاه‌های همراه محرمانه به سیستم‌های اطلاعاتی محرمانه را بر اساس [اختصاص: خط‌مشی امنیتی تعیین‌شده توسط سازمان] محدود می‌کند.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: CA-6, IR-4.

(۵) کنترل دسترسی دستگاه‌های همراه / رمزگذاری کل دستگاه یا رمزگذاری مبتنی بر حافظه

سازمان با استفاده از [انتخاب: رمزگذاری کل دستگاه، رمزگذاری حافظه]، از محرمانگی و یکپارچگی اطلاعات روی [اختصاص: دستگاه‌های همراه تعیین‌شده توسط سازمان] محافظت می‌کند.

راهنمایی‌های تکمیلی: رمزگذاری مبتنی بر حافظه رویکرد بهتری را برای رمزگذاری داده‌ها و اطلاعات روی دستگاه‌های همراه در اختیار سازمان قرار می‌دهد. به عنوان مثال، می‌توان ساختارهای داده خاصی مانند فایل‌ها، سوابق یا فیلدها را رمزگذاری کرد. کنترل‌های مربوطه: MP-5, SC-13, SC-28.

مراجع: تفهیم‌نامه OMB 06-16؛ نشریه‌های ویژه شماره ۱۱۴-۸۰۰، ۱۲۴-۸۰۰ و ۱۶۴-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AC-19 اولویت پایین	AC-19(5) اولویت متوسط	AC-19(5) اولویت بالا

AC-20: استفاده از سیستم‌های اطلاعاتی خارج از سازمان

کنترل: سازمان در راستای روابط اعتمادآمیز خود با سازمان‌هایی که سیستم‌های اطلاعاتی خارجی را دارا هستند، اجرا می‌کنند و/یا تعمیر و نگهداری می‌نمایند، شرایط و ضوابطی را تعیین می‌کند که به برخی افراد اجازه دهد تا:

الف. از طریق سیستم‌های اطلاعاتی خارج از سازمان، به سیستم اطلاعاتی دسترسی پیدا کنند؛ و

ب. اطلاعات کنترل‌شده توسط سازمان را با استفاده از سیستم‌های اطلاعاتی خارج از سازمان، پردازش، ذخیره یا منتقل کنند.

راهنمایی‌های تکمیلی: سیستم‌های اطلاعاتی خارج از سازمان آن دسته از سیستم‌های اطلاعاتی و مؤلفه‌های آن‌ها هستند که خارج از مرزهای اختیار سازمان قرار دارند و سازمان هیچ نظارت مستقیمی بر اجرای کنترل‌های امنیتی در آن‌ها ندارد و نمی‌تواند اثربخشی کنترل‌های آن‌ها را بررسی کند. سیستم‌های اطلاعاتی خارج از سازمان مواردی از این دست را در بر می‌گیرند: (۱) دستگاه‌ها و سیستم‌های اطلاعاتی با مالکیت شخصی (مانند لپتاپ‌ها، گوشی‌های هوشمند، تبلت‌ها و دستیارهای دیجیتالی شخصی)؛ (۲) دستگاه‌های ارتباطی و محاسباتی با مالکیت خصوصی که در تأسیسات عمومی یا تجاری مانند هتل‌ها، ایستگاه‌های راه آهن، بازارها یا فرودگاه‌ها استفاده می‌شوند؛ (۳) سیستم‌های اطلاعاتی تحت مالکیت یا کنترل سازمان‌های دولتی غیر

فدرال؛ و (۴) سیستم‌های اطلاعاتی فدرال که تحت مالکیت، عملکرد، اختیار یا نظارت مستقیم سازمان نیستند. این کنترل همچنین به استفاده از سیستم‌های اطلاعاتی خارج از سازمان برای پردازش، ذخیره‌سازی و انتقال اطلاعات سازمان نیز می‌پردازد.

در مورد برخی از سیستم‌های اطلاعاتی خارج از سازمان (مانند سیستم‌های اطلاعاتی که توسط سایر آژانس‌های فدرال و سازمان‌های تابعه آن‌ها پیاده‌سازی می‌شوند)، ممکن است روابط اعتماد آمیز بین دو طرف به گونه‌ای باشد که هیچ شرایط و ضوابطی در نظر گرفته نشده باشد. سیستم‌های اطلاعاتی این سازمان‌ها جزء سیستم‌های اطلاعاتی خارج از سازمان به شمار نمی‌آیند. به عنوان مثال، ممکن است موافقت‌نامه‌های اشتراک‌گذاری یا اعتماد از پیش به طور آشکار یا ضمنی بین آژانس‌ها تنظیم شده باشد یا این که این موافقت‌نامه‌ها بر اساس قوانین، دستورات، رهنمودها و خط‌مشی‌ها به امضا رسیده باشند. افراد مجاز می‌توانند شامل کارکنان سازمان، پیمانکارها یا سایر افرادی باشند که حق دسترسی به سیستم‌های اطلاعاتی سازمان را دارند و سازمان می‌تواند رفتار آن‌ها در زمینه دسترسی به این سیستم‌ها را مدیریت کند و قوانینی برای آن‌ها تنظیم نماید. محدودیت‌هایی که سازمان برای این افراد در نظر می‌گیرد الزاماً یکسان نیستند و این محدودیت‌ها می‌توانند متأثر از روابط اعتمادآمیز بین سازمان‌ها باشند. بنابراین، ممکن است سازمان‌ها محدودیت‌های امنیتی مختلفی را برای پیمانکاران، فرمانداری‌ها، شهرداری‌ها و مقامات کشوری در نظر گیرند.

این کنترل، در مورد استفاده از سیستم‌های اطلاعاتی خارج از سازمان برای دسترسی به واسطهای عمومی جهت دست یافتن به سیستم‌های اطلاعاتی سازمان صدق نمی‌کند (مثلاً افرادی که از طریق www.usa.gov به اطلاعات فدرال دست پیدا می‌کنند). در این موارد، سازمان‌ها با توجه به رویه‌ها و خط‌مشی‌های امنیتی خود، شرایط و ضوابطی را تعیین می‌نمایند. این شرایط و ضوابط، دست کم موارد روبرو را در بر می‌گیرند: انواع برنامه‌های کاربردی روی سیستم‌های اطلاعاتی خارج از سازمان که می‌توان از طریق سیستم‌های اطلاعاتی سازمان به آن‌ها دست یافت؛ و بالاترین دسته امنیتی اطلاعات که می‌توان روی سیستم‌های اطلاعاتی خارج از سازمان پردازش، ذخیره یا منتقل کرد. اگر سازمان‌ها نتوانند شرایط و ضوابط مذکور را با مالکان سیستم‌های اطلاعاتی خارج از سازمان تنظیم نمایند، ممکن است محدودیت‌هایی را برای آن دسته از کارکنان خود در نظر بگیرند که از این سیستم‌های خارجی استفاده می‌کنند. کنترل‌های مربوطه: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.

کنترل‌های پیشرفته:

(۱) استفاده از سیستم‌های اطلاعاتی خارج از سازمان / محدودیت‌های استفاده مجاز

سازمان تنها در صورتی به افراد مجاز امکان می‌دهد تا از سیستم‌های اطلاعاتی خارج از سازمان برای دسترسی به سیستم اطلاعاتی یا پردازش، ذخیره‌سازی یا انتقال اطلاعات تحت کنترل سازمان استفاده کنند که فعالیت‌های زیر را انجام داده باشد:

(الف) تأیید پیاده‌سازی کنترل‌های امنیتی ضروری روی سیستم‌های اطلاعاتی خارج از سازمان بر اساس طرح امنیتی و خط‌مشی امنیت اطلاعات سازمان؛ یا

(ب) حفظ موافقت‌نامه‌های تأییدشده پردازش یا اتصال سیستم اطلاعاتی با آن دسته از موجودیت‌های سازمان که سیستم‌های اطلاعاتی خارج از سازمان را میزبانی می‌کنند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته توجه دارد که در برخی شرایط، افرادی که از سیستم‌های اطلاعاتی خارج از سازمان استفاده می‌کنند (مانند پیمانکاران یا شرکای ائتلاف)، نیز دارند که به سیستم‌های اطلاعاتی سازمان دسترسی داشته باشند. در این شرایط، سازمان‌ها باید اطمینان حاصل نمایند که سیستم‌های اطلاعاتی خارج از سازمان از کنترل‌های امنیتی لازم استفاده می‌کنند و خطر یا خسارتی متوجه سیستم‌های اطلاعاتی سازمان نیست. تأیید پیاده‌سازی این کنترل‌های امنیتی توسط شخص ثالث، بازرسان مستقل، شاهدان یا ازطریق ابزارهای دیگر انجام می‌شود. این امر به سطح اعتماد تعیین‌شده توسط سازمان بستگی دارد. کنترل مربوطه: CA-2.

(۲) استفاده از سیستم‌های اطلاعاتی خارج از سازمان / حافظه‌های قابل حمل

سازمان استفاده از حافظه‌های قابل حمل تحت کنترل سازمان توسط افراد مجاز در سیستم‌های اطلاعاتی خارج از سازمان را [انتخاب: محدود می‌کند، ممنوع می‌کند].

راهنمایی‌های تکمیلی: به عنوان نمونه‌هایی از محدودیت‌های اعمالی، ممکن است استفاده از این دستگاه‌ها به طور کلی ممنوع شود یا محدودیت‌هایی در زمینه چگونگی و شرایط استفاده از آن‌ها تعیین گردد.

(۳) استفاده از سیستم‌های اطلاعاتی خارج از سازمان / دستگاه‌ها، مؤلفه‌ها و سیستم‌هایی که تحت مالکیت سازمان نیستند

سازمان استفاده از دستگاه‌ها، مؤلفه‌ها و سیستم‌های با مالکیت غیر سازمانی برای پردازش، ذخیره‌سازی یا انتقال اطلاعات سازمان را [انتخاب: محدود می‌کند، ممنوع می‌کند].

راهنمایی‌های تکمیلی: منظور از دستگاه‌های با مالکیت غیر سازمانی، دستگاه‌هایی است که تحت مالکیت سایر سازمان‌ها (از جمله پیمانکاران و آژانس‌های فدرال) یا تحت مالکیت اشخاص هستند.

استفاده از این دستگاه‌ها مخاطراتی را به همراه خواهد داشت. در برخی موارد، این مخاطرات به اندازه‌ای هستند که سازمان استفاده از دستگاه‌ها را به طور کلی ممنوع می‌کند. در برخی موارد دیگر نیز مخاطرات کمتر هستند و محدودیت‌هایی برای استفاده از این دستگاه‌ها در نظر گرفته می‌شود. به عنوان مثال‌هایی از این محدودیت‌ها می‌توان به موارد روبرو اشاره کرد: (۱) الزام به پیاده‌سازی کنترل‌های امنیتی مورد تأیید سازمان پیش از صدور مجوز برقراری اتصال؛ (۲) محدود کردن دسترسی به انواع خاصی از اطلاعات، خدمات یا برنامه‌های کاربردی؛ (۳) استفاده از شیوه‌های مجازی‌سازی برای این که تنها سرورها و سایر مؤلفه‌ای مورد تأیید سازمان بتوانند پردازش و ذخیره‌سازی را انجام دهند؛ و (۴) موافقت با شرایط و ضوابط استفاده. در مورد دستگاه‌های با مالکیت شخصی، سازمان‌ها با دفتر مشاوره عمومی در خصوص موارد قانونی استفاده از این دستگاه‌ها در محیط‌های عملیاتی همفکری می‌کنند؛ به عنوان مثال، الزامات تحلیل‌های جرم‌شناسی در جریان بررسی حوادث امنیتی را مرور می‌کنند.

(۴) استفاده از سیستم‌های اطلاعاتی خارج از سازمان / حافظه‌های قابل دسترس از طریق شبکه

سازمان استفاده از [اختصاص: حافظه‌های قابل دسترس از طریق شبکه که توسط سازمان تعیین شده‌اند] در سیستم‌های اطلاعاتی خارج از سازمان را ممنوع می‌کند.

راهنمایی‌های تکمیلی: به عنوان مثال‌هایی از حافظه‌های قابل دسترس از طریق شبکه، می‌توان به دستگاه‌های ذخیره‌سازی آنلاین در سیستم‌های عمومی، هیبریدی یا انجمنی مبتنی بر کلاد اشاره کرد.

مراجع: نشریه FIPS 199.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AC-20 اولویت پایین	AC-20(1) اولویت متوسط	AC-20(1)(2) اولویت بالا

AC-21: اشتراک‌گذاری اطلاعات

کنترل: سازمان:

الف. کاربران مجاز را قادر می‌سازد تا تطبیق مجوز دسترسی طرف اشتراک‌گذارنده اطلاعات با محدودیت‌های دسترسی در [اختصاص: شرایط تعیین‌شده توسط سازمان در زمینه اشتراک‌گذاری اطلاعات که در آن‌ها نیاز به نظر کاربر است] را تأیید کنند و بدین ترتیب، اشتراک‌گذاری اطلاعات را تسهیل نمایند.

ب. برای کمک به کاربران در اتخاذ تصمیمات مربوط به همکاری و اشتراک‌گذاری اطلاعات، از [اختصاص: فرایندهای دستی و سازوکارهای خودکار تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: این کنترل درباره اطلاعاتی است که به دلایلی بر اساس مقررات اداری و رسمی، محدود شده‌اند. از جمله این اطلاعات می‌توان به اطلاعات درمانی ویژه، اطلاعات حساس قرارداد، اطلاعات اختصاصی، اطلاعات شناسایی شخصی و اطلاعات محرمانه مربوط به برنامه‌های دسترسی خاص اشاره کرد. بسته به شرایط اشتراک‌گذاری اطلاعات، ممکن است طرفین در سطح فردی، گروهی یا سازمانی تعریف شوند. اطلاعات نیز می‌توانند بر اساس محتوا، نوع، دسته امنیتی یا برنامه‌های دسترسی خاص تقسیم‌بندی شوند. کنترل مربوطه: AC-3.

کنترل‌های پیشرفته:

(۱) اشتراک‌گذاری اطلاعات / پشتیبانی خودکار از تصمیمات

سیستم اطلاعاتی تصمیمات مربوط به اشتراک‌گذاری اطلاعات توسط کاربران مجاز را بر اساس مجوزهای دسترسی طرفین و محدودیت‌های دسترسی به اطلاعات مورد نظر، اجرا می‌نماید.

(۲) اشتراک‌گذاری اطلاعات / جستجو و بازیابی اطلاعات

سیستم اطلاعاتی خدمات جستجو و بازیابی اطلاعات را پیاده‌سازی می‌نماید که مبنای اجرای [اختصاص: محدودیت‌های تعیین‌شده توسط سازمان در زمینه اشتراک‌گذاری اطلاعات] هستند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب نشده، اولویت پایین	AC-21 اولویت متوسط	AC-21 اولویت بالا

AC-22: **محتوای قابل دسترسی توسط عموم**

کنترل: سازمان:

الف. افرادی که می‌توانند اطلاعات را در سیستم‌های اطلاعاتی قابل دسترسی توسط عموم قرار دهند، تعیین می‌نماید؛

ب. افراد مجاز را آموزش می‌دهد تا اطمینان حاصل نماید که اطلاعات قابل دسترسی توسط عموم شامل اطلاعات غیر عمومی نیستند؛

پ. محتوای پیشنهادی را پیش از قرار گرفتن در سیستم‌های اطلاعاتی قابل دسترسی توسط عموم بازبینی می‌کند تا اطمینان حاصل نماید که شامل اطلاعات غیر عمومی نیستند؛ و

ت. محتوای سیستم‌های اطلاعاتی قابل دسترسی توسط عموم را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند و در صورت یافتن اطلاعات غیر عمومی، این اطلاعات را پاک می‌کند.

راهنمایی‌های تکمیلی: بر اساس راهنمایی‌ها، استانداردها، مقررات، خط‌مشی‌ها، رهنمودها، دستورات اجرایی و قوانین فدرال، عموم مردم اجازه ندارند به اطلاعات غیر عمومی دسترسی داشته باشند. این کنترل برای آن دسته از سیستم‌های اطلاعاتی است که تحت کنترل سازمان قرار دارند و قابل دسترسی توسط عموم هستند (معمولاً بدون نیاز به شناسایی و احراز هویت). قرار دادن اطلاعات در سیستم‌های اطلاعاتی غیر سازمانی، بر اساس خط‌مشی‌های سازمان مدیریت می‌شوند. کنترل‌های مربوطه: AC-3, AC-4, AT-2, AT-3, AU-13.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	AC-22 اولویت پایین	AC-22 اولویت متوسط	AC-22 اولویت بالا

AC-23: **جلوگیری از داده‌کاوی**

کنترل: سازمان با استفاده از [اختصاص: شیوه‌های تعیین‌شده توسط سازمان برای شناسایی و جلوگیری از داده‌کاوی] برای [اختصاص: موجودیت‌های ذخیره‌سازی تعیین‌شده توسط سازمان]، موارد داده‌کاوی را شناسایی می‌کند و از آن‌ها جلوگیری به عمل می‌آورد.

راهنمایی‌های تکمیلی: به عنوان مثال‌هایی از موجودیت‌های ذخیره‌سازی می‌توان به پایگاه‌های داده، سوابق پایگاه‌های داده و فیلدهای پایگاه‌های داده اشاره کرد. شیوه‌های شناسایی و جلوگیری از داده‌کاوی نیز مواردی از این دست را در بر می‌گیرند: (۱) محدود کردن انواع پاسخ‌های ارائه‌شده به کوئری‌های پایگاه داده؛ (۲) محدود

کردن تعداد و فراوانی کوئری‌های پایگاه داده برای افزایش عامل کار[۱۵۴] مورد نیاز برای تعیین محتوای این پایگاه‌های داده؛ و (۳) اطلاع‌رسانی به کارکنان سازمان در مواقع رخ دادن دسترسی‌ها یا کوئری‌های غیر معمول در پایگاه‌های داده. این کنترل به دنبال حفاظت از اطلاعات سازمانی ذخیره‌شده در مخازن داده سازمان در برابر داده‌کاوی است. در مقابل، کنترل AU-13 به پایش آن دسته از اطلاعات سازمانی می‌پردازد که ممکن است کاوش شده یا به روش دیگری از مخازن داده سازمان به دست آمده باشند، و اکنون به عنوان منابع آزاد اطلاعات در وب‌سایت‌های خارجی از جمله شبکه‌های اجتماعی قرار گرفته باشند.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

AC-24: **تصمیمات کنترل دسترسی**

کنترل: سازمان با استفاده از رویه‌های مناسب اطمینان حاصل می‌کند که پیش از تحقق دسترسی، [اختصاص: تصمیمات کنترل دسترسی تعیین‌شده توسط سازمان] در تمامی موارد درخواست‌های دسترسی اعمال شده‌اند.

راهنمایی‌های تکمیلی: تصمیمات کنترل دسترسی (که به آن‌ها تصمیمات صدور مجوز نیز گفته می‌شود) هنگامی رخ می‌دهند که اطلاعات مربوط به صدور مجوز به موارد دسترسی خاص اعمال می‌شوند. در مقابل، تحقق دسترسی هنگامی اتفاق می‌افتد که سیستم‌های اطلاعاتی تصمیمات کنترل دسترسی را پیاده‌سازی می‌کنند. هرچند بسیار مرسوم است که تصمیمات کنترل دسترسی و تحقق دسترسی توسط یک موجودیت واحد پیاده‌سازی شوند، این امر ضروری نیست و در تمامی شرایط نیز بهترین گزینه به شمار نمی‌آید. در برخی از معماری‌ها و سیستم‌های اطلاعاتی توزیع‌شده، ممکن است موجودیت‌های مختلف تصمیمات کنترل دسترسی و تحقق دسترسی را به روش‌های مختلف پیاده‌سازی نمایند.

کنترل‌های پیشرفته:

[154] work factor

(۱) تصمیمات کنترل دسترسی / ارسال اطلاعات مجوز دسترسی

سیستم اطلاعاتی [اختصاص: اطلاعات مجوز دسترسی تعیین‌شده توسط سازمان] را با استفاده از [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] به [اختصاص: سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] که تصمیمات کنترل دسترسی را اجرا می‌کنند، ارسال می‌نماید.

راهنمایی‌های تکمیلی: در سیستم‌های اطلاعاتی توزیع‌شده، ممکن است فرایندهای صدور مجوز و تصمیمات کنترل دسترسی در بخش‌های مختلفی از این سیستم‌ها رخ دهند. در این شرایط، اطلاعات صدور مجوز به صورت امن به منتقل می‌شوند تا بتوان تصمیمات کنترل دسترسی را به شکل به‌هنگام و در مکان مناسب اجرا نمود. برای پشتیبانی از تصمیمات کنترل دسترسی، ممکن است لازم باشد که ویژگی‌های امنیتی نیز به همراه اطلاعات مجوز دسترسی ارسال شوند. این امر بدین دلیل است که در سیستم‌های اطلاعاتی توزیع‌شده، تصمیمات کنترل دسترسی مختلفی را باید اتخاذ نمود و موجودیت‌های مختلفی (از جمله خدمات) که این تصمیمات را به صورت متوالی اتخاذ می‌کنند، هر یک نیاز به برخی ویژگی‌های امنیتی برای اتخاذ تصمیم خود دارند. با حفاظت از اطلاعات مجوز دسترسی (یعنی تصمیمات کنترل دسترسی) می‌توان اطمینان حاصل نمود که این اطلاعات تغییر نمی‌کنند، سرقت نمی‌شوند یا به هر طریق دیگری در معرض خطر قرار نمی‌گیرند.

(۲) تصمیمات کنترل دسترسی / آشکار نشدن هویت کاربران یا فرایندها

سیستم اطلاعاتی تصمیمات کنترل دسترسی را بر اساس [اختصاص: ویژگی‌های امنیتی تعیین‌شده توسط سازمان] اجرا می‌کند، به نحوی که هویت کاربر یا فرایندی که از سوی وی عمل می‌کند، آشکار نگردد.

راهنمایی‌های تکمیلی: در برخی شرایط خاص، لازم است که تصمیمات کنترل دسترسی بدون مشخص شدن هویت کاربران درخواست‌دهنده اتخاذ شوند. این موارد معمولاً حالت‌هایی هستند که در آن‌ها حفظ حریم خصوصی افراد از اهمیت بالایی برخوردار است. در برخی موارد نیز برای اتخاذ تصمیمات کنترل دسترسی به اطلاعات هویتی نیاز نیست و به ویژه در مورد سیستم‌های اطلاعاتی توزیع‌شده، ممکن است ارسال امن و تضمین‌شده این اطلاعات بسیار پرهزینه یا دشوار باشد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

AC-25: **پایش مرجع**

کنترل: سیستم اطلاعاتی پایش مرجع [اختصاص: خط‌مشی‌های کنترل دسترسی تعیین‌شده توسط سازمان] را به شکلی انجام می‌دهد که ضد سرقت، همواره فراخوانی‌شده[155] و به اندازه‌ای کوچک باشد که بتوان آن را تحلیل و آزمون کرد و از تکمیل آن اطمینان حاصل نمود.

راهنمایی‌های تکمیلی: اطلاعات به وسیله ساختارهای داده در سیستم‌های اطلاعاتی نشان داده می‌شوند. ساختارهای داده درونی می‌توانند انواع مختلف موجودیت‌های فعال و غیر فعال را نمایندگی کنند. موجودیت‌های فعال که به آن‌ها «subject» نیز گفته می‌شود، معمولاً مرتبط با افراد، دستگاه‌ها یا فرایندهایی هستند که از سوی آن‌ها عمل می‌کنند. موجودیت‌های غیر فعال که به آن‌ها «object» نیز گفته می‌شود، معمولاً مرتبط با ساختارهای داده مانند سوابق، بافرها، جداول، فایل‌ها و پورت‌های ارتباطی هستند. پایش مرجع معمولاً خط‌مشی‌های اجباری کنترل دسترسی را اجرا می‌کند. این نوع کنترل دسترسی، دسترسی به موجودیت‌های غیر فعال را بر اساس هویت موجودیت‌های فعال یا گروه‌هایی که به آن تعلق دارند، محدود می‌نماید. این کنترل‌های دسترسی به این دلیل اجباری هستند که موجودیت‌های فعال دارای برخی امتیازات ویژه خاص (یعنی مجوز دسترسی) نمی‌توانند امتیازات خود را به طور مستقیم یا غیر مستقیم به موجودیت‌های فعال دیگر منتقل کنند؛ بدین معنی که سیستم اطلاعاتی خط‌مشی کنترل دسترسی را بر اساس مجموعه قوانین برگرفته از این خط‌مشی به طور دقیق اجرا می‌نماید. ویژگی «ضد سرقت بودن» پایش مرجع سبب می‌شود که مهاجمان نتوانند عملکرد سازوکار را به خطر اندازند. ویژگی «همواره فراخوانی‌شده» نیز مانع از این می‌شود که مهاجمان، سازوکار را دور بزنند و خط‌مشی امنیتی را نقض نمایند. ویژگی «کوچک بودن» نیز کمک می‌کند که تحلیل و آزمون سازوکار به طور کامل انجام شود و معایب و نقاط ضعفی که از اجرای خط‌مشی امنیتی جلوگیری می‌کنند، شناسایی گردند. کنترل‌های مربوطه: AC-3, AC-16, SC-3, SC-39.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

[155] always invoked

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

خانواده: آموزش و آگاهی‌رسانی

AT-1: **خط‌مشی و رویه‌های** آموزش و آگاهی‌رسانی

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۳. خط‌مشی آموزش و آگاهی‌رسانی شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و
۴. رویه‌های تسهیل پیاده‌سازی خط‌مشی آموزش و آگاهی‌رسانی و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] مرور و به‌روز می‌کند:

۳. خط‌مشی آموزش و آگاهی‌رسانی امنیتی؛ و
۴. رویه‌های آموزش و آگاهی‌رسانی امنیتی.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل های خانواده AT را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. استراتژی مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: شماره‌های ویژه NIST 800-12, 800-16, 800-50, 800-100.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AT-1 اولویت پایین	AT-1 اولویت متوسط	AT-1 اولویت بالا

AT-2: **آموزش آگاهی‌رسانی امنیتی**

کنترل: سازمان بدین ترتیب آموزش‌های امنیتی را به کاربران سیستم اطلاعاتی از جمله مدیران، مدیران اجرایی ارشد و پیمانکاران ارائه می‌کند:

الف. به عنوان بخشی از آموزش اولیه کاربران جدید؛

ب. هنگامی که این آموزش‌ها در اثر تغییر سیستم اطلاعاتی لازم شوند؛ و

پ. پس از [اختصاص: بازه زمانی تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: سازمان‌ها بر اساس الزامات خاص خود و همچنین با توجه به سیستم‌های اطلاعاتی که کارکنان به آن‌ها دسترسی دارند، محتوای روش‌های آگاهی‌رسانی امنیتی را تعیین می‌نمایند. این محتوا شامل درک اولیه‌ای از نیازهای سازمان در زمینه امنیت اطلاعات و همچنین اقداماتی است که کاربران باید برای حفظ امنیت و مواجهه با رخدادهای مشکوک انجام دهند. این محتوا همچنین باید به گونه‌ای باشد که آگاهی لازم را در زمینه نیاز به امنیت در سازمان ایجاد کند. از جمله روش‌های آگاهی‌رسانی امنیتی می‌توان به نمایش پوستر، ارائه اقلامی که نکات امنیتی در آن‌ها گنجانده شده است، ارسال ایمیل‌هایی از سوی مدیران ارشد سازمان، نمایش پیام‌هایی روی صفحه نمایشگر کارکنان در هنگام ورود به سیستم، و انجام اقداماتی برای آگاهی‌رسانی در زمینه امنیت اطلاعات اشاره کرد. کنترل‌های مربوطه: AT-3, AT-4, PL-4.

کنترل پیشرفته:

(۱) آگاهی‌رسانی امنیتی / تمرین‌های عملی

سازمان در روش‌های آگاهی‌رسانی امنیتی خود برخی تمرین‌های عملی را برای کارکنان در نظر می‌گیرد و در این تمرین‌ها، حملات سایبری واقعی را شبیه‌سازی می‌کند.

راهنمایی‌های تکمیلی: تمرین‌های عملی شامل مواردی از جمله شبیه‌سازی روش‌های مهندسی اجتماعی برای جمع‌آوری اطلاعات، دسترسی غیرمجاز، و تأثیرات منفی باز کردن پیوست‌های مخرب

ایمیل‌ها یا فراخوانی لینک‌های مخرب ایمیلی از طریق حملات فیشینگ است. کنترل‌های مربوطه: CA-2, CA-7, CP-4, IR-3.

(۲) آگاهی‌رسانی امنیتی / تهدیدات داخلی

سازمان‌ها آموزش‌هایی را برای آگاهی‌رسانی امنیتی ترتیب می‌دهند تا کارکنان بتوانند نشانه‌های بالقوه تهدیدات داخلی را شناسایی کنند و گزارش دهند.

راهنمایی‌های تکمیلی: از جمله نشانه‌های بالقوه تهدیدات داخلی می‌توان به رفتارهایی از جمله نارضایتی شغلی بیش از حد و طولانی‌مدت، تلاش برای دسترسی به اطلاعاتی که برای انجام وظایف شغلی لازم نیستند، دسترسی به منابع مالی بدون ارائه توضیح مناسب، ارعاب یا آزار جنسی همکاران، خشونت در محیط کار، و سایر موارد نقش جدی فرایندها، خط‌مشی‌ها، رویه‌ها، رهنمودها و قوانین سازمانی اشاره کرد. در آموزش‌های مربوطه، به کارکنان و مدیران گفته می‌شود که چگونه دغدغه‌های خود در زمینه تهدیدات داخلی را از طریق کانال‌های سازمانی مقتضی و بر اساس رویه‌ها و خط‌مشی‌های سازمانی، به افراد مسئول انتقال دهند. کنترل‌های مربوطه: PL-4, PM-12, PS-3, PS-6.

مراجع: بخش پنجم C.F.R، قسمت C (5 C.F.R. 930.301)؛ دستور اجرایی ۱۳۵۸۷؛ شماره ویژه NIST 800-50.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AT-2 اولویت پایین	AT-2(2) اولویت متوسط	AT-2(2) اولویت بالا

AT-3: آموزش‌های امنیتی مبتنی بر شغل

کنترل: سازمان به ترتیب زیر آموزش‌های امنیتی را بر اساس شغل کارکنان برای آن‌ها در نظر می‌گیرد و نقش‌ها و مسئولیت‌هایی را در این زمینه به آن‌ها اختصاص می‌دهد:

الف. پیش از دسترسی مجاز به سیستم اطلاعاتی یا انجام وظایف تخصیص‌یافته؛

ب. در صورتی که آموزش‌های مذکور در اثر تغییرات سیستم اطلاعاتی لازم شوند؛ و

پ. پس از [اختصاص: بازه زمانی تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: سازمان‌ها بر اساس نقش‌ها و مسئولیت‌های تخصیص‌یافته به افراد، الزامات امنیتی خاص خود و همچنین سیستم‌های اطلاعاتی که کارکنان به آن‌ها دسترسی دارند، محتوای روش‌های آگاهی‌رسانی امنیتی را تعیین می‌نمایند. علاوه بر این، سازمان‌ها آموزش‌های فنی و امنیتی خاصی را با توجه به وظایف خاص معماران، توسعه‌دهندگان سیستم‌های اطلاعاتی، توسعه‌دهندگان نرم‌افزار، مسئولیت تدارکات، مدیران سیستم‌های اطلاعاتی، راهبران سیستم و شبکه، مسئولین پیکربندی و ممیزی، مسئولین تأیید عملیات، مسئولین کنترل امنیت، و سایر کارکنانی که به نرم‌افزارهای سطح سیستم دسترسی دارند، به آن‌ها ارائه می‌کنند. در این آموزش‌های جامع، به نقش‌ها و مسئولیت‌های مدیریتی، عملیاتی و فنی پرداخته می‌شود که شاخص‌ها و ابزارهای فیزیکی، پرسنلی و فنی را پوشش می‌دهند. آموزش‌های مذکور شامل مواردی از جمله خط‌مشی‌ها، رویه‌ها، ابزارها و روش‌های مربوط به نقش‌های امنیتی تعیین‌شده در سازمان هستند. سازمان‌ها همچنین آموزش‌های لازم را به کارکنان ارائه می‌کنند تا این افراد بتوانند مسئولیت‌های خود در زمینه امنیت زنجیره تأمین و عملیات را چارچوب برنامه امنیت اطلاعات سازمان به نحو شایسته انجام دهند. آموزش‌های مبتنی بر شغل، به پیمانکاران ارائه‌کننده خدمات فدرال نیز ارائه می‌شود. کنترل‌های مربوطه: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

کنترل پیشرفته:

(۱) آموزش امنیتی مبتنی بر شغل / کنترل‌های محیطی

سازمان آموزش‌های لازم در زمینه به‌کارگیری و اجرای کنترل‌های محیطی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] به [اختصاص: نقش‌ها و کارکنان تعیین‌شده توسط سازمان] ارائه می‌کند.

راهنمایی‌های تکمیلی: کنترل‌های محیطی مواردی از جمله سیستم‌ها و ابزارهای شناسایی و جلوگیری از تهدیدات، سیستم‌های آب‌پاش، کپسول‌های آتش‌نشانی، شلنگ‌های آتش‌نشانی، سیستم‌های تشخیص دود، سیستم‌های تعیین حرارت و رطوبت، سیستم‌های تهویه و گرمایش، و سیستم‌های تأمین توان در ساختمان را در بر می‌گیرند.

(۲) آموزش امنیتی مبتنی بر شغل / کنترل‌های امنیتی فیزیکی

سازمان آموزش‌های لازم در زمینه به‌کارگیری و اجرای کنترل‌های امنیتی فیزیکی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] به [اختصاص: نقش‌ها و کارکنان تعیین‌شده توسط سازمان] ارائه می‌کند.

راهنمایی‌های تکمیلی: کنترل‌های امنیتی فیزیکی مواردی از جمله ابزارهای کنترل دسترسی فیزیکی، هشدارهای ورود فیزیکی غیرمجاز، ابزارهای نظارت و پایش، و محافظ‌های امنیتی را در بر می‌گیرند. سازمان‌ها تعیین می‌کنند که کدام کارکنان نقش‌ها و مسئولیت‌های مربوط به امنیت فیزیکی را بر دارند و باید در این زمینه آموزش داده شوند. کنترل‌های مربوطه: PE-2, PE-3, PE-4, PE-5.

(۳) آموزش امنیتی مبتنی بر شغل / تمرین‌های عملی

سازمان تمرین‌هایی عملی را برای آموزش امنیت در نظر می‌گیرد، تا بتواند به اهداف آموزشی خود دست یابد.

راهنمایی‌های تکمیلی: تمرین‌های عملی مواردی از جمله آموزش امنیت برای توسعه‌دهندگان نرم‌افزار را در بر می‌گیرد. در این آموزش‌ها، برخی حملات سایبری شبیه‌سازی می‌شوند که ضعف‌های نرم‌افزاری مانند سرریز بافر را هدف قرار می‌دهند. گاهی نیز حملات فیشینگ شبیه‌سازی می‌شوند که به رهبران و مدیران ارشد حمله می‌کنند. این تمرین‌های عملی، توسعه‌دهندگان را یاری می‌کنند تا درک بهتری از تأثیرات ضعف‌های نرم‌افزاری داشته باشند و دریابند که باید از استانداردها و فرایندهای کدگذاری امنیتی استفاده کنند.

(۴) آموزش امنیتی مبتنی بر شغل / ارتباطات مشکوک و رفتارهای غیر معمول سیستم

سازمان آموزش‌هایی را در زمینه [اختصاص: شاخص کدهای مخرب تعیین‌شده توسط سازمان] به کارکنان خود ارائه می‌کند تا ارتباطات مشکوک و رفتارهای غیر معمول را در سیستم‌های اطلاعات سازمان تشخیص دهند.

راهنمایی‌های تکمیلی: کارکنان آموزش‌دیده در واقع بخشی از استراتژی دفاعی سازمان هستند که آن را در برابر کدهای مخرب واردشده از طریق ایمیل‌ها یا برنامه‌های کاربردی وب محافظت می‌کنند. کارکنان به نحو مناسب آموزش داده می‌شوند تا بتوانند نشانه‌های حاکی از دریافت ایمیل‌های مخرب را شناسایی کنند (به عنوان مثال می‌توان به مواردی از جمله دریافت ایمیل‌های ناخواسته، دریافت ایمیل‌هایی با جمله‌بندی نادرست یا ضعیف، یا دریافت ایمیل از یک فرستنده ناشناس که خود را به عنوان یک حامی مالی یا پیمانکار شناخته‌شده جا زده است، اشاره کرد). کارکنان همچنین آموزش می‌بینند که چگونه در برابر این ارتباطات اینترنتی یا ایمیل‌های مشکوک واکنش نشان دهند (مثلاً این که پیوست‌ها را باز نکنند، روی لینک‌های ارسال‌شده کلیک نکنند، و آدرس ایمیل‌های دریافتی را چک کنند). برای این که فرایند آموزشی مذکور به شکل مؤثری انجام شود، تمام کارکنان سازمان‌ها آموزش داده می‌شوند تا ارتباطات مشکوک را شناسایی کنند. آموزش کارکنان برای شناسایی رفتارهای غیر معمول در

سیستم‌های اطلاعات سازمانی، سبب می‌شود که نشانه‌های اولیه دال بر وجود کدهای مخرب شناسایی شوند. تشخیص این رفتارهای غیر معمول توسط کارکنان سازمان، مکمل سیستم‌ها و روش‌های خودکاری است که در سازمان برای ردیابی کدهای مخرب و حفاظت در برابر آن‌ها به کار گرفته می‌شوند.

مراجع: بخش پنجم C.F.R، قسمت C (5 C.F.R. 930.301)؛ شماره‌های ویژه NIST 800-16, 800-50.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AT-3 اولویت پایین	AT-3 اولویت متوسط	AT-3 اولویت بالا

AT-4: **ثبت اطلاعات آموزش‌های امنیتی**

کنترل: سازمان:

الف. فعالیت‌هایی را که در زمینه آموزش امنیت سیستم‌های اطلاعاتی صورت گرفته است، ثبت می‌کند. در این فرایند، اطلاعات مربوط به آموزش‌های آگاهی‌رسانی امنیتی اولیه و آموزش‌های خاص در زمینه امنیت سیستم‌های اطلاعاتی ثبت می‌شوند؛

ب. اطلاعات مربوط به این آموزش‌ها را به مدت [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] نگهداری می‌کند.

راهنمایی‌های تکمیلی: ممکن است سازمان تصمیم بگیرد که اطلاعات و مستندات مربوط به آموزش‌های تخصصی، توسط ناطران نگهداری شوند. کنترل‌های مربوطه: AT-2, AT-3, PM-14.

کنترل پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	AT-4 اولویت پایین	AT-4 اولویت متوسط	AT-4 اولویت بالا

AT-5: ارتباط با انجمن‌ها و گروه‌های امنیتی

[حذف شد: در بخش PM-15 گنجانده شد].

خانواده: ممیزی و پاسخگویی

AU-1: خط‌مشی و رویه‌های ممیزی و پاسخگویی

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۱. خط‌مشی ممیزی و پاسخگویی شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و
۲. رویه‌های تسهیل پیاده‌سازی خط‌مشی ممیزی و پاسخگویی و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] مرور و به‌روز می‌کند:

۳. خط‌مشی ممیزی و پاسخگویی؛ و
۴. رویه‌های ممیزی و پاسخگویی.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل های خانواده AU را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. استراتژی مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: شماره‌های ویژه NIST 800-12, 800-100.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AU-1 اولویت پایین	AU-1 اولویت متوسط	AU-1 اولویت بالا

AU-2: رویدادهای ممیزی

کنترل: سازمان:

الف. تعیین می‌کند که سیستم اطلاعاتی می‌تواند رویدادهای زیر را ممیزی کند:

[اختصاص: رویدادهای قابل ممیزی تعیین‌شده توسط سازمان]؛

ب. بخش ممیزی امنیت را با سایر بخش‌های سازمان که به اطلاعات ممیزی نیاز دارند، هماهنگ می‌کند تا پشتیبانی متقابل ارتقا یابد و انتخاب رویدادهای قابل ممیزی به شکل بهتری صورت گیرد؛

پ. تشریح می‌کند که چرا رویدادهای قابل ممیزی برای پشتیبانی از بررسی‌های پس از رخدادهای امنیتی کفایت می‌کنند؛ و

ت. تعیین می‌کند که رویدادهای زیر باید در سیستم امنیتی سازمان ممیزی شوند:

[اختصاص: رویدادهای امنیتی تعیین‌شده توسط سازمان (زیرمجموعه‌ای از رویدادهای قابل ممیزی تعریف‌شده در AU-2 الف) به همراه فراوانی ممیزی برای هر یک از رویدادهای تعیین‌شده (یا شرایط لازم برای این امر)].

راهنمایی‌های تکمیلی: منظور از یک رویداد، هر اتفاق قابل مشاهده‌ای است که در سیستم اطلاعاتی سازمان رخ می‌دهد. رویدادهایی از سوی سازمان‌ها به عنوان رویدادهای ممیزی تعیین می‌شوند که مهم و مربوط به امنیت سیستم‌های اطلاعاتی یا محیط عملیاتی این سیستم‌ها باشند. رویدادهای ممیزی مواردی از جمله تغییر گذرواژه، ورود ناموفق به سیستم، دسترسی ناموفق به سیستم‌های اطلاعاتی، استفاده از امتیازات ویژه راهبری، استفاده از اطلاعات حساب کاربری PIV، و یا استفاده از اطلاعات حساب کاربری شخص ثالث را شامل می‌شوند. برای تعیین مجموعه رویدادهای قابل ممیزی، سازمان‌ها تعیین می‌کنند که برای هر یک از کنترل‌های امنیتی باید از کدام روش ممیزی استفاده کرد. به منظور انطباق دادن الزامات ممیزی با سایر نیازهای سیستم‌های اطلاعاتی، باید تعیین کرد که کدام رویدادهای «قابل ممیزی» پیشتر «ممیزی شده‌اند». به عنوان مثال، ممکن است سازمان‌ها تصمیم بگیرند که سیستم‌های اطلاعاتی باید قابلیت ثبت تمام تلاش‌های موفق و ناموفق دسترسی به

فایل‌ها را داشته باشند، اما این قابلیت را تنها در شرایط خاصی فعال کنند. دلیل این امر آن است که فعالل کردن این گزینه می‌تواند فشار کاری زیادی به سیستم وارد کند. الزامات حسابداری، شامل نیاز به رویدادهای قابل ممیزی، ممکن است در سایر کنترل‌های امنیتی و کنترل‌های پیشرفته مورد اشاره قرار گیرند. سازمان‌ها همچنین رویدادهای قابل ممیزی تعیین‌شده در دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال را نیز در نظر می‌گیرند. اطلاعات ممیزی ممکن است به اشکال مختلف خلاصه‌سازی شوند، مثلاً در قالب بسته‌هایی در شبکه منتقل شوند. انتخاب سطح مناسب خلاصه‌سازی، یکی از جنبه‌های مهم فرایند ممیزی است که می‌تواند سازمان را در شناسایی ریشه‌های مشکلات یاری کند. در تعریف رویدادهای قابل ممیزی، سازمان‌ها به این امر توجه می‌کنند که با استفاده از چه روش‌هایی می‌توان رویدادهای مربوطه را پوشش داد. به عنوان مثال، می‌توان به مراحل مختلف فرایندهای توزیع‌شده و مبتنی بر تراکنش (مانند فرایندهایی که بین سازمان‌های مختلف توزیع شده‌اند) و اقدامات انجام‌شده در معماری‌های مبتنی بر خدمت اشاره کرد. کنترل‌های مربوطه: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

کنترل پیشرفته:

(۱) رویدادهای ممیزی / گردآوری اطلاعات ممیزی از منابع مختلف
[حذف شد: در بخش AU-12 گنجانده شد].

(۲) رویدادهای ممیزی / انتخاب رویدادهای امنیتی توسط مؤلفه
[حذف شد: در بخش AU-12 گنجانده شد].

(۳) رویدادهای ممیزی / بررسی و به‌روزرسانی

سازمان رویدادهای ممیزی را [انتخاب: در بازه‌های زمانی تعیین‌شده توسط سازمان] بررسی و به‌روز می‌کند.

راهنمایی‌های تکمیلی: ممکن است رویدادهایی که از نظر سازمان باید ممیزی شوند، به مرور زمان تغییر کنند. مرور و به‌روزرسانی دوره‌ای رویدادهای ممیزی‌شده سبب حصول اطمینان از این امر می‌شود که مجموعه موجود هنوز لازم و کافی است.

(۴) رویدادهای ممیزی / بخش‌های دارای امتیاز ویژه
[حذف شد: در بخش AC-6 (9) گنجانده شد].

مراجع: شماره ویژه NIST 800-92؛ آدرس اینترنتی http://idmanagement.gov.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AU-2 اولویت پایین	AU-2(3) اولویت متوسط	AU-2(3) اولویت بالا

AU-3: **محتوای سوابق ممیزی**

کنترل: سیستم اطلاعاتی، سوابق ممیزی را تولید می‌کند. این اسناد شامل اطلاعاتی هستند که تعیین می‌کنند چه نوع رویدادهایی به وقوع پیوسته‌اند، این رویدادها چه هنگام رخ داده‌اند، رویدادهای مذکور کجا اتفاق افتاده‌اند، منبع رویدادها چه بوده است، این رویدادها چه پیامدهایی داشته‌اند، و چه افراد و گروه‌هایی در این میان ایفای نقش کرده‌اند.

راهنمایی‌های تکمیلی: محتوای سوابق ممیزی شامل مواردی از جمله مهرهای زمانی، آدرس‌های مبدأ و مقصد، شناسه‌های کاربران و فرایندها، توضیحات مربوط به رویدادها، نشانه‌های دال بر موفقیت یا عدم موفقیت، نام فایل‌های مربوطه، و قوانین کنترل جریان و کنترل دسترسی فراخوانی‌شده هستند. پیامدهای رویدادها، شاخص‌های مربوط به موفقیت یا شکست رویدادها و نتایج آن‌ها (مانند وضعیت امنیتی سیستم اطلاعاتی پس از وقوع رویداد) را شامل می‌شوند. کنترل‌های مربوطه: AU-2, AU-8, AU-12, SI-11.

کنترل پیشرفته:

(۳) محتوای سوابق ممیزی / سایر اطلاعات ممیزی

سیستم اطلاعاتی، سوابق ممیزی را تولید می‌کند که شامل این اطلاعات اضافی هستند:

[اختصاص: اطلاعات اضافی و دقیق تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: اطلاعات دقیقی که ممکن است سازمان در سوابق ممیزی خود در نظر بگیرد، مواردی از جمله متن کامل دستورات ویژه و هویت کاربران حساب‌های گروهی را در بر می‌گیرند. سازمان‌ها این اطلاعات ممیزی اضافی را محدود به مواردی می‌کنند که برای رعایت الزامات ممیزی خاص، لازم هستند. بدین ترتیب، اطلاعات گمراه‌کننده یا اطلاعاتی که مانع یافتن موارد مطلوب می‌شوند، ثبت نمی‌گردند و استفاده از اطلاعات ممیزی آسان‌تر می‌شود.

(۴) محتوای سوابق ممیزی / مدیریت متمرکز محتوای سوابق ممیزی

سیستم اطلاعاتی، امکان مدیریت متمرکز و پیکربندی محتوای گردآوری‌شده در سوابق ممیزی را فراهم می‌آورد. این اسناد توسط [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] تهیه می‌شوند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته لازم می‌دارد که محتوای گردآوری‌شده در سوابق ممیزی از یک مکان متمرکز پیکربندی شوند. بدین ترتیب، استفاده از سیستم‌های اتوماسیون ضروری خواهد بود. سازمان‌ها فرایند انتخاب محتوای ممیزی را به گونه‌ای هماهنگ می‌کنند که از مدیریت متمرکز و قابلیت پیکربندی ارائه‌شده توسط سیستم اطلاعاتی پشتیبانی شود. کنترل‌های مربوطه: AU-6, AU-7.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AU-3 اولویت پایین	AU-3(1) اولویت متوسط	AU-3(1)(2) اولویت بالا

AU-4: ظرفیت ذخیره‌سازی اطلاعات ممیزی

کنترل: سازمان ظرفیت ذخیره‌سازی اطلاعات ممیزی را با توجه به [اختصاص: الزامات تعیین‌شده توسط سازمان در زمینه ذخیره‌سازی اطلاعات ممیزی] تعیین می‌کند.

راهنمایی‌های تکمیلی: سازمان‌ها در هنگام تعیین ظرفیت ذخیره‌سازی اطلاعات ممیزی، تعیین می‌کنند که از چه روش ممیزی باید استفاده شود و چه الزاماتی باید در این زمینه رعایت شوند. اختصاص دادن ظرفیت ذخیره‌سازی زیاد، سبب می‌شود که سازمان در آینده با کمبود ظرفیت مواجه نشود. کنترل‌های مربوطه: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.

کنترل پیشرفته:

(۱) ظرفیت ذخیره‌سازی اطلاعات ممیزی / انتقال به یک حافظه دیگر

سیستم اطلاعاتی، اطلاعات سوابق ممیزی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] از سیستم در حال ممیزی، به یک سیستم یا رسانه دیگر منتقل می‌کند.

راهنمایی‌های تکمیلی: انتقال اطلاعات به یک سیستم دیگر بدین منظور انجام می‌شود که محرمانگی و یکپارچگی اطلاعات ممیزی حفظ شود. این روش، در سیستم‌های اطلاعاتی که ظرفیت ذخیره‌سازی

زیادی ندارند بسیار شایع است. در این روش، از حافظه ذخیره‌سازی اطلاعات ممیزی به صورت موقتی و تنها تا هنگامی استفاده می‌شود که حافظه دیگری برای انتقال اطلاعات مهیا شود.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AU-4 اولویت پایین	AU-4 اولویت متوسط	AU-4 اولویت بالا

AU-5: پاسخ به عدم موفقیت در پردازش اطلاعات ممیزی

کنترل: سیستم اطلاعاتی:

الف. در صورت عدم موفقیت در پردازش اطلاعات ممیزی، مراتب را به [اختصاص: نقش‌ها و کارکنان تعیین‌شده توسط سازمان] اطلاع می‌دهد؛ و

ب. این اقدامات را نیز انجام می‌دهد: [اختصاص: اقدامات تعیین‌شده توسط سازمان (مانند از کار انداختن سیستم اطلاعاتی، بازنویسی روی قدیمی‌ترین اطلاعات ممیزی، توقف تولید اسناد و اطلاعات ممیزی)].

راهنمایی‌های تکمیلی: عدم موفقیت در پردازش اطلاعات ممیزی، مواردی از جمله خطاهای سخت‌افزاری و نرم‌افزاری، عملکرد نادرست مکانیسم‌های جمع‌آوری اطلاعات ممیزی، و تجاوز از ظرفیت ذخیره‌سازی اطلاعات ممیزی را در بر می‌گیرد. ممکن است سازمان تصمیم بگیرند که اقداماتی را در هر یک از این موارد انجام دهند (مثلاً بر اساس نوع، مکان یا شدت عوامل مذکور، فعالیت‌هایی را صورت دهند). این کنترل در مورد هر یک از حافظه‌های ذخیره‌سازی اطلاعات ممیزی (یعنی مؤلفه‌های مجزای سیستم اطلاعاتی که اطلاعات ممیزی در آن‌ها ذخیره می‌شود)، کل ظرفیت ذخیره‌سازی اطلاعات ممیزی در سازمان (یعنی مجموع تمام حافظه‌های ذخیره‌سازی اطلاعات ممیزی)، یا هر دو این موارد صدق می‌کند. کنترل‌های مربوطه: AU-4, SI-12.

کنترل پیشرفته:

(۱) پاسخ به عدم موفقیت در پردازش اطلاعات ممیزی / ظرفیت ذخیره‌سازی اطلاعات ممیزی

سیستم اطلاعاتی [اختصاص: در بازه زمانی تعیین‌شده توسط سازمان] در هنگام رسیدن به [اختصاص: درصد تعیین‌شده توسط سازمان] محدودیت ظرفیت تعیین‌شده برای ذخیره‌سازی اطلاعات ممیزی، هشداری را به [اختصاص: کارکنان، نقش‌ها و/یا مکان‌های تعیین‌شده توسط سازمان] ارسال می‌کند.

راهنمایی‌های تکمیلی: ممکن است سازمان‌ها حافظه‌های مختلفی یا ظرفیت‌های متفاوت، برای ذخیره‌سازی اطلاعات ممیزی در بخش‌های مختلف سیستم اطلاعاتی داشته باشند.

(۲) پاسخ به عدم موفقیت در پردازش اطلاعات ممیزی / هشدارهای بلادرنگ

هنگامی که رویدادهای ممیزی روبرو رخ می‌دهند، سیستم اطلاعاتی هشدارهایی را [اختصاص: در بازه‌های زمانی بلادرنگ تعیین‌شده توسط سازمان] به [اختصاص: کارکنان، نقش‌ها و/یا مکان‌های تعیین‌شده توسط سازمان] ارسال می‌کند: [اختصاص: رویدادهای ممیزی تعیین‌شده توسط سازمان که نیازمند هشدار بلادرنگ هستند].

راهنمایی‌های تکمیلی: هشدارها در واقع پیام‌های فوری برای سازمان‌ها هستند. سرعت ارسال این هشدارهای بلادرنگ، به فناوری‌های مورد استفاده سازمان بستگی دارد. این کار معمولاً طی یک ثانیه یا کمتر انجام می‌شود.

(۳) پاسخ به عدم موفقیت در پردازش اطلاعات ممیزی / آستانه ترافیک قابل پیکربندی

سیستم اطلاعاتی یک آستانه قابل پیکربندی را برای ترافیک شبکه در نظر می‌گیرد که محدودیتی را برای ظرفیت ممیزی تعیین می‌کند و ترافیک بالاتر از آستانه تعیین‌شده را [اختصاص: متوقف می‌نماید، به تأخیر می‌اندازد].

راهنمایی‌های تکمیلی: سازمان‌ها این توانایی را دارند که در صورت تجاوز از ظرفیت ذخیره‌سازی سیستم اطلاعاتی، پردازش ترافیک شبکه را متوقف کنند یا به تأخیر اندازند. این توقف یا تأخیر به آستانه تعیین‌شده بستگی دارد، که می‌توان آن را بسته به تغییرات ظرفیت ذخیره‌سازی اطلاعات ممیزی تغییر داد.

(۴) پاسخ به عدم موفقیت در پردازش اطلاعات ممیزی / خاموش کردن سیستم در صورت عملکرد ناموفق

در صورت رخ دادن [اختصاص: شکست ممیزی تعیین‌شده توسط سازمان]، سیستم اطلاعاتی [انتخاب: سیستم را به طور کامل خاموش می‌کند، برخی از بخش‌های سیستم را خاموش می‌کند، محدودیت‌هایی را برای عملکرد سیستم در نظر می‌گیرد]، مگر این که یک ظرفیت ممیزی ثانویه وجود داشته باشد.

راهنمایی‌های تکمیلی: سازمان‌ها تعیین می‌کنند که کدام انواع شکست ممیزی منجر به خاموش شدن خودکار سیستم اطلاعاتی یا محدود شدن عملکرد آن می‌گردند. از آنجا که ادامه فعالیت‌ها و مأموریت‌ها

اهمیت بسیار زیادی دارد، ممکن است سازمان‌ها تصمیم بگیرند که در صورت بروز شکست‌های نه چندان جدی، نیازی به خاموش کردن کامل سیستم اطلاعاتی نیست. در این شرایط، ممکن است بخشی از سیستم اطلاعاتی خاموش شود، یا این که عملکرد این سیستم محدود گردد. کنترل‌های مربوطه: AU-15.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AU-5 اولویت پایین	AU-5 اولویت متوسط	AU-5(1)(2) اولویت بالا

AU-6: **مرور، تحلیل و گزارش‌دهی ممیزی**

کنترل: سازمان:

الف. سوابق ممیزی سیستم اطلاعاتی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] مرور و تحلیل می‌کند، تا نشانه‌های [اختصاص: فعالیت‌های نامناسب یا غیر معمول تعیین‌شده توسط سازمان] را بیابد؛ و

ب. یافته‌های خود را به [اختصاص: کارکنان و نقش‌های تعیین‌شده توسط سازمان] گزارش می‌کند.

راهنمایی‌های تکمیلی: مرور، تحلیل و گزارش‌دهی ممیزی، فرایند ممیزی اطلاعات امنیتی توسط سازمان را در بر می‌گیرد. به عنوان مثال، می‌توان به فرایند ممیزی نتایج حاصل از پایش کاربرد حساب‌های کاربری، دسترسی راه‌دور، اتصال بی‌سیم، اتصال دستگاه‌های همراه، تنظیمات پیکربندی، موجودی مؤلفه‌های سیستم، کاربرد ابزارهای تعمیر و نگهداری داخل و خارج سازمان، دسترسی فیزیکی، درجه حرارت و رطوبت، جابجایی و تحویل تجهیزات، ارتباطات در مرزهای سیستم اطلاعاتی، استفاده از کدهای موبایل، و استفاده از VoIP اشاره کرد. یافته‌ها به موجودیت‌های سازمانی از جمله تیم واکنش به رویدادها، تیم کمکی و گروه یا دپارتمان امنیت اطلاعات گزارش می‌شوند. اگر مرور و تحلیل اطلاعات ممیزی برای سازمان‌ها ممنوع باشد یا این که سازمان‌ها قادر به انجام این فعالیت‌ها نباشند (مثلاً در برخی سیستم‌ها یا کاربردهای مربوط به امنیت ملی)، ممکن است این وظیفه به سازمان‌های دیگری سپرده شود. کنترل‌های مربوطه: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.

کنترل پیشرفته:

(۱) مرور، تحلیل و گزارش‌دهی ممیزی / یکپارچه‌سازی فرایندها

سازمان، مکانیسم‌های خودکاری را برای یکپارچه‌سازی فرایندهای مرور، تحلیل و گزارش‌دهی ممیزی به کار می‌گیرد تا بتواند فعالیت‌های مشکوک را بررسی کند و به آن‌ها واکنش مناسب نشان دهد.

راهنمایی‌های تکمیلی: فرایندهای سازمانی که از سیستم یکپارچه مرور، تحلیل و گزارش‌دهی ممیزی سود می‌برند، شامل مواردی از جمله واکنش به رویدادها، پایش پیوسته، برنامه‌ریزی در شرایط اضطراری، و ممیزی‌های صورت‌گرفته توسط بازرس کل هستند. کنترل‌های مربوطه: AU-12, PM-7.

(۲) مرور، تحلیل و گزارش‌دهی ممیزی / هشدارهای امنیتی خودکار

[حذف شد: در بخش SI-4 گنجانده شد].

(۳) مرور، تحلیل و گزارش‌دهی ممیزی / حافظه‌های ممیزی به‌هم‌پیوسته

سازمان، سوابق ممیزی موجود در حافظه‌های مختلف را تحلیل و ترکیب می‌کند تا به درک جامعی از شرایط در سراسر سازمان درست یابد.

راهنمایی‌های تکمیلی: درک جامع شرایط در سراسر سازمان، شامل هر سه جنبه مدیریت مخاطرات (یعنی مدیریت مخاطرات سازمانی، مخاطرات فرایند کسب‌وکار و مخاطرات سیستم اطلاعاتی) است که به ایجاد درکی از شرایط بین‌سازمانی نیز منجر می‌شود. کنترل‌های مربوطه: AU-12, IR-4.

(۴) مرور، تحلیل و گزارش‌دهی ممیزی / مرور و تحلیل مرکزی

سیستم اطلاعاتی، امکان مرور و تحلیل مرکزی سوابق ممیزی را از طریق مؤلفه‌های مختلف موجود در سیستم فراهم می‌آورد.

راهنمایی‌های تکمیلی: مکانیسم‌های خودکار مرور و تحلیل مرکزی شامل مواردی از جمله ابزارهای مدیریت اطلاعات امنیتی هستند. کنترل‌های مربوطه: AU-2, AU-12.

(۵) مرور، تحلیل و گزارش‌دهی ممیزی / یکپارچه‌سازی، بررسی و پایش قابلیت‌ها

سازمان، قابلیت تحلیل سوابق ممیزی را با قابلیت تحلیل [انتخاب (یک یا چند مورد): اطلاعات مربوط به بررسی نقاط ضعف؛ داده‌های عملکردی؛ اطلاعات مربوط به پایش سیستم اطلاعاتی؛ [اختصاص: داده‌ها و اطلاعات گردآوری‌شده از سایر منابع که توسط سازمان تعیین شده‌اند]] ترکیب می‌کند تا بهتر از گذشته بتوان فعالیت‌های نامناسب یا غیر معمول را شناسایی کرد.

راهنمایی‌های تکمیلی: در این کنترل پیشرفته، نیازی به بررسی نقاط ضعف، تولید داده‌های عملکردی، یا پایش سیستم اطلاعاتی نیست. در عوض، به موجب این کنترل پیشرفته باید اطلاعات تولیدشده در

حوزه‌های مذکور را به همراه اطلاعات ممیزی تحیل نمود. سیستم مدیریت اطلاعات و رویدادهای امنیتی می‌تواند فرایند ترکیب و یکپارچه‌سازی اطلاعات ممیزی موجود در مؤلفه‌های مختلف سیستم اطلاعاتی و همچنین تحلیل و ترکیب سوابق ممیزی را تسهیل کند. استفاده از اسکریپت‌های استاندارد تحلیل سوابق ممیزی ارائه‌شده توسط سازمان (با تنظیمات و تغییرات محلی، در صورت لزوم)، رویکرد به‌صرفه‌تری را برای تحلیل اطلاعات ممیزی گردآوری‌شده در اختیار سازمان‌ها قرار می‌دهد. ترکیب اطلاعات سوابق ممیزی با اطلاعات مربوط به بررسی نقاط ضعف، سازمان‌ها را یاری می‌کند تا صحت بررسی‌های انجام‌شده را تأیید کنند و حملات شناسایی‌شده را با نتایج حاصل از این بررسی‌ها تطبیق دهند. ترکیب اطلاعات ممیزی با داده‌های عملکردی، سازمان‌ها را قادر می‌سازد تا حملات DOS یا حملات منجر به استفاده غیر مجاز از منابع را شناسایی کنند. ترکیب اطلاعات ممیزی با اطلاعات حاصل از پایش سیستم نیز سازمان‌ها را کمک می‌کند تا حملات را شناسایی نمایند و اطلاعات ممیزی را به صورت بهتری با شرایط عملیاتی ارتباط دهند. کنترل‌های مربوطه: AU-12, IR-4, RA-5.

(۶) مرور، تحلیل و گزارش‌دهی ممیزی / ترکیب اطلاعات ممیزی با اطلاعات مربوط به پایش فیزیکی

سازمان، اطلاعات ممیزی را با اطلاعات مربوط به پایش فیزیکی ترکیب می‌کند، تا بهتر بتواند فعالیت‌های مشکوک، نامناسب، غیر معمول یا مخرب را شناسایی نماید.

راهنمایی‌های تکمیلی: ترکیب اطلاعات پایش فیزیکی با اطلاعات ممیزی سیستم اطلاعاتی، سازمان‌ها را یاری می‌کند تا رفتارهای مشکوک یا شواهد دال بر این رفتارها را شناسایی کنند. به عنوان مثال، می‌توان اطلاعات هویتی افراد برای ورود به یک سیستم اطلاعاتی را در کنار اطلاعات حاکی از حضور فیزیکی فرد در هنگام دسترسی به سیستم قرار داد و تحقیقات را به شکل بهتری انجام داد.

(۷) مرور، تحلیل و گزارش‌دهی ممیزی / اقدامات مجاز

سازمان، اقدامات مجاز در زمینه مرور، تحلیل و گزارش‌دهی اطلاعات ممیزی را برای هر یک از [انتخاب (یک یا چند مورد): فرایند سیستم اطلاعاتی؛ نقش؛ کاربر] تعیین می‌کند.

راهنمایی‌های تکمیلی: سازمان‌ها با استفاده از روش‌های مدیریت حساب‌های کاربری، اقدامات مجاز در زمینه مرور، تحلیل و گزارش‌دهی اطلاعات ممیزی را برای هر یک از فرایندهای سیستم اطلاعاتی، نقش‌ها و کاربران تعیین می‌کنند. تعیین اقدامات مجاز در زمینه اطلاعات ممیزی، یکی از راه‌های پیاده‌سازی اصل حداقل بودن اختیارات[۱۵۶] است. اقدامات مجاز شامل مواردی از جمله خواندن، نوشتن، اجرا کردن، پیوست کردن و پاک کردن هستند.

[156] Principle of least privilege

(۸) مرور، تحلیل و گزارش‌دهی ممیزی / تحلیل متن کامل دستورات ویژه

سازمان، تحلیل متن کامل دستورات ویژه را در مؤلفه‌های مجزا یا زیرمجموعه‌هایی از سیستم اطلاعاتی اصلی خود، یا سیستم اطلاعاتی دیگری که به این تحلیل اختصاص داده شده است، انجام می‌دهد.

راهنمایی‌های تکمیلی: به موجب این کنترل پیشرفته، لازم است یک محیط مجزا برای تحلیل اطلاعات ممیزی مربوط به کاربران دارای امتیاز ویژه ایجاد شود، بدون این که اطلاعات مذکور در سیستم اطلاعاتی به خطر افتند (از جمله امتیازات ویژه مذکور می‌توان به توانایی اجرای دستورات ویژه اشاره کرد). تحلیل متن کامل یعنی تحلیل که در آن متن کامل دستورات ویژه (یعنی دستورات به همراه تمامی پارامترهای آن‌ها) تحلیل می‌شود. این تحلیل، در مقابل تحلیلی قرار می‌گیرد که در آن تنها نام دستور بررسی می‌شود. در تحلیل متن کامل از روش‌هایی مانند انطباق الگو و روش‌های اکتشافی استفاده می‌شود. کنترل‌های مربوطه: AU-3, AU-9, AU-11, AU-12.

(۹) مرور، تحلیل و گزارش‌دهی ممیزی / ترکیب کردن اطلاعات ممیزی با اطلاعات به دست آمده از منابع غیر فنی

سازمان، اطلاعات به دست آمده از منابع غیر فنی را با اطلاعات ممیزی ترکیب می‌کند تا درک جامعی از شرایط خود به دست آورد.

راهنمایی‌های تکمیلی: منابع غیر فنی شامل منابعی از جمله اسناد منابع انسانی است که موارد نقض خط‌مشی‌های سازمانی را ثبت کرده‌اند (مانند آزار جنسی و استفاده نامناسب از سرمایه‌های اطلاعاتی سازمان). این اطلاعات، سازمان‌ها را یاری می‌کنند تا تحلیل‌های بهتری را صورت دهند و فعالیت‌های زیان‌آور داخلی را شناسایی کنند. به دلیل ماهیت حساس اطلاعات به دست آمده از منابع غیر فنی، سازمان‌ها سطح دسترسی به این اطلاعات را محدود می‌کنند تا احتمال افشای اطلاعات مربوط به حریم خصوصی افراد به حداقل برسد. بنابراین، ترکیب اطلاعات به دست آمده از منابع غیر فنی با اطلاعات ممیزی عموماً تنها در شرایطی رخ می‌دهد که افرادی مظنون به دست داشتن در رویدادهای امنیتی باشند. سازمان‌ها پیش از آن که چنین اقدامی را انجام دهند، مشاوره‌های قانونی لازم را دریافت می‌کنند. کنترل‌های مربوطه: AT-2.

(۱۰) مرور، تحلیل و گزارش‌دهی ممیزی / تنظیم سطح ممیزی

هنگامی که اطلاعات به دست آمده از نهادهای مجری قانون، نهادهای امنیتی یا سایر منابع موثق، حاکی از بروز تغییراتی در میزان مخاطرات سازمان باشد، سازمان اقدام به تغییر سطح مرور، تحلیل و گزارش‌دهی ممیزی در سیستم اطلاعاتی می‌کند.

راهنمایی‌های تکمیلی: ممکن است فراوانی، حیطه و/یا عمق فرایند مرور، تحلیل و گزارش‌دهی ممیزی به گونه‌ای تغییر یابد که نیازهای سازمانی حاصل از اطلاعات جدید را برآورده کند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AU-6 اولویت پایین	AU-6(1)(3) اولویت متوسط	AU-6(1)(3)(5)(6) اولویت بالا

AU-7: تهیه گزارشات و خلاصه‌سازی اطلاعات ممیزی

کنترل: سیستم اطلاعاتی، قابلیت تهیه گزارشات و خلاصه‌سازی اطلاعات ممیزی را فراهم می‌کند. این قابلیت:

الف. از الزامات مرور، تحلیل و گزارش‌دهی ممیزی بر حسب تقاضا و همچنین از تحقیقات پس از رویدادهای امنیتی پشتیبانی می‌کند؛ و

ب. محتوای اصلی یا زمان‌بندی گزارشات ممیزی را تغییر نمی‌دهد.

راهنمایی‌های تکمیلی: خلاصه‌سازی اطلاعات ممیزی، فرایندی است که اطلاعات ممیزی گردآوری‌شده را دستکاری و در قالب خلاصه‌ای سازماندهی می‌کند. بدین ترتیب، تحلیل اطلاعات ممیزی آسان‌تر خواهد شد. قابلیت‌های تهیه گزارشات و خلاصه‌سازی اطلاعات ممیزی، همواره توسط یک سیستم اطلاعاتی یا بخش سازمانی که وظیفه ممیزی را انجام می‌دهد، فراهم نمی‌شوند. قابلیت خلاصه‌سازی اطلاعات ممیزی شامل مواردی از جمله روش‌های نوین داده‌کاوی است که از فیلترهای پیشرفته داده برای شناسایی رفتارهای غیر معمول در فعالیت‌های ممیزی بهره می‌برند. قابلیت تهیه گزارشات، که توسط سیستم اطلاعاتی ارائه می‌شود، منجر به تهیه گزارشاتی می‌شود که قابل شخصی‌سازی هستند. اگر ویژگی دانه‌بندی[۱۵۷] مهر زمانی[۱۵۸] در سوابق ممیزی مهم نباشد، زمان‌بندی سوابق ممیزی مسئله‌ای جدی خواهد بود. کنترل‌های مربوطه: AU-6.

کنترل پیشرفته:

(۱) تهیه گزارشات و خلاصه‌سازی اطلاعات ممیزی / پردازش خودکار

[157] granularity
[158] timestamp

سیستم اطلاعاتی، قابلیت پردازش سوابق ممیزی مربوط به رویدادهای مورد توجه را بر اساس [اختصاص: بخش‌هایی از سوابق ممیزی که توسط سازمان تعیین شده‌اند] فراهم می‌آورد.

راهنمایی‌های تکمیلی: رویدادهای مورد توجه را می‌توان با توجه به محتوای سوابق ممیزی خاص، تعیین نمود. این محتوا می‌تواند شامل مواردی از جمله هویت افراد، نوع رویداد، مکان رویداد، زمان رویداد، تاریخ رویداد، منابع سیستمی دخیل در فرایند، آدرس‌های IP دخیل در فرایند، یا اطلاعات گردآوری‌شده باشد. سازمان‌ها می‌توانند ملاک‌های ممیزی را تا سطح دانه‌بندی مورد نیاز، تعیین نمایند. به عنوان مثال، ممکن است مکان رویداد توسط مکان عمومی شبکه (مثلاً توسط شبکه یا یک زیرشبکه) یا توسط یکی از مؤلفه‌های خاص سیستم اطلاعاتی، تعیین گردد. کنترل‌های مربوطه: AU-2, AU-12.

(۲) تهیه گزارشات و خلاصه‌سازی اطلاعات ممیزی / مرتب‌سازی و جستجوی خودکار

سیستم اطلاعاتی، قابلیت مرتب‌سازی و جستجوی سوابق ممیزی برای یافتن رویدادهای مورد توجه را بر اساس [اختصاص: بخش‌هایی از سوابق ممیزی که توسط سازمان تعیین شده‌اند] فراهم می‌آورد.

راهنمایی‌های تکمیلی: مرتب‌سازی و جستجوی سوابق ممیزی بر اساس محتوای بخش‌های مختلف این اسناد انجام می‌شود. از جمله این بخش‌ها می‌توان به موارد روبرو اشاره کرد: (۱) تاریخ و زمان رویدادها، (۲) شناسه‌های هویتی کاربران، (۳) آدرس IP دخیل در رویداد، (۴) نوع رویداد، یا (۵) موفقیت یا شکست رویداد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب نشده، اولویت پایین	AU-7(1) اولویت متوسط	AU-7(1) اولویت بالا

AU-8: مهرهای زمانی

کنترل: سیستم اطلاعاتی:

الف. از ساعت داخلی سیستم جهت تولید مهرهای زمانی برای سوابق ممیزی استفاده می‌کند؛ و

ب. مهرهای زمانی را برای سوابق ممیزی ثبت می‌کند که می‌توان آن‌ها را به ساعت هماهنگ جهانی (UTC) و ساعت گرینویچ (GMT) تبدیل کرد و [اختصاص: دانه‌بندی تعیین‌شده توسط سازمان برای سنجش زمان] را رعایت نمود.

راهنمایی‌های تکمیلی: مهرهای زمانی تولیدشده توسط سیستم اطلاعاتی دارای زمان و تاریخ هستند. زمان معمولاً بر اساس ساعت هماهنگ جهانی بیان می‌شود که نسخه مدرن‌تر ساعت گرینویچ است، یا این که از تطابق ساعت محلی با ساعت هماهنگ جهانی استفاده می‌شود. منظور از دانه‌بندی سنجش زمان، میزان هماهنگی بین ساعت‌های سیستم اطلاعاتی و ساعت‌های مرجع است. به عنوان مثال، ساعت‌ها با دقت چند صد یا چند ده میلی ثانیه تنظیم می‌شوند. ممکن است سازمان‌ها دانه‌بندی‌های زمانی مختلفی را برای مؤلفه‌های مختلف سیستم در نظر گیرند. تنظیمات زمانی می‌تواند بر سایر قابلیت‌های امنیتی از جمله کنترل دسترسی، شناسایی و احراز هویت نیز تأثیرگذار باشد. این امر به ماهیت مکانیسم‌های مورد استفاده برای پشتیبانی از این قابلیت‌ها بستگی دارد. کنترل‌های مربوطه: AU-3, AU-12.

کنترل پیشرفته:

(۱) مهرهای زمانی / هماهنگی با مرجع زمانی معتبر

سیستم اطلاعاتی:

(الف) ساعت‌های داخلی سیستم اطلاعاتی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] با [اختصاص: مرجع زمانی معتبر تعیین‌شده توسط سازمان] مقایسه می‌کند؛ و

(ب) هنگامی که تفاوت زمانی بزرگتر از [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] باشد، ساعت‌های داخلی سیستم را با مرجع زمانی معتبر هماهنگ می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، مهرهای زمانی سیستم‌های اطلاعاتی دارای چند ساعت داخلی و همچنین مهرهای زمانی سیستم‌های متصل به هم از طریق شبکه را یکپارچه می‌کند.

(۲) مهرهای زمانی / مرجع زمانی معتبر ثانویه

سیستم اطلاعاتی، یک مرجع زمانی معتبر ثانویه را تعیین می‌کند که مکان جغرافیایی آن با مرجع معتبر اول تفاوت دارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AU-8 اولویت پایین	AU-8(1) اولویت متوسط	AU-8(1) اولویت بالا

AU-9: **حفاظت از اطلاعات ممیزی**

کنترل: سیستم اطلاعاتی، از اطلاعات و ابزارهای ممیزی در برابر پاک شدن، تغییر و دسترسی غیر مجاز محافظت می‌کند.

راهنمایی‌های تکمیلی: اطلاعات ممیزی شامل تمامی اطلاعات مورد نیاز برای ممیزی موفق فعالیت‌های سیستم اطلاعاتی است. این اطلاعات شامل مواردی مانند سوابق ممیزی، تنظیمات ممیزی، و گزارشات ممیزی هستند. تمرکز این کنترل بر حفاظت فنی از اطلاعات ممیزی است. حفاظت فیزیکی از اطلاعات ممیزی، در کنترل‌های مربوط به حفاظت از رسانه‌ها، حفاظت فیزیکی و حفاظت محیطی مطرح شده است. کنترل‌های مربوطه: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6.

کنترل پیشرفته:

(۱) حفاظت از اطلاعات ممیزی / رسانه‌های سخت‌افزاری با قابلیت یک‌بارنویسی[۱۵۹]

سیستم اطلاعاتی، اقدام به نوشتن روندهای ممیزی[۱۶۰] روی رسانه‌های سخت‌افزاری با قابلیت یک‌بارنویسی می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، در مورد تولید روندهای ممیزی (یعنی گردآوری سوابق ممیزی که اطلاعات ممیزی مورد استفاده در فرایندهای شناسایی، تحلیل و گزارش‌دهی را در بر می‌گیرند) صدق می‌کند و به عنوان یک نسخه پشتیبان برای این روندهای ممیزی عمل می‌نماید. کنترل پیشرفته حاضر، در مورد تولید سوابق ممیزی پیش از نوشته شدن در یک روند ممیزی صدق نمی‌کند. رسانه‌های با قابلیت یک‌بارنویسی و چندبارخوانی (WORM)[۱۶۱] شامل مواردی از جمله لوح فشرده قابل ضبط (CD-R) و لوح ویدئویی دیجیتال قابل ضبط (DVD-R) هستند. در مقابل، رسانه‌های غیر قابل نوشتن مانند نوارهای ضبط یا USB درایوها، قابلیت یک‌بارنویسی را ندارند. کنترل‌های مربوطه: AU-4, AU-5.

[159] Hardware write-once media
[160] Audit trail
[161] Write-once read-many media

(۲) حفاظت از اطلاعات ممیزی / تهیه نسخه پشتیبان اطلاعات ممیزی روی مؤلفه‌ها و سیستم‌های فیزیکی مجزا

سیستم اطلاعاتی، نسخه‌های پشتیبانی از سوابق ممیزی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] روی سیستم‌ها یا مؤلفه‌های دیگری، به جز سیستم‌ها و مؤلفه‌های در حال ممیزی شدن، تهیه می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، سبب می‌شود که به خطر افتادن سیستم اطلاعاتی مورد ممیزی، منجر به از دست رفتن اسناد و اطلاعات ممیزی نشود. کنترل‌های مربوطه: AU-4, AU-5, AU-11.

(۳) حفاظت از اطلاعات ممیزی / حفاظت رمزنگاری

سیستم اطلاعاتی، مکانیسم‌های رمزنگاری را برای حفاظت از صحت و یکپارچگی ابزارها و اطلاعات ممیزی به کار می‌گیرد.

راهنمایی‌های تکمیلی: مکانیسم‌های رمزنگاری مورد استفاده برای حفاظت از صحت و یکپارچگی اطلاعات ممیزی، شامل مواردی از جمله توابع درهم‌سازی امضاشده با استفاده از روش‌های رمزنگاری نامتقارن است. بدین ترتیب، می‌توان کلید عمومی را توزیع کرد و اطلاعات درهم‌سازی را تأیید نمود، و در عین حال محرمانگی کلید رمزی مورد استفاده برای تولید درهم‌ساز را نیز حفظ کرد. کنترل‌های مربوطه: AU-10, SC-12, SC-13.

(۴) حفاظت از اطلاعات ممیزی / دسترسی توسط زیرمجموعه‌ای از کاربران دارای امتیازات ویژه

سازمان اجازه مدیریت کارکرد ممیزی را تنها به [اختصاص: زیرمجموعه‌ای از کاربران دارای امتیازات ویژه که سازمان آن‌ها را تعیین کرده است] می‌دهد.

راهنمایی‌های تکمیلی: افراد دارای امتیازات ویژه دسترسی به یک سیستم اطلاعاتی که خود توسط سیستم ممیزی می‌شوند، ممکن است از فعالیت‌های ممیزی جلوگیری به عمل آورند یا سوابق ممیزی را دستکاری کنند و بدین ترتیب اعتبار اطلاعات ممیزی را زیر سؤال ببرند. این کنترل پیشرفته لازم می‌دارد که امتیازات ویژه مربوط به فعالیت‌های ممیزی و سایر امتیازات ویژه به شکل بهتری تعریف شوند و محدودیت‌هایی برای کاربران دارای امتیازات ممیزی ویژه در نظر گرفته شود. کنترل‌های مربوطه: AC-5.

(۵) حفاظت از اطلاعات ممیزی / فعالیت‌های نیازمند تأیید دوگانه

سازمان، فعالیت‌های نیازمند تأیید دوگانه جهت [انتخاب (یک یا چند مورد): جابجایی، حذف] [اختصاص: اطلاعات ممیزی تعیین‌شده توسط سازمان] را مشخص می‌نماید.

راهنمایی‌های تکمیلی: ممکن است سازمان‌ها انتخاب‌های دیگری را برای انواع مختلف اطلاعات ممیزی در نظر گیرند. اجرای مکانیسم‌های صدور مجوز دوگانه، نیازمند تأیید دو فرد دارای اختیار است. صدور مجوز دوگانه ممکن است با عنوان «کنترل توسط دو شخص» نیز معرفی شود. کنترل‌های مربوطه: AC-3, MP-2.

(۶) حفاظت از اطلاعات ممیزی / دسترسی تنها با مجوز خواندن

سازمان، امکان دسترسی به اطلاعات ممیزی تنها با مجوز خواندن را برای [اختصاص: زیرمجموعه‌ای از کاربران دارای امتیاز ویژه که توسط سازمان تعیین شده‌اند] فراهم می‌کند.

راهنمایی‌های تکمیلی: محدود کردن سطح دسترسی کاربران دارای امتیاز ویژه و صرفاً صدور مجوز خواندن برای آن‌ها، امکان وارد آمدن خسارت از سوی این کاربران را کاهش می‌دهد (در غیر این صورت، این افراد می‌توانند اطلاعات ممیزی را پاک کنند تا فعالیت‌های خرابکارانه خود را مخفی کنند).

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	AU-9 اولویت پایین	AU-9(4) اولویت متوسط	AU-9(2)(3)(4) اولویت بالا

AU-10: **عدم انکار**[۱۶۲]

کنترل: سیستم اطلاعاتی به افراد (یا فرایندهایی که از سوی آن‌ها فعالیت می‌کنند) اجازه نمی‌دهد که انجام [اختصاص: اقدامات مربوط به این بخش که از سوی سازمان تعیین می‌شوند] را به دروغ انکار کنند.

راهنمایی‌های تکمیلی: فعالیت‌هایی که در این دسته قرار می‌گیرند شامل مواردی از جمله تولید اطلاعات، ارسال و دریافت پیام، و تأیید اطلاعات (مانند تأیید وقوع یک رویداد یا امضا کردن یک قرارداد) هستند. خدمات عدم انکار، افراد را در برابر این ادعاها محافظت می‌کنند: (۱) ادعای نویسندگان مبنی بر عدم نوشتن اسناد خاص، (۲) ادعای ارسال‌کنندگان مبنی بر عدم ارسال پیام‌ها، (۳) ادعای دریافت‌کنندگان مبنی بر عدم دریافت پیام‌ها، یا (۴) ادعای امضاکنندگان مبنی بر عدم امضای اسناد. می‌توان با استفاده از این خدمات مشخص کرد که آیا

[162] Non-repudiation

اطلاعات از یک فرد خاص نشأت می‌گیرند، یا این که وی اقدامات خاصی را انجام داده (اقداماتی مانند ارسال یک ایمیل، امضای یک قرارداد، یا تأیید یک درخواست خاص) یا اطلاعات خاصی را دریافت کرده است. سازمان‌ها در ارائه خدمات عدم انکار، از روش‌ها و مکانیسم‌های مختلفی استفاده می‌کنند (روش‌هایی مانند امضای دیجیتال یا ارائه رسیدهای دیجیتال). کنترل‌های مربوطه: SC-12, SC-8, SC-13, SC-16, SC-17, SC-23.

کنترل پیشرفته:

(۱) عدم انکار / تعیین هویت تولیدکننده اطلاعات

سیستم اطلاعاتی:

(الف) هویت تولیدکننده اطلاعات را [اختصاص: تا حد تعیین‌شده توسط سازمان] با اطلاعات پیوند می‌دهد؛ و

(ب) ابزاری را برای تعیین هویت تولیدکننده اطلاعات در اختیار افراد مجاز قرار می‌دهد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، از آن دسته از الزامات ممیزی پشتیبانی می‌کند که کارکنان را قادر به تعیین هویت تولیدکننده اطلاعات می‌سازند. سازمان‌ها بر اساس دسته‌بندی امنیتی اطلاعات و عوامل مخاطرات مربوطه، سطح پیوند بین اطلاعات تولیدشده و هویت تولیدکننده آن‌ها را تعیین می‌کنند. کنترل‌های مربوطه: AC-4, AC-16.

(۲) عدم انکار / تأیید پیوند اطلاعات با تولیدکننده آن

سیستم اطلاعاتی:

(الف) پیوند اطلاعات با تولیدکننده آن را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] تأیید می‌کند؛ و

(ب) [اختصاص: اقدامات تعیین‌شده توسط سازمان] را، در صورت تأیید نشدن پیوند اطلاعات با تولیدکننده آن، انجام می‌دهد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، از تغییر و دستکاری اطلاعات در بازه زمانی بین تولید و مرور آن جلوگیری می‌نماید. برای تأیید پیوند اطلاعات با تولیدکننده آن می‌توان به عنوان مثال از چک‌لیست‌های رمزنگاری استفاده کرد. سازمان‌ها تعیین می‌کنند که آیا فرایند تأیید به درخواست کاربر صورت می‌گیرد یا باید به شکل خودکار انجام شود. کنترل‌های مربوطه: AC-3, AC-4, AC-16.

(۳) عدم انکار / زنجیره تغییرات

سیستم اطلاعاتی، برای تمامی اطلاعاتی که بازنگری و منتشر شده‌اند، هویت و اطلاعات مربوط به فرد بازنگری‌کننده یا منتشرکننده اطلاعات را ثبت و نگهداری می‌کند.

راهنمایی‌های تکمیلی: زنجیره تغییرات، فرایندی است که در آن روند جابجایی مدارک در جریان گردآوری، حفاظت، و تحلیل آن‌ها ثبت می‌شود. برای این کار، ثبت می‌شود که چه افرادی مدارک را مدیریت کرده‌اند یا تغییر داده‌اند، مدارک در چه زمان و تاریخی گردآوری یا منتقل شده‌اند، و هدف از این انتقال چه بوده است. اگر بازنگری توسط یک فرد انجام شده باشد یا این که توسط یک بخش خودکار اما مجزا از بخش انتشار/انتقال صورت گرفته باشد، سیستم اطلاعاتی هویت فرد بازنگری‌کننده اطلاعات را با اطلاعات و برچسب آن پیوند می‌دهد. در صورتی که بازنگری توسط یک فرد صورت گرفته باشد، این کنترل پیشرفته ابزاری برای مسئولین سازمان خواهد بود تا دریابند چه فردی اطلاعات را بازبینی و منتشر کرده است. در صورتی که بازنگری اطلاعات به صورت خودکار انجام شده باشد، این کنترل پیشرفته اطمینان حاصل می‌نماید که تنها از سیستم‌های مجاز و معتبر برای این کار استفاده شده است. کنترل‌های مربوطه: AC-4, AC-16.

(۴) عدم انکار / تأیید هویت بازنگری‌کننده اطلاعات

سیستم اطلاعاتی:

(الف) پیش از انتشار یا انتقال اطلاعات بین [اختصاص: بخش‌های امنیتی تعیین‌شده توسط سازمان]، پیوند اطلاعات را با هویت بازنگری‌کننده اطلاعات تأیید می‌کند؛ و

(ب) [اختصاص: اقدامات تعیین‌شده توسط سازمان] را، در صورت تأیید نشدن پیوند اطلاعات با بازنگری‌کننده آن، انجام می‌دهد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، از تغییر و دستکاری اطلاعات در بازه زمانی بین تولید و مرور آن جلوگیری می‌نماید. برای تأیید پیوند اطلاعات با تولیدکننده آن می‌توان به عنوان مثال از چک‌لیست‌های رمزنگاری استفاده کرد. سازمان‌ها تعیین می‌کنند که آیا فرایند تأیید به درخواست کاربر صورت می‌گیرد یا باید به شکل خودکار انجام شود. کنترل‌های مربوطه:AC-4, AC-16.

(۵) عدم انکار / امضاهای دیجیتال

[حذف شد: در بخش SI-7 گنجانده شد].

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	AU-10 اولویت بالا

AU-11: **نگهداری سوابق ممیزی**

کنترل: سازمان، سوابق ممیزی را برای [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] نگهداری می‌کند تا در بررسی رویدادهای امنیتی در آینده مورد استفاده قرار گیرند الزامات مقرراتی و اطلاعاتی سازمان رعایت شوند.

راهنمایی‌های تکمیلی: سازمان‌ها سوابق ممیزی را تا زمانی نگهداری می‌کنند که مشخص شود دیگر برای اهداف راهبری، قانونی، ممیزی یا سایر اهداف عملیاتی به آن‌ها نیاز نیست. به عنوان مثالی از این سوابق می‌توان به درخواست‌های مربوط به قانون آزادی اطلاعات (FOIA)، احضاریه‌ها و اسناد مربوط به اقدامات قانونی اشاره کرد. سازمان‌ها، دسته‌بندی‌های استانداردی از سوابق ممیزی را برای انواع مختلف اقدامات انجام‌شده تهیه می‌کنند. برنامه زمانی اسناد عمومی دفتر ملی بایگانی و مدارک آمریکا (NARA)، خط‌مشی‌های فدرال را در زمینه نگهداری سوابق ارائه کرده است. کنترل‌های مربوطه: AU-4, AU-5, AU-9, MP-6.

کنترل پیشرفته:

(۱) نگهداری سوابق ممیزی / قابلیت بازیابی طولانی مدت سوابق

سازمان با استفاده از [اختصاص: شاخص‌های تعیین‌شده توسط سازمان]، اطمینان حاصل می‌نماید که امکان بازیابی سوابق ممیزی طولانی مدت تهیه‌شده توسط سیستم اطلاعاتی وجود دارد.

راهنمایی‌های تکمیلی: شاخص‌های به کار گرفته شده توسط سازمان برای تسهیل بازیابی سوابق ممیزی شامل مواردی همچون قرار دادن سوابق در فرمت جدیدتر، حفظ تجهیزاتی که قادر به خواندن سوابق هستند، و نگهداری اسنادی است که کارکنان را یاری می‌کنند تا سوابق را تفسیر نمایند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	AU-11 اولویت پایین	AU-11 اولویت متوسط	AU-11 اولویت بالا

AU-12: **تولید سوابق ممیزی**

کنترل: سیستم اطلاعاتی:

الف. قابلیت تولید سوابق ممیزی برای رویدادهای قابل ممیزی را، چنان که در AU-2 تعریف شده است، در [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] فراهم می‌آورد؛

ب. به [اختصاص: نقش‌ها و کارکنان تعیین‌شده توسط سازمان] اجازه می‌دهد تا تعیین کنند کدام رویدادهای قابل ممیزی توسط مؤلفه‌های خاصی از سیستم اطلاعاتی، ممیزی می‌شوند؛ و

پ. سوابق ممیزی را برای رویدادهای تعریف‌شده در بخش ت AU-2 با محتوای تعریف‌شده در AU-3 تولید می‌کند.

راهنمایی‌های تکمیلی: سوابق ممیزی ممکن است در مؤلفه‌های مختلف سیستم اطلاعاتی تولید شوند. لیست رویدادهای ممیزی‌شده شامل رویدادهایی است که باید برای آن‌ها گزارش ممیزی تهیه کرد. این رویدادها به طور معمول زیرمجموعه‌ای از تمام رویدادهایی هستند که سیستم اطلاعاتی قابلیت تهیه گزارش‌های ممیزی را برای آن‌ها دارد. کنترل‌های مربوطه: AC-3, AU-2, AU-3, AU-6, AU-7.

کنترل پیشرفته:

(۱) تولید سوابق ممیزی / مسیر ممیزی[۱۶۳] سراسری سیستم با همبستگی زمانی

سیستم اطلاعاتی، سوابق ممیزی را از [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] در قالب یک مسیر ممیزی سراسری سیستم (منطقی یا فیزیکی) با هم ترکیب می‌کند که در محدوده [اختصاص: سطح رواداری[۱۶۴] تعیین‌شده توسط سازمان در زمینه رابطه بین مهرهای زمانی گزارشات موجود در مسیر ممیزی] دارای همبستگی زمانی است.

راهنمایی‌های تکمیلی: در صورتی که بتوان مهرهای زمانی گزارشات ممیزی را به مهرهای زمانی سایر گزارش‌های ممیزی ارتباط داد و مسیر زمانی گزارش‌ها را در حیطه رواداری سازمان تعیین نمود، مسیرهای ممیزی دارای همبستگی زمانی خواهند بود. کنترل‌های مربوطه: AU-8, AU-12.

(۲) تولید سوابق ممیزی / فرمت‌های استاندارد

سیستم اطلاعاتی، یک مسیر ممیزی (منطقی یا فیزیکی) سراسری سیستم را فراهم می‌آورد که از سوابق ممیزی با فرمت استاندارد تشکیل شده است.

---

[163] Audit trail
[164] Tolerance

راهنمایی‌های تکمیلی: اطلاعات ممیزی استاندارد، قابلیت همکاری و امکان جابجایی اطلاعات بین سیستم‌های اطلاعاتی و دستگاه‌های غیر مشابه را فراهم می‌آورد. بدین ترتیب، بهتر می‌توان اطلاعات مربوط به رویدادها را در یک قالب قابل تحلیل تهیه نمود. به عنوان نمونه‌ای از فرمت‌های استاندارد، می‌توان به سوابق ممیزی اشاره کرد که مطابق با استاندارد بیان مرسوم رویدادها (CEE)[۱۶۵] هستند. اگر مکانیسم‌های ثبت سوابق در سیستم‌های اطلاعاتی مطابق با فرمت‌های استاندارد نباشند، سیستم‌ها می‌توانند در هنگام تهیه مسیرهای ممیزی، گزارشات ممیزی را به فرمت استاندارد درآورند.

(۳) تولید سوابق ممیزی /تغییرات صورت‌گرفته توسط افراد مجاز

سیستم اطلاعاتی، [اختصاص: نقش‌ها و کارکنان تعیین‌شده توسط سازمان] را قادر می‌سازد تا فرایند ممیزی [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] را بر اساس [اختصاص: معیارهای قابل انتخاب تعیین‌شده توسط سازمان] و در محدوده [اختصاص: آستانه‌های زمانی تعیین‌شده توسط سازمان] تغییر دهند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، سازمان‌ها را قادر می‌سازد تا فرایند ممیزی را در صورت لزوم و به منظور برآورده ساختن الزامات سازمان، توسعه دهند یا محدود کنند. فرایند ممیزی که محدود به حفظ منابع سیستم اطلاعاتی است، ممکن است به گونه‌ای توسعه داده شود که برخی تهدیدات را نیز شامل گردد. علاوه بر این، ممکن است فرایند ممیزی محدود به مجموعه خاصی از رویدادها شود تا تحلیل و گزارش‌دهی ممیزی تسهیل گردد. سازمان‌ها می‌توانند آستانه‌های زمانی را برای تغییر اقدامات ممیزی در نظر گیرند. به عنوان مثال، ممکن است آستانه زمانی بلادرنگ، ظرف چند دقیقه، یا ظررف چند ساعت برای این امر در نظر گرفته شود. کنترل‌های مربوطه: AU-7.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	AU-12 اولویت پایین	AU-12 اولویت متوسط	AU-12(1)(3) اولویت بالا

AU-13: **پایش افشای اطلاعات**

[165] Common Event Expressions

کنترل: سازمان [اختصاص: سایت‌های اطلاعاتی و/یا اطلاعات منبع باز تعیین‌شده توسط سازمان] را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] پایش می‌کند تا موارد افشای غیر مجاز اطلاعات سازمانی مشخص گردد.

راهنمایی‌های تکمیلی: اطلاعات منبع باز شامل مواردی همچون سایت‌های شبکه اجتماعی هستند. کنترل‌های مربوطه: PE-3, SC-7.

کنترل پیشرفته:

(۱) پایش افشای اطلاعات / استفاده از ابزارهای خودکار

سازمان با استفاده از مکانیسم‌های خودکار تعیین می‌کند که آیا اطلاعات سازمانی به طور غیر مجاز افشا شده‌اند یا خیر.

راهنمایی‌های تکمیلی: به عنوان مثالی از مکانیسم‌های خودکار می‌توان از اسکریپت‌های خودکار مورد استفاده برای پایش پست‌های جدید در شبکه‌های اجتماعی و خدمات تجاری نام برد که نوتیفیکیشن‌ها و هشدارهایی را به سازمان‌ها ارسال می‌کنند.

(۲) پایش افشای اطلاعات / بازنگری سایت‌های پایش‌شده

سازمان، سایت‌های اطلاعات منبع باز که در حال پایش شدن هستند را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازنگری می‌کند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

AU-14: ممیزی نشست

کنترل: سیستم اطلاعاتی، این امکان را برای کاربران مجاز فراهم می‌آورد که یک نشست کاربری را برای ثبت و ضبط یا برای مشاهده و شنیدن انتخاب کنند.

راهنمایی‌های تکمیلی: ممیزی‌های نشست شامل مواردی از جمله پایش کلیدهای فشرده‌شده روی صفحه کلید، ردگیری وب‌سایت‌های بازدیدشده، و ثبت اطلاعات و/یا انتقال فایل‌ها هستند. فعالیت‌های ممیزی نشست بر اساس دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال تعیین و اجرا می‌شوند. کنترل‌های مربوطه: AC-3, AU-4, AU-5, AU-9, AU-11.

کنترل پیشرفته:

(۱) ممیزی نشست / راه‌اندازی سیستم

سیستم اطلاعاتی، ممیزی‌های نشست را در هنگام راه‌اندازی سیستم آغاز می‌کند.

(۲) ممیزی نشست/ ثبت اطلاعات

سیستم اطلاعاتی، این امکان را برای کاربران مجاز فراهم می‌آورد که محتوای مربوط به یک نشست کاربری را ثبت و ضبط کنند.

(۳) ممیزی نشست/ مشاهده و شنیدن از راه دور

سیستم اطلاعاتی، این امکان را برای کاربران مجاز فراهم می‌آورد که تمامی محتوای مربوط به یک نشست کاربری را به صورت بلادرنگ و از راه دور ثبت و ضبط کنند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

AU-15: **قابلیت ممیزی جایگزین**

کنترل: سازمان، یک قابلیت ممیزی جایگزین را فراهم می‌آورد تا در صورت از کار افتادن قابلیت ممیزی اولیه، [اختصاص: کارکردهای ممیزی جایگزین تعیین‌شده توسط سازمان] را انجام دهد.

راهنمایی‌های تکمیلی: از آنجا که قابلیت‌های ممیزی جایگزین به عنوان یک حفاظت کوتاه‌مدت و تا هنگامی که سیستم اولیه به فعالیت خود ادامه دهد مورد استفاده قرار می‌گیرند، ممکن است سازمان تصمیم بگیرد که

قابلیت ممیزی جایگزین، تنها زیرمجموعه‌ای از کارکردهای ممیزی اولیه که دچار اخلال شده‌اند را ارائه کند. کنترل‌های مربوطه: AU-5.

کنترل پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

AU-16: ممیزی بین‌سازمانی

کنترل: سازمان، [اختصاص: روش‌های تعیین‌شده توسط سازمان] را به کار می‌گیرد و با استفاده از آن‌ها [اختصاص: اطلاعات ممیزی تعیین‌شده توسط سازمان] را در هنگام جابجایی بین مرزهای سازمان‌ها تنظیم و مدیریت می‌کند.

راهنمایی‌های تکمیلی: هنگامی که سازمان‌ها از خدمات و/یا سیستم‌های اطلاعاتی سازمان‌های دیگر استفاده می‌کنند، برای استفاده از قابلیت‌های ممیزی لازم است که تمام سازمان‌ها روش هماهنگی را به کار گیرند. به عنوان مثال، شناسایی هویت افرادی که درخواست استفاده از خدمات خاصی را در بین مرزهای سازمانی دارند معمولاً بسیار دشوار است و نیاز به انجام فعالیت‌ها و هماهنگی‌های زیادی دارد. بنابراین، در فرایندهای ممیزی بین‌سازمانی (مانند نوعی از قابلیت ممیزی که در معماری‌های سرویس‌محور ارائه می‌شود)، معمولاً هویت افرادی که موردی را از سیستم اطلاعاتی اولیه درخواست کرده‌اند ثبت می‌شود و سیستم‌های بعدی نیز تأیید می‌کنند که درخواست از سوی یک فرد مجاز مطرح شده است. کنترل‌های مربوطه: AU-6.

کنترل پیشرفته:

(۱) ممیزی بین‌سازمانی / ثبت و نگهداری هویت

سازمان الزام می‌دارد که هویت افراد در مسیر ممیزی بین‌سازمانی ثبت و نگهداری شود.

راهنمایی‌های تکمیلی: این کنترل پیشرفته هنگامی به کار گرفته می‌شود که نیاز باشد اقدامات انجام‌شده در بین مرزهای سازمانی، با هویت یک فرد خاص ارتباط داده شود.

(۲) ممیزی بین‌سازمانی / اشتراک‌گذاری اطلاعات ممیزی

سازمان، بر اساس [اختصاص: موافقت‌نامه‌های تعیین‌شده توسط سازمان در زمینه اشتراک‌گذاری اطلاعات بین سازمان‌ها]، اطلاعات سازمانی بین‌سازمانی را در اختیار [اختصاص: سازمان‌های تعیین‌شده توسط سازمان] قرار می‌دهد.

راهنمایی‌های تکمیلی: به دلیل ماهیت توزیع‌شده اطلاعات ممیزی، اشتراک‌گذاری اطلاعات ممیزی بین‌سازمانی امری ضروری برای تحلیل اثربخش فرایند ممیزی به شمار می‌آید. به عنوان مثال، سوابق ممیزی یک سازمان ممکن است اطلاعات کافی را برای تعیین کاربرد مناسب یا نامناسب منابع اطلاعاتی سازمانی توسط افرادی در سازمان‌های دیگر ارائه نکند. در برخی موارد، تنها سازمان اصلی این افراد می‌تواند در این خصوص تصمیم‌گیری کند. بنابراین، لازم است که اطلاعات ممیزی بین سازمان‌ها به اشتراک گذاشته شوند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

خانواده: صدور مجوز و بررسی امنیتی

CA-1: خط‌مشی و روش‌های اجرایی صدور مجوز و بررسی امنیتی

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۵. خط‌مشی صدور مجوز و بررسی امنیتی شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و
۶. رویه‌های تسهیل پیاده‌سازی خط‌مشی صدور مجوز و بررسی امنیتی و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] مرور و به‌روز می‌کند:

۵. خط‌مشی صدور مجوز و بررسی امنیتی ؛ و
۶. رویه‌های صدور مجوز و بررسی امنیتی.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل های خانواده CA را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. استراتژی مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: شماره‌های ویژه NIST 800-12, 800-37, 800-53, 800-100.

اولویت و تخصیص به مجموعه‌های پایه:

P1	CA-1 اولویت پایین	CA-1 اولویت متوسط	CA-1 اولویت بالا

CA-2: بررسی‌های امنیتی

کنترل: سازمان:

الف. یک طرح بررسی امنیتی را تهیه می‌کند که دامنه شمول بررسی و موارد زیر را تشریح می‌کند:

۱. کنترل‌های امنیتی و کنترل‌های پیشرفته مورد بررسی؛
۲. رویه‌های برسی مورد بررسی برای تعیین اثربخشی کنترل‌های امنیتی؛ و
۳. محیط بررسی، تیم بررسی، و مسئولیت‌ها و نقش‌های بررسی؛

ب. کنترل‌های امنیتی موجود در سیستم‌های اطلاعاتی و محیط کاری مربوطه را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بررسی می‌کند تا تعیین شود که کنترل‌های مذکور تا چه حد به درستی پیاده‌سازی شده‌اند، مطابق با اهداف عمل کرده‌اند، به نتایج مطلوب ختم شده‌اند و مبتنی بر الزامات امنیتی بوده‌اند؛

پ. یک گزارش بررسی امنیتی را تهیه می‌کند که نتایج بررسی در آن مستندسازی شده‌اند؛ و

ت. نتایج بررسی کنترل‌های امنیتی را در اختیار [اختصاص: نقش‌ها یا افراد تعیین‌شده توسط سازمان] قرار می‌دهد.

راهنمایی‌های تکمیلی: سازمان‌ها، کنترل‌های امنیتی موجود در سیستم‌های اطلاعاتی و محیط کاری مربوطه را به عنوان بخشی از این فرایندها بررسی می‌کنند: (۱) صدور مجوز اولیه و مستمر؛ (۲) بررسی‌های سالانه FISMA؛ (۳) پایش مستمر؛ و (۴) فعالیت‌های مربوط به چرخه عمر توسعه سیستم. بررسی‌های امنیتی: (۱) اطمینان حاصل می‌کنند که امنیت اطلاعات در سیستم‌های اطلاعاتی سازمان به طور خاص مورد توجه قرار گرفته است؛ (۲) کاستی‌ها و نقاط ضعف را در مراحل اول توسعه شناسایی می‌کنند؛ (۳) اطلاعات لازم برای اتخاذ تصمیمات مبتنی بر مخاطره را به عنوان بخشی از فرایندهای صدور مجوز امنیتی فراهم می‌آورند؛ و (۴) اطمینان حاصل می‌کنند که رویه‌های کاهش کاستی‌ها مورد توجه قرار گرفته‌اند و از آن‌ها تبعیت شده است. این بررسی‌ها، بر اساس آنچه در طرح‌های امنیت سیستم و طرح‌های برنامه امنیت اطلاعات گفته شده است، در خصوص کنترل‌های امنیتی مورد اشاره در پیوست ج (کاتالوگ اصلی) و کنترل چ (کنترل‌های مدیریت برنامه)

صورت می‌گیرند. سازمان‌ها می‌توانند از انواع دیگر بررسی‌ها مانند پایش کاستی‌ها و نظارت بر سیستم نیز برای حصول اطمینان از عملکرد امنیتی مطلوب سیستم‌های اطلاعاتی در سرتاسر چرخه عمر آن‌ها استفاده کنند. گزارش‌های بررسی امنیتی، نتایج را با جزئیات کافی مستندسازی می‌کنند. سازمان می‌تواند بر اساس این نتایج، دقیق و کامل بودن گزارشات را تعیین کند و مشخص نماید که کنترل‌های امنیتی تا چه حد به درستی پیاده‌سازی شده‌اند، مطابق با اهداف عمل کرده‌اند، به نتایج مطلوب ختم شده‌اند و مبتنی بر الزامات امنیتی بوده‌اند. FISMA در الزامات خود بیان کرده است که کنترل‌های امنیتی باید دست کم یک بار در سال بررسی شوند. در این الزامات، به لزوم انجام بررسی‌های دیگر، علاوه بر آنچه در فرایندهای صدور مجوز امنیتی سازمان صورت می‌گیرد، اشاره‌ای نشده است. نتایج بررسی‌های امنیتی در اختیار نقش‌ها و افراد مسئول قرار می‌گیرند. به عنوان مثال، بررسی‌های انجام‌شده برای پشتیبانی از تصمیمات صدور مجوز امنیتی، در اختیار مسئولین صدور مجوز یا نمایندگان آن‌ها قرار داده می‌شوند.

برای رعایت الزام انجام بررسی‌های سالانه، سازمان‌ها می‌توانند از نتایج بررسی‌های به دست آمده از این منابع استفاده کنند: (۱) صدور مجوز اولیه یا مستمر سیستم‌های اطلاعاتی؛ (۲) پایش پیوسته؛ یا (۳) فعالیت‌های مربوط به چرخه عمر توسعه سیستم. سازمان‌ها باید اطمینان حاصل کنند که نتاج بررسی‌های امنیتی، به‌روز و تعیین‌کننده اثربخشی کنترل‌های امنیتی هستند و فرد یا نهاد تهیه‌کننده آن‌ها از استقلال کافی برخوردار بوده است. در صورتی که نتایج بررسی‌های هنوز معتبر باشند، می‌توان باز هم از آن‌ها استفاده کرد یا آن‌ها را با انجام بررسی‌های بیشتر تکمیل نمود. سازمان‌ها پس از صدور مجوز اولیه و بر اساس خط‌مشی OMB، پایش‌های پیوسته‌ای را انجام می‌دهند تا کنترل‌های امنیتی را به طور منظم بررسی نمایند. سازمان‌ها بر اساس راهبردهای پایش پیوسته خود تعیین می‌کنند که بررسی کنترل‌های امنیتی در چه بازه‌های زمانی انجام شود. هشدارهای آسیب‌پذیری ضمانت اطلاعات[۱۶۶]، مثال مناسبی از رویه‌های کاهش کاستی‌ها هستند. ممیزی‌های خارجی (مانند ممیزی‌های انجام‌شده توسط مؤسسات خارجی مانند ادارات قانونی) خارج از دامنه شمول این کنترل هستند. کنترل‌های مربوطه: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.

کنترل‌های پیشرفته:

(۱) بررسی‌های امنیتی / بررسی‌کنندگان مستقل

سازمان، بررسی‌کنندگان و تیم‌های بررسی را با [اختصاص: سطح استقلال تعیین‌شده توسط سازمان] به کار می‌گیرد تا وظیفه بررسی کنترل‌های امنیتی را انجام دهند.

[166] Information Assurance Vulnerability Alert

راهنمایی‌های تکمیلی: بررسی‌کنندگان یا تیم‌های بررسی مستقل، افراد یا گروه‌هایی هستند که سیستم‌های اطلاعاتی سازمان را به صورت بی‌طرفانه بررسی می‌کنند. منظور از بی‌طرفی این است که بررسی‌کنندگان، هیچ زیان یا منفعتی در زمینه توسعه، اجرایی کردن و مدیریت سیستم‌های اطلاعاتی سازمانی مورد بررسی، یا تعیین اثربخشی کنترل‌های امنیتی ندارند. بررسی‌کنندگان باید برای دستیابی به بی‌طرفی، از موارد روبرو پرهیز کنند: (۱) ایجاد منافع مشترک یا متضاد با سازمان‌های مورد بررسی؛ (۲) بررسی کار خود؛ (۳) کار به عنوان مدیر یا کارمند سازمان‌های مورد بررسی؛ و (۴) نمایندگی کردن سازمان‌هایی که خدمات آن‌ها را دریافت می‌کنند. بررسی‌های مستقل می‌توانند توسط بخش‌هایی از سازمان ارائه شوند، یا این که سازمان‌ها می‌توانند این فعالیت‌ها را به سازمان‌های بخش خصوصی یا دولتی برون سپاری کنند. مسئولین صدور مجوز، سطح استقلال مورد نیاز را بر اساس قابلیت‌های امنیتی سیستم‌های اطلاعاتی و/یا مخاطرات موجود در برابر عملیات، سرمایه‌های سازمانی و افراد، تعیین می‌نمایند. مسئولین مذکور همچنین تعیین می‌کنند که ایا میزان استقلال بررسی‌کنندگان کافی است و بر اساس گزارشات آنان می‌توان تصمیمات معتبری اتخاذ کرد یا خیر. آن‌ها مشخص می‌کنند که آیا خدمات بررسی امنیتی از استقلال کافی برخوردار هستند یا خیر؛ به عنوان مثال تعیین می‌کنند که آیا مالکان سیتم‌های اطلاعاتی نقش مستقیمی در بررسی‌ها ایفا کرده‌اند یا خیر. در برخی شرایط خاص، مثلاً هنگامی که سازمان‌های مالک سیستم‌های اطلاعاتی، کوچک باشند یا لازم باشد بررسی‌ها توسط افرادی انجام شود که خود در فرایند توسعه، اجرا، یا مدیریت سیستم‌های اطلاعاتی نقش دارند، می‌توان برای حصول اطمینان از استقلال بررسی‌ها، گروهی از متخصصان مستقل و بی‌طرف را به کار گرفت تا بر نتایج بررسی‌ها نظارت نمایند. سازمان‌ها دریافته‌اند که بررسی‌های انجام‌شده توسط افراد و گروه‌های مستقل، درجه اعتبار بالاتری دارند و نیاز به تکرار بررسی‌ها را کاهش خواهند داد.

(۲) بررسی‌های امنیتی / بررسی‌های تخصصی

سازمان [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان]، فعالیت‌های [انتخاب: با اعلام قبلی، بدون اعلام قبلی] [انتخاب (یک یا چند مورد): پایش جامع و دقیق، بررسی آسیب‌پذیری‌ها، آزمایش فعالیت‌های مخرب کاربران، بررسی تهدیدات داخلی، آزمایش عملکرد و بار، [اختصاص: انواع دیگر بررسی‌های تعیین‌شده توسط سازمان]] را در بررسی‌های امنیتی خود وارد می‌کند.

راهنمایی‌های تکمیلی: سازمان‌ها می‌توانند با استفاده از فعالیت‌هایی همچون نظارت بر سیستم‌های اطلاعاتی، بررسی تهدیدات داخلی، آزمایش فعالیت‌های مخرب کاربران یا سایر انواع بررسی‌ها (از جمله تأیید و اعتبارسنجی)، قابلیت‌های سازمانی و سطح عملکرد موجود را مشخص کنند و تعیین نمایند که

برای ارتقای امنیت چه باید کرد. سازمان‌ها، بررسی‌های امنیتی خود را بر اساس دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال انجام می‌دهند. مسئولین صدور گواهی روش‌های بررسی را با توجه به نتیجه تحلیل مخاطرات سازمان تأیید می‌کنند. سازمان‌ها می‌توانند آسیب‌پذیری‌های مشاهده‌شده در جریان بررسی‌ها را در فرایند جبران آسیب‌پذیری‌ها مورد توجه قرار دهند. کنترل‌های مربوطه: PE-3, SI-2.

(۳) بررسی‌های امنیتی / سازمان‌های خارجی

سازمان، هنگامی نتایج بررسی [اختصاص: سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] انجام‌شده توسط [اختصاص: سازمان‌های خارجی تعیین‌شده توسط سازمان] را می‌پذیرد که بررسی‌ها مطابق با [اختصاص: الزامات تعیین‌شده توسط سازمان] باشند.

راهنمایی‌های تکمیلی: سازمان‌ها در اکثر مواقع نتایج بررسی‌های انجام‌شده توسط سازمان‌های دیگر در مورد سیستم‌های اطلاعاتی خاص را مورد استفاده قرار می‌دهند. استفاده از این بررسی‌ها (یعنی استفاده مجدد از نتایج بررسی موجود) سبب می‌شود که سازمان‌ها نیاز کمتری به انجام بررسی‌های مستقل داشته باشند و بدین ترتیب صرفه‌جویی قابل توجهی در زمان و منابع مورد استفاده صورت می‌گیرد. عوامل مختلفی تعیین‌کننده امکان استفاده مجدد از نتایج موجود هستند. به عنوان مثالی از این عوامل می‌توان به تجربیات گذشته بررسی یک سازمان توسط سازمانی دیگر، شهرت و اعتبار سازمان در زمینه بررسی، میزان اطلاعات ارائه‌شده در اسناد بررسی، یا موارد خواسته‌شده از سازمان‌ها در قوانین، خط‌مشی‌ها و رهنمودهای فدرال اشاره کرد.

مراجع: دستور اجرایی ۱۳۵۸۷، FIPS 199، شماره‌های ویژه NIST 800-37, 800-39, 800-53, 800-115, 800-137.

اولویت و تخصیص به مجموعه‌های پایه:

P2	CA-2 اولویت پایین	CA-2(1) اولویت متوسط	CA-2(1)(2) اولویت بالا

CA-3: ارتباطات درونی سیستم‌ها

کنترل: سازمان:

الف. اجازه اتصال سیستم اطلاعاتی به سایر سیستم‌های اطلاعاتی از طریق موافقت‌نامه امنیتی ارتباطات درونی[۱۶۷] را فراهم می‌آورد؛

ب. ویژگی‌های واسط و الزامات امنیتی، و همچنین ماهیت اطلاعات ردوبدل‌شده را برای هر یک از ارتباطات درونی مستندسازی می‌کند؛ و

پ. موافقت‌نامه‌های امنیتی ارتباطات درونی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روزرسانی می‌کند.

راهنمایی‌های تکمیلی: این کنترل مربوط به ارتباطات بین سیستم‌های اطلاعاتی است (یعنی ارتباطات درونی سیستم‌ها) و در مورد ارتباطات موقتی و کنترل‌شده توسط کاربر، مانند ایمیل‌ها و مرورهای اینترنتی، صدق نمی‌کند. سازمان‌ها به دقت مخاطرات مربوط به اتصال سیستم‌های اطلاعاتی به سیستم‌های دیگری با الزامات امنیتی و کنترل‌های امنیتی متفاوت را بررسی می‌کنند؛ چه این سیستم‌های اطلاعاتی در درون سازمان و چه خارج از سازمان قرار داشته باشند. مسئولین صدور مجوز، مخاطرات مربوط به اتصال سیستم‌های اطلاعاتی را تعیین می‌کنند و مشخص می‌نمایند که از چه کنترل‌های امنیتی باید در این خصوص استفاده کرد. اگر سیستم‌های متصل‌شده دارای مسئولین صدور مجوز واحدی باشند، نیازی به امضای موافقت‌نامه‌های امنیتی ارتباطات درونی بین سازمان‌ها نخواهد بود. در این شرایط، سازمان‌ها می‌توانند در طرح‌های امنیتی خود به تشریح واسطه‌های مورد استفاده بین این سیستم‌ها بپردازند. اگر سیستم‌های متصل به هم، مسئولین صدور مجوز مختلفی در درون یک سازمان واحد داشته باشند، سازمان‌ها می‌توانند موافقت‌نامه‌های امنیتی ارتباطات درونی را تهیه کنند یا ویژگی‌های واسطه‌های مورد استفاده بین این سیستم‌ها را در طرح امنیتی مربوط به هر سیستم تشریح نمایند. سازمان‌ها همچنین می‌توانند موافقت‌نامه‌های امنیتی ارتباطات درونی را در قرادادهای اصلی بگنجانند. این امر به ویژه در مورد روابط کاری بین سازمان‌های فدرال و غیر فدرال (یعنی سازمان‌های بخش خصوصی) صدق می‌کند. در مورد سیستم‌های اطلاعاتی که از شبکه‌های یکسانی استفاده می‌کنند، باید ملاحظات مربوط به مخاطرات را نیز در نظر گرفت. در مورد برخی فناوری‌های خاص (مانند فناوری‌های فضایی، سفینه‌های فضایی بدون سرنشین، و دستگاه‌های پزشکی و درمانی)، ممکن است در جریان آزمایشات اولیه، ارتباطات خاصی بین آن‌ها وجود داشته باشد. ممکن است این ارتباطات سبب نیاز به موافقت‌نامه‌های امنیتی

167 Interconnection Security Agreements

ارتباطات درونی یا مجموعه‌ای از کنترل‌های امنیتی اضافی شوند. کنترل‌های مربوطه: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

کنترل‌های پیشرفته:

(۱) ارتباطات درونی سیستم‌ها / ارتباطات بین سیستم‌های امنیت ملی غیر محرمانه

سازمان از ارتباط مستقیم یک [اختصاص: سیستم امنیت ملی غیر محرمانه تعیین‌شده توسط سازمان] و یک شبکه خارجی، بدون استفاده از [اختصاص: دستگاه حفاظت مرزی تعیین‌شده توسط سازمان]، جلوگیری می‌کند.

راهنمایی‌های تکمیلی: سازمان‌ها معمولاً کنترلی بر شبکه‌های خارجی (مانند اینترنت) ندارند. دستگاه‌های مورد تأیید حفاظت مرزی (مانند مسیریاب‌ها و فایروال‌ها) به عنوان واسط ارتباطی بین سیستم‌های امنیت ملی غیر محرمانه و شبکه‌های خارجی عمل می‌کنند. این کنترل پیشرفته برای سازمان‌هایی که اطلاعات غیر محرمانه کنترل‌شده (CUI) را پردازش، ذخیره یا منتقل می‌کنند، ضروری است.

(۲) ارتباطات درونی سیستم‌ها / ارتباطات بین سیستم‌های امنیت ملی محرمانه

سازمان از ارتباط مستقیم یک سیستم امنیت ملی محرمانه و یک شبکه خارجی، بدون استفاده از [اختصاص: دستگاه حفاظت مرزی تعیین‌شده توسط سازمان]، جلوگیری می‌کند.

راهنمایی‌های تکمیلی: سازمان‌ها معمولاً کنترلی بر شبکه‌های خارجی (مانند اینترنت) ندارند. دستگاه‌های مورد تأیید حفاظت مرزی (مانند مسیریاب‌ها و فایروال‌ها) به عنوان واسط ارتباطی بین سیستم‌های امنیت ملی محرمانه و شبکه‌های خارجی عمل می‌کنند. علاوه بر این، دستگاه‌های مورد تأیید حفاظت مرزی (معمولاً شامل سیستم‌های بین‌دامنه‌ای با واسط‌های مدیریت‌شده) امکان جریان اطلاعات بین سیستم‌های اطلاعاتی و شبکه‌های خارجی را فراهم می‌آورند.

(۳) ارتباطات درونی سیستم‌ها / ارتباطات بین سیستم‌های امنیت غیر ملی غیر محرمانه

سازمان از ارتباط مستقیم یک [اختصاص: سیستم امنیت غیر ملی غیر محرمانه تعیین‌شده توسط سازمان] و یک شبکه خارجی، بدون استفاده از [اختصاص: دستگاه حفاظت مرزی تعیین‌شده توسط سازمان]، جلوگیری می‌کند.

راهنمایی‌های تکمیلی: سازمان‌ها معمولاً کنترلی بر شبکه‌های خارجی (مانند اینترنت) ندارند. دستگاه‌های مورد تأیید حفاظت مرزی (مانند مسیریاب‌ها و فایروال‌ها) به عنوان واسط ارتباطی بین

سیستم‌های امنیت غیر ملی غیر محرمانه و شبکه‌های خارجی عمل می‌کنند. این کنترل پیشرفته برای سازمان‌هایی که اطلاعات غیر محرمانه کنترل‌شده (CUI) را پردازش، ذخیره یا منتقل می‌کنند، ضروری است.

(۴) ارتباطات درونی سیستم‌ها / ارتباط با شبکه‌های عمومی

سازمان از ارتباط مستقیم یک [اختصاص: سیستم اطلاعاتی تعیین‌شده توسط سازمان] و یک شبکه عمومی جلوگیری می‌کند.

راهنمایی‌های تکمیلی: شبکه عمومی به هر شبکه‌ای گفته می‌شود که عموم مردم امکان دسترسی به آن را داشته باشند. به عنوان مثال، می‌توان به اینترنت یا اکسترانت‌های سازمانی اشاره کرد که در دسترس همگان قرار دارند.

(۵) ارتباطات درونی سیستم‌ها / محدودیت‌های موجود در زمینه ارتباط با سیستم‌های خارجی

سازمان بر اساس خط‌مشی [انتخاب: صدور مجوز برای همه، عدم صدور مجوز با استثنا؛ عدم صدور مجوز برای همه، صدور مجوز با استثنا]، به [اختصاص: سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] اجازه می‌دهد تا به سیستم‌های اطلاعاتی خارجی متصل شوند.

راهنمایی‌های تکمیلی: سازمان‌ها می‌توانند قابلیت اتصال سیستم‌های اطلاعاتی با دامنه‌های خارجی (مانند وبسایت‌ها) را با استفاده از یکی از این دو خط‌مشی، محدود نمایند: (۱) خط‌مشی «صدور مجوز برای همه، عدم صدور مجوز با استثنا»، که به آن «تهیه لیست سیاه» هم می‌گویند (این خط‌مشی نسبت به خط مشی دیگر ضعیف‌تر است)؛ یا (۲) خط‌مشی «عدم صدور مجوز برای همه، صدور مجوز با استثنا» که به آن «تهیه لیست سفید» هم می‌گویند. در مورد هر یک از این دو خط‌مشی، سازمان‌ها باید موارد استثنا را در صورت لزوم مشخص نمایند. کنترل مربوطه: CM-7.

مراجع: FIPS 199، شماره ویژه NIST 800-47.

اولویت و تخصیص به مجموعه‌های پایه:

P1	CA-3 اولویت پایین	CA-3(5) اولویت متوسط	CA-3(5) اولویت بالا

CA-4: صدور گواهی امنیتی

[حذف شد: در بخش CA-2 گنجانده شد].

CA-5: **طرح عملیاتی و مراحل اصلی**

کنترل: سازمان:

الف. طرح عملیاتی و مراحل اصلی را برای سیستم اطلاعاتی تعیین می‌کند تا بر اساس آن، اقدامات جبرانی طرح‌ریزی شوند و نقاط ضعف و آسیب‌پذیری‌هایی که در بررسی‌ها مشخص شده‌اند، اصلاح شوند و آسیب‌پذیری‌های سیستم برطرف شوند؛ و

ب. طرح عملیاتی و مراحل اصلی که قبلاً تهیه شده‌اند را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بر اساس نتایج بررسی کنترل‌های امنیتی، تحلیل اثرات امنیتی و نظارت‌های مستمر، به‌روزرسانی می‌کند.

راهنمایی‌های تکمیلی: طرح‌های عملیاتی و مراحل اصلی، از جمله اسناد مهم موجود در بسته صدور مجوز امنیتی هستند و الزامات گزارش‌دهی فدرال در مورد آن‌ها صدق می‌کند. کنترل‌های مربوطه: CA-2, CA-7, CM-4, PM-4.

کنترل‌های پیشرفته:

(۱) طرح عملیاتی و مراحل اصلی / استفاده از روش‌های خودکارسازی برای ارتقای دقت و به‌روزرسانی
سازمان با استفاده از مکانیسم‌های خودکار اطمینان حاصل می‌نماید که طرح عملیاتی و مراحل مهم تعیین‌شده در مورد سیستم‌های عملیاتی، دقیق و به‌روز و در دسترس هستند.

مراجع: تفاهم‌نامه OMB 02-01، شماره ویژه NIST 800-37.

اولویت و تخصیص به مجموعه‌های پایه:

P3	CA-5 اولویت پایین	CA-5 اولویت متوسط	CA-5 اولویت بالا

CA-6: **صدور مجوز امنیتی**

کنترل: سازمان:

الف. یک مدیر اجرایی ارشد را به عنوان مسئول صدور مجوز سیستم‌های اطلاعاتی منصوب می‌کند؛

ب. اطمینان حاصل می‌کند که مسئول صدور مجوز، پیش از آغاز عملیات اقدام به بررسی و صدور مجوز سیستم اطلاعاتی می‌نماید؛ و

پ. مجوز امنیتی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] به‌روزرسانی می‌کند.

راهنمایی‌های تکمیلی: مجوزهای امنیتی در واقع نوعی تصمیم مدیریتی هستند که در اسناد مربوطه و توسط مدیران یا مقامات ارشد سازمان (یعنی مسئولین صدور مجوز) ثبت می‌شوند تا اجازه فعالیت سیستم‌های اطلاعاتی سازمانی را صادر کنند. سازمان بر اساس این مجوزها، مخاطرات موجود در برابر سرمایه‌ها و عملیات سازمانی، افراد، سایر سازمان‌ها و مردم را با به‌کارگیری کنترل‌های امنیتی مناسب می‌پذیرد. مسئولین صدور مجوز سازمانی، بودجه لازم برای سیستم‌های اطلاعاتی را تعیین می‌کنند و همچنین مسئولیت انجام مأموریت‌ها و فرایندهای کسب‌وکار سازمان را مشخص می‌نمایند. فرایند صدور مجوز امنیتی، یک مسئولیت فدرال است و بنابراین لازم است که مسئولین صدور مجوز، از کارکنان فدرال باشند. مسئولین صدور محوز، در قبال مخاطرات مربوط به استفاده از سیستم‌های اطلاعاتی سازمانی پاسخگو خواهند بود. اختیارات این مسئولین نیز متناسب با این مخاطرات امنیتی خواهد بود. به موجب خط‌مشی OMB، سازمان‌ها باید برنامه‌های نظارت مستمری را به کار گیرند و بدین ترتیب مجوز فعالیت سیستم‌های اطلاعاتی را به طور منظم و مستمر تمدید نمایند. با پیاده‌سازی برنامه‌های نظارت مستمر می‌توان تا سه سال مجوز فعالیت سیستم‌های اطلاعاتی را تمدید کرد، بدون این که نیاز به صدور مجوز مجدد باشد. از طریق پیاده‌سازی برنامه‌های نظارت مستمر جامع، اطلاعات مهم موجود در بسته‌های صدور مجوز (یعنی طرح‌های امنیتی، گزارشات بررسی امنیتی، و برنامه‌های عملیاتی و مراحل مهم) به طور منظم به‌روزرسانی می‌شوند. بدین ترتیب، مسئولین صدور مجوز و مالکان سیستم‌های اطلاعاتی، از وضعیت امنیتی فعلی سیستم‌های اطلاعاتی و محیط کاری آن‌ها آگاه خواهند شد. به منظور کاهش هزینه‌های راهبردی صدور مجوز امنیتی مجدد، مسئولین صدور مجوز تا حد امکان از نتایج فرایندهای بررسی پیوسته استفاده می‌کنند. کنترل‌های مربوطه: CA-2, CA-7, PM-9, PM-10.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: بخشنامه OMB A-130، تفاهم‌نامه OMB 11-33، شماره‌های ویژه NIST 800-37, 800-137.

اولویت و تخصیص به مجموعه‌های پایه:

P2	CA-6 اولویت پایین	CA-6 اولویت متوسط	CA-6 اولویت بالا

CA-7: **نظارت پیوسته**

کنترل: سازمان، یک راهبرد نظارت پیوسته را به کار می‌گیرد و برنامه نظارت پیوسته‌ای را پیاده‌سازی می‌نماید که شامل مراحل زیر است:

الف. تعیین [اختصاص: معیارهای تعیین‌شده توسط سازمان] که باید بر آن‌ها نظارت نمود؛

ب. تعیین [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان] برای نظارت، و [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان] برای انجام بررسی‌های متعاقب این نظارت‌ها؛

پ. بررسی‌های امنیتی پیوسته بر اساس راهبرد نظارت پیوسته سازمان؛

ت. نظارت پیوسته بر وضعیت امنیتی معیارهای تعیین‌شده توسط سازمان بر اساس راهبرد نظارت پیوسته سازمان؛

ث. تحلیل و اصلاح اطلاعات امنیتی تولیدشده در فرایندهای بررسی و نظارت؛

ج. انجام اقدامات مقتضی بر اساس نتایج تحلیل اطلاعات امنیتی؛ و

چ. گزارش‌دهی وضعیت امنیت سازمان و سیستم اطلاعاتی به [اختصاص: نقش‌ها و کارکنان تعیین‌شده توسط سازمان] [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: برنامه‌های نظارت پیوسته سبب می‌شوند که سازمان به طور مستمر از وضعیت تهدیدات، آسیب‌پذیری‌ها و امنیت اطلاعات آگاه باشد و بتواند تصمیمات مبتنی بر مخاطرات را بر آن اساس اتخاذ نماید. عبارت‌های «پیوسته» و «مستمر» نشان می‌دهند که بررسی و تحلیل کنترل‌های امنیتی و مخاطرات مربوط به امنیت اطلاعات در فواصل زمانی نسبتاً کوتاه صورت می‌گیرد تا سازمان بتواند تصمیمات مبتنی بر مخاطرات را به خوبی اتخاذ نماید. نتایج برنامه‌های نظارت پیوسته سبب می‌شوند که سازمان بتواند واکنش‌های مناسبی به مخاطرات نشان دهد. این برنامه‌های همچنین سازمان‌ها را یاری می‌کنند تا در محیط‌های پویا و در شرایط تغییر مأموریت‌های و الزامات کسب‌وکار، تهدیدات، آسیب‌پذیری‌ها و فناوری‌ها، در خصوص تمدید مجوز سیستم‌های اطلاعاتی و کنترل‌های معمول تصمیم‌گیری کنند. مقامات سازمان می‌توانند با دسترسی به نتایج این برنامه‌های

نظارت پیوسته، تصمیمات زمان‌مندتر و آگاهانه‌تری در خصوص مخاطرات اتخاذ کنند؛ به عنوان مثال، در مورد صدور مجوزهای امنیتی تصمیم بگیرند. با استفاده از روش‌های خودکارسازی می‌توان مجوزهای امنیتی، نرم‌افزارها و سخت‌افزارها و ثابت‌افزارهای موجود، و سایر سیستم‌های اطلاعاتی را به نحو مناسبی به‌روزرسانی کرد. برای دستیابی به اثربخشی بیشتر می‌توان اطلاعات خاص، قابل سنجش، قابل اجرا، مربوط و زمان‌مندی را بر اساس نتایج برنامه‌های نظارت پیوسته تولید کرد. مقیاس فعالیت‌های نظارت پیوسته بر اساس دسته‌بندی‌های امنیتی سیستم‌های اطلاعاتی تعیین می‌شود. کنترل‌های مربوطه: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

کنترل‌های پیشرفته:

(۱) نظارت پیوسته / بررسی مستقل

سازمان، بررسی‌کنندگان و تیم‌های بررسی دارای [اختصاص: سطح استقلال تعیین‌شده توسط سازمان] را برای نظارت پیوسته بر کنترل‌های امنیتی موجود در سیستم اطلاعاتی به کار می‌گیرد.

راهنمایی‌های تکمیلی: سازمان‌ها می‌توانند با به‌کارگیری بررسی‌کنندگان و تیم‌های بررسی دارای سطح استقلال مناسب، کنترل‌های امنیتی را به شکل بهتری بررسی کنند. استقلال بررسی‌کنندگان سبب می‌شود که فرایند نظارت به شکل بی‌طرفانه‌ای انجام شود. بررسی‌کنندگان باید برای دستیابی به بی‌طرفی، از موارد روبرو پرهیز کنند: (۱) ایجاد منافع مشترک یا متضاد با سازمان‌های مورد بررسی؛ (۲) بررسی کار خود؛ (۳) کار به عنوان مدیر یا کارمند سازمان‌های مورد بررسی؛ و (۴) نمایندگی کردن سازمان‌هایی که خدمات آن‌ها را دریافت می‌کنند.

(۲) نظارت پیوسته / انواع بررسی‌ها

[حذف شد: در بخش CA-2 گنجانده شد].

(۳) نظارت پیوسته / تحلیل روند

سازمان با استفاده از تحلیل روند تعیین می‌کند که آیا نیاز به ایجاد تغییر در پیاده‌سازی کنترل‌های امنیتی، فواصل زمانی فعالیت‌های نظارت پیوسته، و/یا انواع فعالیت‌های مورد استفاده در فرایند نظارت پیوسته وجود دارد یا خیر.

راهنمایی‌های تکمیلی: تحلیل روند می‌تواند شامل فعالیت‌هایی از این دست باشد: بررسی انواع تهدیدات صورت‌گرفته در سازمان یا دولت فدرال، نرخ موفقیت برخی از انواع حملات سایبری، آسیب‌پذیری‌های

نوظهور در فناوری‌های اطلاعاتی، روش‌های جدید مهندسی اجتماعی، نتایج بررسی‌های کنترل‌های امنیتی، اثربخشی تنظیمات پیکربندی‌ها، و یافته‌ها و مشاهدات ممیزان و بازرسان کل.

مراجع: تفاهم‌نامه OMB 11-33، شماره‌های ویژه NIST 800-37, 800-39, 800-53A, 800-115, 800-137؛ هشدارهای امنیتی سایبری و فنی US-CERT؛ هشدارهای آسیب‌پذیری ضمانت اطلاعات DoD.

اولویت و تخصیص به مجموعه‌های پایه:

P2	CA-7 اولویت پایین	CA-7(1) اولویت متوسط	CA-7(1) اولویت بالا

CA-8: آزمون نفوذ

کنترل: سازمان، آزمون نفوذ را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] روی [اختصاص: سیستم‌های اطلاعاتی یا مؤلفه‌های تعیین‌شده توسط سازمان] انجام می‌دهد.

راهنمایی‌های تکمیلی: آزمون نفوذ نوع خاصی از بررسی است که در خصوص سیستم‌های اطلاعاتی یا مؤلفه‌های این سیستم‌ها انجام می‌شود تا آسیب‌پذیری‌های آن‌ها مشخص گردد. با استفاده از این آزمون‌ها می‌توان آسیب‌پذیری‌ها یا میزان مقاومت سیستم‌های اطلاعاتی در برابر تهدیدات را با توجه به منابع موجود (مانند زمان، منابع و/یا مهارت‌ها) مشخص نمود. در آزمون نفوذ، اقدامات مهاجمان شبیه‌سازی می‌شود و تحلیل دقیقی از ضعف‌های امنیتی سازمان صورت می‌گیرد. سازمان‌ها همچنین می‌توانند از نتایج تحلیل‌های صورت‌گرفته، برای انجام بهتر آزمون‌های نفوذ بهره گیرند. آزمون نفوذ را می‌توان روی نرم‌افزار، سخت‌افزار و ثابت افزار ومؤلفه‌های سیستم‌های اطلاعاتی انجام داد. بدین منظور می‌توان هم از کنترل‌های امنیتی فنی و هم از کنترل‌های امنیتی فیزیکی استفاده نمود. فرایند آزمون نفوذ می‌تواند چنین مراحلی را شامل شود: (۱) آزمون اولیه بر اساس دانش کاملی از سیستم هدف؛ (۲) شناسایی اولیه آسیب‌پذیری‌های بالقوه بر اساس آزمون اولیه؛ و (۳) انجام آزمونی برای تعیین امکان استفاده متخاصمان از آسیب‌پذیری‌های موجود. پیش از آغاز آزمون نفوذ، تمامی طرفین باید در خصوص قوانین مشارکت[۱۶۸] توافق نمایند. سازمان‌ها در انجام این آزمون، روش‌ها و ابزارهای مورد استفاده متخاصمان را مد نظر قرار می‌دهند. سطح استقلال افراد یا گروه‌های انجام‌دهنده این آزمون، بر اساس بررسی مخاطرات سازمان تعیین می‌شود. کنترل مربوطه: SA-12.

[168] rules of engagement

کنترل‌های پیشرفته:

(۱) آزمون نفوذ / مأمور یا تیم مستقل آزمون نفوذ

سازمان، مأموران یا تیم‌های مستقل را برای انجام آزمون نفوذ روی سیستم‌های اطلاعاتی یا مؤلفه‌های آن‌ها به کار می‌گیرد.

راهنمایی‌های تکمیلی: مأموران یا تیم‌های مستقل آزمون نفوذ، افراد یا گروه‌هایی هستند که سیستم‌های اطلاعاتی سازمان را به صورت بی‌طرفانه آزمون می‌کنند. بی‌طرفی به این معنی است که این مأموران یا تیم‌ها هیچ گونه تضاد منافعی در خصوص توسعه، اجرا یا مدیریت سیستم‌های اطلاعاتی مورد بررسی ندارند. راهنمایی‌های تکمیلی CA-2(1)، اطلاعات بیشتری را در خصوص بررسی‌های مستقل ارائه می‌کند. این اطلاعات در مورد آزمون‌های نفوذ مستقل نیز صدق می‌کنند. کنترل مربوطه: CA-2.

(۲) آزمون نفوذ / استفاده از تیم سرخ[۱۶۹]

سازمان با استفاده از [اختصاص: فعالیت‌های تیم سرخ تعیین‌شده توسط سازمان]، فعالیت‌های متخاصمان برای حمله به سیستم‌های اطلاعاتی خود را بر اساس [اختصاص: قوانین مشارکت تعیین‌شده توسط سازمان] شبیه‌سازی می‌کند.

راهنمایی‌های تکمیلی: سازمان‌ها می‌توانند با استفاده از تیم‌های سرخ، دامنه فعالیت‌های خود در زمینه آزمون نفوذ را گسترش دهند و وضعیت امنیتی و توانایی خود برای مقابله با حملات سایبری را بررسی نمایند. در واقع، تیم‌های سرخ اقدام به شبیه‌سازی فعالیت‌های متخاصمان می‌کنند و تعیین می‌نمایند که سازمان و سیستم اطلاعاتی چه قابلیت‌های امنیتی و توانایی‌های برای مقابله با آن‌ها دارند. حملات شبیه‌سازی‌شده توسط تیم‌های سرخ شامل حملات فناورانه (مانند حملات مبتنی بر تعامل با سخت‌افزارها، نرم‌افزارها و ثابت‌افزارها، و/یا مأموریت‌ها و فرایندهای کسب‌وکار سازمان) و حملات مبتنی بر مهندسی اجتماعی (مانند برقراری تعامل از طریق ایمیل، تلفن، یا گفتگوهای شخصی) هستند. به طور معمول، آزمون نفوذ بیشتر شکل آزمایشگاهی دارد، اما سازمان‌ها از تیم‌های سرخ استفاده می‌کنند تا بررسی‌های واقع‌گرایانه‌تری را بر اساس آنچه در جهان واقع صورت می‌گیرد انجام دهند. با استفاده از تیم‌های سرخ می‌توان آگاهی امنیتی سازمان را ارتقا داد، آموزش‌های امنیتی را ترتیب داد، و میزان اثربخشی کنترل‌های امنیتی را بررسی کرد.

[169] red team exercise

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	CA-8 اولویت بالا

CA-9: ارتباط درونی سیستم‌ها

کنترل: سازمان:

الف. مجوز ارتباط درونی [اختصاص: مؤلفه‌های سیستم‌های اطلاعاتی یا دسته‌هایی از مؤلفه‌های تعیین‌شده توسط سازمان] با سیستم اطلاعاتی را صادر می‌کند؛ و

ب. در مورد هر یک از ارتباطات درونی، ویژگی‌های واسط، الزامات امنیتی و ماهیت ارتباطات منتقل‌شده را مستندسازی می‌کند.

راهنمایی‌های تکمیلی: این کنترل در مورد ارتباطات بین سیستم اطلاعاتی سازمان و مؤلفه‌های مجزای تشکیل‌دهنده سیستم (یعنی ارتباطات درون سیستم) صدق می‌کند. به عنوان مثال، می‌توان به ارتباطات سیستم با دستگاه‌های همراه، لپتاپ‌ها و کامپیوترهای دسکتاپ، پرینترها، دستگاه‌های کپی، دستگاه‌های چاپ، اسکنرها، حسگرها، و سرورها اشاره کرد. سازمان‌ها می‌توانند به جای صدور مجوز برای هر یک از ارتباطات درونی، این مجوز را برای دسته‌ای از مؤلفه‌های دارای ویژگی‌های مشابه صادر نمایند. به عنوان مثال، می‌توانند این کار را برای تمام دستگاه‌های کپی، اسکنرها و پرینترهای دیجیتال دارای قابلیت‌های پردازش، ذخیره‌سازی و انتقال خاص، یا برای تمام گوشی‌های هوشمند دارای پیکربندی اولیه خاص انجام دهند. کنترل‌های مربوطه: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.

کنترل‌های پیشرفته:

(۱) ارتباط درونی سیستم‌ها / بررسی انطباق با استانداردهای امنیتی

سیستم اطلاعاتی، پیش از آن که ارتباطات درونی را برقرار کند، انطباق مؤلفه‌های سیستم با استانداردهای امنیتی را بررسی می‌کند.

راهنمایی‌های تکمیلی: بررسی انطباق با استانداردهای امنیتی می‌تواند شامل مواردی از جمله تأیید پیکربندی‌های اولیه باشد. کنترل‌های مربوطه: CM-6.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	CA-9 اولویت پایین	CA-9 اولویت متوسط	CA-9 اولویت بالا

خانواده: مدیریت پیکربندی[۱۷۰]

CM-1: خط‌مشی و رویه‌های مدیریت پیکربندی

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۷. خط‌مشی مدیریت پیکربندی شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و
۸. رویه‌های تسهیل پیاده‌سازی خط‌مشی مدیریت پیکربندی و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] مرور و به‌روز می‌کند:

۷. خط‌مشی مدیریت پیکربندی؛ و
۸. رویه‌های مدیریت پیکربندی

راهنمایی تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل های خانواده CM را ارتقا داد. خط‌مشی و رویه‌ها بازگوکننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل مربوطه: PM-9.

کنترل‌های پیشرفته: وجود ندارد.

[170] Configuration management

مراجع: شماره‌های ویژه۱۰۰-۸۰۰ و ۱۲-۸۰۰ سازمان NIST

اولویت و تخصیص به مجموعه‌های پایه:

P1	CM-1 اولویت پایین	CM-1 اولویت متوسط	CM-1 اولویت بالا

CM-2: پیکربندی اولیه

کنترل: سازمان، بر اساس کنترل پیکربندی، پیکربندی اولیه سیستم اطلاعاتی را تهیه، مستندسازی و حفظ و نگهداری می‌کند.

راهنمایی تکمیلی: این کنترل پیکربندی‌های اولیه برای سیستم‌های اطلاعاتی و مؤلفه‌های آن‌ها از قبیل ارتباطات و جنبه‌های مربوط به اتصال‌پذیری ایجاد می‌کند. پیکربندی‌های اولیه مستند و رسماً بازبینی‌شده هستند و بر سر آن‌ها، بر اساس مجموعه‌هایی از ویژگی‌های سیستم‌های اطلاعاتی یا موارد پیکربندی درون آن‌ها، توافق شده است. پیکربندی‌های اولیه به عنوان بنیانی برای تغییرات بعدی در سیستم‌های اطلاعاتی مورد استفاده قرار می‌گیرند. پیکربندی‌های اولیه شامل اطلاعاتی در باب مؤلفه‌های سیستم‌های اطلاعاتی (مثل)، توپولوژی شبکه، و مکان منطقی این مؤلفه‌ها در معماری سیستم هستند. از آنجا که سیستم‌های اطلاعاتی سازمان به مرور زمان تغییر می‌کنند، حفظ پیکربندی‌های اولیه مستلزم این است که مجموعه‌های اولیه جدیدی ایجاد شوند. پیکربندی اولیه سیستم‌های اطلاعاتی، نشان‌دهنده معماری کنونی سازمان است. کنترل‌های مربوطه: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.

کنترل‌های پیشرفته:

(۱) پیکربندی اولیه / بازبینی و به‌روزرسانی

سازمان، پیکربندی اولیه سیستم اطلاعاتی را در موارد و شرایط زیر، بازبینی و به‌روزرسانی می‌کند:

الف. [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان]؛

ب. هنگامی که [اختصاص: شرایط تعیین‌شده توسط سازمان] ایجاب کند؛ و

پ. به عنوان بخشی از فرایند نصب و ارتقای مؤلفه‌های سیستم اطلاعاتی.

راهنمایی تکمیلی: کنترل مربوطه: CM-5.

(۲) پیکربندی اولیه / پشتیبانی خودکار از دقت و به‌روزبودن

سازمان با استفاده از سازوکارهای خودکار، پیکربندی اولیه سیستم اطلاعاتی را به‌روز نگه می‌دارد، کامل و دقیق می‌کند، و در دسترس قرار می‌دهد.

راهنمایی تکمیلی: به عنوان مثال‌هایی از این سازوکارهای خودکار، می‌توان به ابزارهای مدیریت موجودی سخت‌افزار و نرم‌افزار، ابزارهای مدیریت پیکربندی، و ابزارهای مدیریت شبکه اشاره کرد. این ابزارها را می‌توان به عنوان کنترل‌های معمول در سطح سیستم اطلاعاتی، در سطح سیستم‌عامل، یا در سطح مؤلفه‌ها مورد استفاده قرار داد (مثلا در ایستگاه‌های کاری، سرورها، کامپیوترهای نوت بوک، مؤلفه‌های شبکه، یا ابزارهای همراه). با استفاده از این ابزارها می‌توان نسخه برنامه‌های کاربردی سیستم‌عامل، نوع نرم‌افزارهای نصب‌شده، و بسته‌های تعمیری مورد استفاده را پیگیری کرد. سازمان‌هایی که می‌خواهند فعالیت‌های مربوط به پیکربندی اولیه و فرایندهای مدیریت موجودی مؤلفه‌های سیستم را با هم ترکیب کنند، می‌توانند برای تحقق این کنترل پیشرفته، CM-8(2) را پیاده‌سازی نمایند. کنترل‌های مربوطه: CM-7, RA-5.

(۳) پیکربندی اولیه / حفظ پیکربندی‌های پیشین

سازمان، [اختصاص: نسخه‌های قبلی پیکربندی سیستم اطلاعاتی که سازمان آن‌ها را تعیین کرده است] را نگهداری می‌کند تا در آینده، امکان بازگشت به حالت قبل را داشته باشد.

راهنمایی تکمیلی: به عنوان مثال‌هایی از این نسخه‌های قبلی، می‌توان به سوابق پیکربندی، فایل‌های پیکربندی، ثابت‌افزار، نرم‌افزار، و سخت‌افزار اشاره کرد.

(۴) پیکربندی اولیه / نرم‌افزارهای غیر مجاز

[حذف شد: به بخش CM-7 منتقل شد].

(۵) پیکربندی اولیه / نرم‌افزارهای مجاز

[حذف شد: به بخش CM-7 منتقل شد].

(۶) پیکربندی اولیه / محیط آزمون و توسعه

سازمان، پیکربندی اولیه محیط‌های توسعه و آزمون را حفظ می‌کند. این پیکربندی‌ها، به صورت مجزا از پیکربندی اولیه عملیاتی، مدیریت می‌شوند.

راهنمایی تکمیلی: ایجاد پیکربندی‌های اولیه مجزایی برای محیط‌های توسعه، آزمون و عملیات، سیستم‌های اطلاعاتی را در برابر رویدادهای برنامه‌ریزی‌نشده و غیر منتظره مربوط به فعالیت‌های توسعه و آزمون، محافظت می‌نماید. پیکربدی‌های اولیه مجزا به سازمان‌ها اجازه می‌دهند تا از بهترین روش پیکربندی استفاده کنند. به عنوان مثال، مدیریت پیکربندی‌های عملیاتی به طور معمول در راستای

حفظ ثبات انجام می‌شود، در حالی که مدیریت پیکربندی‌های توسعه و آزمون، نیازمند انعطاف بیشتری است. پیکربندی‌های مورد استفاده در محیط آزمون، تا حد امکان بازتاب‌دهنده پیکربندی‌های محیط عملیاتی هستند، به گونه‌ای که نتایج آزمون‌ها را می‌توان نماینده تغییرات صورت‌گرفته در سیستم‌های عملیاتی دانست. این کنترل پیشرفته نیازمند پیکربندی‌های مجزا است، اما الزاما به محیط‌های فیزیکی مجزا نیاز ندارد. کنترل‌های مربوطه: CM-4, SC-3, SC-7.

(۷) پیکربندی اولیه / پیکربندی سیستم‌ها، مؤلفه‌ها و دستگاه‌ها در نواحی با مخاطره بالا

سازمان:

الف. [اختصاص: سیستم‌های اطلاعاتی، مولفه‌های سیستم، یا دستگاه‌های تعیین‌شده توسط سازمان] به همراه [اختصاص: پیکربندی‌های تعیین‌شده توسط سازمان] را در اختیار افرادی قرار می‌دهد که به نواحی با مخاطره بالا مسافرت می‌کنند؛ و

ب. پس از بازگشت افراد، از [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] در دستگاه‌ها استفاده می‌کند.

راهنمایی تکمیلی: در صورتی که سازمان بداند که سیستم‌های اطلاعاتی، مؤلفه‌های سیستم‌ها و دستگاه‌ها (مانند کامپیوترهای نوت بوک یا دستگاه‌های همراه) در نواحی با مخاطره بالا قرار خواهند گرفت، ممکن است کنترل‌های امنیتی اضافه‌ای را به کار گیرد و نسبت به نواحی تحت کنترل خود، از ابزارهای کنترل فیزیکی بیشتری استفاده کند. به عنوان مثال، رویه‌ها و خط‌مشی‌های سازمان در مورد استفاده از کامپیوترهای نوت بوک توسط افرادی که به مسافرت می‌روند یا از مسافرت برمی‌گردند، مواردی از جمله تعیین نواحی مستعد خطر، تعیین پیکربندی‌های مورد نیاز این دستگاه‌ها، حصول اطمینان از پیکربندی صحیح دستگاه‌ها پیش از مسافرت، و استفاده از ابزارهای حفاظتی خاص پس از مسافرت را شامل می‌شود. برخی کامپیوترهای نوت بوک به شکل خاصی پیکربندی می‌شوند. به عنوان مثال، از هارد درایوهای خاصی در آن‌ها استفاده می‌شود، برنامه‌های کاربردی محدودی روی آن‌ها نصب می‌شود، و مقاومت فیزیکی آن‌ها افزایش داده می‌شود. هنگامی که دستگاه‌های همراه از سفر برمی‌گردند نیز اقدامات خاصی در مورد آن‌ها صورت می‌گیرد. مثلا بررسی می‌شود که آیا دستکاری فیزیکی شده‌اند و از هارد درایو آن‌ها تصویر گرفته شده است یا خیر. حفاظت از اطلاعات موجود روی دستگاه‌های همراه، در خانواده حفاظت از رسانه‌ها بررسی شده است.

مراجع: شماره‌های ویژه ۱۲۸-۸۰۰ سازمان NIST

اولویت و تخصیص به مجموعه‌های پایه:

P1	CM-2 اولویت پایین	CM-2(1)(3)(7) اولویت متوسط	CM-2(1)(2)(3)(7) اولویت بالا

CM-3: کنترل تغییر پیکربندی

کنترل: سازمان:

۱. نوع تغییراتی را که از طریق پیکربندی در سیستم اطلاعاتی اعمال می‌شوند، شناسایی می‌کند.
۲. تغییرات مذکور را مرور می‌کند و پس از آن که تأثیرات امنیتی آن‌ها را تجزیه و تحلیل نمود، اعمال تغییرات را تأیید یا رد می‌کند.
۳. تصمیماتی که در خصوص تغییر پیکربندی سیستم اطلاعاتی اتخاذ نمود را مستند می‌کند.
۴. تغییرات تأییدشده را در سیستم اطلاعاتی اعمال می‌کند.
۵. سوابق تغییرات را برای [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] حفظ می‌کند.
۶. فعالیت‌های مربوط به اعمال تغییرات در پیکربندی سیستم اطلاعاتی را بازبینی و ممیزی می‌کند.
۷. از طریق [اختصاص: عنصر تعیین‌شده توسط سازمان برای کنترل تغییر پیکربندی (مانند کمیته یا هیئت مسئول)] و با توجه به [اختصاص: بازه زمانی و شرایط تغییر پیکربندی تعیین‌شده توسط سازمان]، بر فعالیت‌های صورت‌گرفته در زمینه کنترل تغییر پیکربندی نظارت می‌کند.

راهنمایی تکمیلی: برای اعمال کنترل‌های تغییر پیکربندی در سیستم‌های اطلاعاتی سازمان، چند فرایند مختلف باید انجام شوند. این فرایندها عبارتند از ارائه پیشنهاد، توجیه، پیاده‌سازی، آزمون، بازبینی، و اعمال تغییرات در سیستم (از جمله تعدیل و ارتقا). کنترل تغییر پیکربندی، مواردی از جمله تغییر پیکربندی اولیه مؤلفه‌ها و آیتم‌های پیکربندی سیستم‌های اطلاعاتی، تغییر تنظیمات پیکربندی محصولات فناوری اطلاعات، تغییرات زمان‌بندی‌نشده و غیر مجاز، و اعمال تغییراتی برای برطرف کردن آسیب‌پذیری‌ها را شامل می‌شود. فرایند معمول مدیریت تغییرات پیکربندی سیستم‌های اطلاعاتی، از طریق نهادهایی از جمله هیئت کنترل پیکربندی صورت می‌گیرد (که تغییرات پیشنهادی در سیستم را تأیید می‌کند). در مورد سیستم‌های اطلاعاتی که به تازگی توسعه داده شده‌اند، یا سیستم‌هایی که تا حد زیادی ارتقا پیدا می‌کنند، سازمان باید از نمایندگان سازمان‌های ذینفع نیز در هیئت کنترل پیکربندی استفاده کند. ممیزی تغییرات، شامل فعالیت‌هایی است که قبل و بعد از اعمال تغییر در سیستم اطلاعاتی سازمان صورت گرفته‌اند، و همچنین فعالیت‌های ممیزی که باید

در خصوص این تغییرات انجام شوند. کنترل‌های مربوطه: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.

کنترل‌های پیشرفته:

(۱) کنترل تغییر پیکربندی / مستندسازی، اطلاع‌رسانی یا ممنوعیت خودکار تغییرات

سازمان، با استفاده از سازوکارهای خودکار:

الف. تغییرات پیشنهادی در سیستم اطلاعاتی را مستندسازی می‌کند؛

ب. تغییرات پیشنهادی در سیستم اطلاعاتی را به [اختصاص: مسئولین تعیین‌شده توسط سازمان] اطلاع می‌دهد و درخواست تأیید می‌نماید؛

پ. تغییرات پیشنهادی در سیستم اطلاعاتی که پس از [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] تأیید یا رد نشده‌اند را مشخص می‌نماید؛

ت. از اعمال تغییرات پیش از تأیید شدن آن‌ها ممانعت به عمل می‌آورد؛

ث. تمام تغییرات صورت گرفته در سیستم اطلاعاتی را مستندسازی می‌کند؛ و

ج. پس از اتمام تغییرات در سیستم اطلاعاتی، مراتب را به [اختصاص: کارکنان تعیین‌شده توسط سازمان] اطلاع می‌دهد.

(۲) کنترل تغییر پیکربندی / آزمون، تأیید و مستندسازی تغییرات

سازمان، تغییرات سیستم اطلاعاتی را، پیش از اعمال در سیستم عملیاتی، آزمون، تأیید و مستندسازی می‌کند.

راهنمایی تکمیلی: تغییرات سیستم اطلاعاتی شامل اعمال تغییرات در سخت‌افزار، نرم‌افزار و ثابت‌افزار، و تغییرات پیکربندی تعریف‌شده در CM-6 است. سازمان‌ها اقدامات لازم را انجام می‌دهند و اطمینان حاصل می‌نمایند که آزمون‌ها، اخلالی در عملکرد سیستم اطلاعاتی ایجاد نمی‌کنند. افراد و گروه‌هایی که آزمون‌ها را انجام می‌دهند، از رویه‌ها و خط‌مشی‌های امنیتی سازمان، رویه‌ها و خط‌مشی‌های امنیتی سیستم اطلاعاتی، مخاطرات و مسائل مربوط به فرایندها و تأسیسات خاص آگاهی دارند. ممکن است لازم باشد که پیش از انجام آزمون، سیستم‌های عملیاتی خاموش شوند یا سیستم‌های جایگزین تهیه شوند. اگر نیاز به خاموش شدن سیستم‌های اطلاعاتی برای انجام آزمون‌ها وجود داشته باشد، آزمون‌ها به گونه‌ای برنامه‌ریزی می‌شوند که در زمان‌های تعیین‌شده برای خاموشی سیستم انجام شوند. اگر

امکان انجام آزمون روی سیستم‌های عملیاتی وجود نداشته باشد، سازمان‌ها از کنترل‌های جبرانی استفاده می‌کنند (مثلا آزمون‌ها روی سیستم‌های جایگزین انجام می‌شوند).

(۳) کنترل تغییر پیکربندی / پیاده‌سازی خودکار تغییرات

سازمان با استفاده از سازوکارهای خودکار، تغییرات را در سیستم اطلاعاتی فعلی اعمال می‌کند و مجموعه‌های اولیه به‌روزشده را به کار می‌گیرد.

(۴) کنترل تغییر پیکربندی / نماینده امنیتی

سازمان، الزام می‌دارد که فردی به عنوان نماینده امنیت اطلاعات، عضو [اختصاص: عنصر کنترل تغییرات پیکربندی تعیین‌شده توسط سازمان] باشد.

راهنمایی تکمیلی: افردی از این دست می‌توانند به عنوان نماینده امنیت اطلاعات منصوب شوند: مدیر ارشد امنیت اطلاعات، مدیر ارشد سیستم اطلاعاتی، یا مدیر امنیت سیستم اطلاعاتی. لازم است که نمایندگان از تخصص بالایی در زمینه امنیت اطلاعات برخوردار باشند، زیرا اعمال تغییر در پیکربندی سیستم اطلاعاتی می‌تواند اثرات جانبی مختلفی را به همراه داشته باشد که برخی از آن‌ها جنبه امنیتی دارند. شناسایی زودهنگام این اثرات، می‌تواند از پدید آمدن اثرات نامطلوب بر وضعیت امنیتی سیستم اطلاعاتی سازمان جلوگیری به عمل آورد. عنصر کنترل تغییر پیکربندی در این کنترل پیشرفته، مشابه عناصر کنترل تغییر پیکربندی است که توسط سازمان در CM-3 تعریف شده‌اند.

(۵) کنترل تغییر پیکربندی / پاسخ امنیتی خودکار

در صورتی که پیکربندی‌های اولیه به شکل غیر مجاز تغییر داده شده باشند، سیستم اطلاعاتی به طور خودکار [اختصاص: پاسخ امنیتی تعیین‌شده توسط سازمان] را اعمال می‌کند.

راهنمایی تکمیلی: پاسخ‌های امنیتی، مواردی از جمله متوقف کردن فرایندهای سیستم اطلاعاتی، متوقف کردن برخی عملکردهای سیستم اطلاعاتی، یا اطلاع‌رسانی به کارکنان سازمان در صورت مشاهده تغییر غیر مجاز را شامل می‌شوند.

(۶) کنترل تغییر پیکربندی / مدیریت رمزنگاری

سازمان اطمینان حاصل می‌کند که سازوکارهای رمزنگاری مورد استفاده برای پیاده‌سازی [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان]، مبتنی بر سازوکار مدیریت پیکربندی هستند.

راهنمایی تکمیلی: صرف‌نظر از ابزارهای رمزنگاری مورد استفاده (مانند کلید عمومی، کلید خصوصی یا اسرار اشتراکی)، سازمان اطمینان حاصل می‌نماید که فرایندها و رویه‌هایی برای مدیریت مؤثر این ابزارها وجود دارند. به عنوان مثال، اگر دستگاه‌ها از گواهی‌نامه‌ها به عنوان مبنای شناسایی و احراز

هویت استفاده کنند، باید فرایندهایی نیز وجود داشته باشد که شرایط انقضای گواهی‌نامه‌های مذکور را مشخص نماید. کنترل مربوطه: SC-13.

مراجع: شماره‌های ویژه ۱۲۸-۸۰۰ سازمان NIST

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	CM-3(2) اولویت متوسط	CM-3(1)(2) اولویت بالا

CM-4: تجزیه و تحلیل اثرات امنیتی ناشی از اعمال تغییر در سیستم اطلاعاتی

کنترل: سازمان پیش از آن که تحولاتی در سیستم اطلاعاتی ایجاد نماید، تغییرات را تجزیه و تحلیل می‌کند تا اثرات امنیتی بالقوه ناشی از آن‌ها را شناسایی کند.

راهنمایی تکمیلی: تجزیه و تحلیل اثرات امنیتی، توسط آن دسته از کارکنان سازمان انجام می‌شود که وظایف امنیتی را بر عهده دارند (مثلا راهبران سیستم اطلاعاتی، مسئولان امنیت سیستم اطلاعاتی، مدیران امنیت سیستم اطلاعاتی، و مهندسان امنیت سیستم اطلاعاتی). افرادی که تجزیه و تحلیل اثرات امنیتی را انجام می‌دهند، باید از مهارت‌های لازم برای تجزیه و تحلیل تغییرات اعمال‌شده در سیستم اطلاعاتی و نتایج بالقوه آن برخوردار باشند. تجزیه و تحلیل اثرات امنیتی، مواردی از جمله بازبینی طرح‌های امنیتی برای درک الزامات کنترل امنیتی، و بازبینی اسناد طراحی سیستم برای درک چگونگی پیاده‌سازی کنترل‌ها و تأثیر تغییرات بر این کنترل‌ها را شامل می‌شود. تجزیه و تحلیل اثرات امنیتی همچنین ممکن است مواردی از جمله بررسی مخاطرات به منظور درک بهتر اثر تغییرات را نیز در بر گیرد، تا بدین ترتیب مشخص شود که آیا نیاز به کنترل‌های امنیتی اضافه‌ای نیز وجود دارد یا خیر. تجزیه و تحلیل اثرات امنیتی بر اساس دسته‌بندی امنیتی سیستم‌های اطلاعاتی انجام می‌شود. کنترل‌های مربوطه: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

کنترل‌های پیشرفته:

(۱) تجزیه و تحلیل اثرات امنیتی/ محیط‌های مجزا برای آزمون

سازمان، تغییرات سیستم اطلاعاتی را پیش از اعمال در محیط عملیاتی، در یک محیط آزمون مجزا تجزیه و تحلیل می‌نماید، تا اثرات عیب‌ها، ضعف‌ها، ناسازگاری‌ها، و خرابکاری‌ها مشخص شوند.

راهنمایی تکمیلی: منظور از محیط آزمون مجزا، محیطی است که به صورت فیزیکی یا منطقی، مجزا از محیط عملیای است. هدف از تفکیک مذکور این است که اطمینان حاصل شود فعالیت‌های صورت‌گرفته در محیط آزمون، تأثیری بر محیط عملیاتی نمی‌گذارند، و اطلاعات موجود در محیط عملیاتی به طور سهوی وارد محیط آزمون نمی‌شوند. در صورت استفاده از تفکیک منطقی به جای تفکیک فیزیکی، سازمان میزان این تفکیک را مشخص خواهد کرد (مثلا تفکیک از طریق ماشین‌های مجازی).
کنترل‌های مربوطه: SA-11, SC-3, SC-7.

(۲) تجزیه و تحلیل اثرات امنیتی / تأیید توابع امنیتی

پس از تغییر سیستم اطلاعاتی، سازمان اقدام به بررسی توابع امنیتی می‌کند تا تأیید نماید که این توابع به شکل مطلوب پیاده‌سازی شده‌اند، عملکرد مطلوب دارند، نتایج مطلوب را به دنبال دارند، و مطابق با الزامات امنیتی سیستم هستند.

راهنمایی تکمیلی: منظور از پیاده‌سازی، نصب کدهای تغییریافته در سیستم اطلاعاتی عملیاتی است.
کنترل مربوطه: SA-11.

مراجع: شماره‌های ویژه ۱۲۸-۸۰۰ سازمان NIST

اولویت و تخصیص به مجموعه‌های پایه:

P2	CM-4 اولویت پایین	CM-4 اولویت متوسط	CM-4(1) اولویت بالا

CM-5: محدودیت‌های دسترسی برای اعمال تغییر در سیستم اطلاعاتی

کنترل: سازمان محدودیت‌های دسترسی فیزیکی و منطقی برای اعمال تغییر در سیستم اطلاعاتی تعریف، مستندسازی، تأیید و اجرا می‌کند.

راهنمایی تکمیلی: هر گونه تغییر در سخت‌افزار، نرم‌افزار و ثابت‌افزار، می‌تواند اثرات قابل‌توجهی بر امنیت کلی سیستم داشته باشد. بنابراین، سازمان تنها به افراد مجاز امکان می‌دهد تا به سیستم اطلاعاتی دسترسی داشته باشند و تغییراتی از جمله به‌روزرسانی و تعدیل را انجام دهند. سازمان‌ها سوابق این دسترسی‌ها را نیز نگه می‌دارند تا اطمینان حاصل کنند که تغییرات صورت‌گرفته در پیکربندی کنترل شده‌اند، و بتوانند در صورت مشاهده تغییرات غیر مجاز، اقدامات لازم را انجام دهند. محدودیت دسترسی، شامل کتابخانه‌های نرم‌افزاری نیز می‌شود. محدودیت دسترسی، مواردی از جمله کنترل‌های دسترسی منطقی و فیزیکی (AC-3 و PE-3 را

ملاحظه کنید)، خودکارسازی جریان کار، کتابخانه‌های رسانه، لایه‌های انتزاعی[۱۷۱] (مانند تغییراتی که نه مستقیما در سیستم اطلاعاتی، بلکه در واسطهای شخص ثالث اعمال می‌شوند)، و پنجره‌های تغییر (مانند تغییراتی که تنها در زمان‌های تعیین‌شده اعمال می‌شوند، تا شناسایی تغییرات غیر مجاز آسان شود) را شامل می‌شود. کنترل‌های مربوطه: AC-3, AC-6, PE-3.

کنترل‌های پیشرفته:

(۱) محدودیت‌های دسترسی برای اعمال تغییر / ممیزی و پیاده‌سازی دسترسی خودکار

سیستم اطلاعاتی، محدودیت‌های دسترسی را پیاده‌سازی می‌کند و از ممیزی اقامات مربوطه، پشتیبانی می‌نماید.

راهنمایی تکمیلی: کنترل‌های مربوطه: AU-2, AU-12, AU-6, CM-3, CM-6.

(۲) محدودیت‌های دسترسی برای اعمال تغییر / بازبینی تغییرات سیستم

سازمان، تغییرات صورت‌گرفته در سیستم‌های اطلاعاتی را در [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان] و [اختصاص: شرایط تعیین‌شده توسط سازمان] بازبینی می‌کند تا مشخص شود که آیا تغییر غیر مجازی صورت گرفته است یا خیر.

راهنمایی تکمیلی: شرایطی که در آن‌ها باید بازبینی را انجام داد، بر اساس فعالیت‌هایی تعیین می‌شوند که سازمان در فرایند تغییر پیکربندی انجام داده است. کنترل‌های مربوطه: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.

(۳) محدودیت‌های دسترسی برای اعمال تغییر / مؤلفه‌های امضاشده

در صورتی که [اختصاص: مؤلفه نرم‌افزاری و ثابت‌افزاری تعیین‌شده توسط سازمان] با استفاده از گواهی‌نامه مورد تأیید سازمان امضای دیجیتال نشده باشد، سیستم اطلاعاتی از نصب شدن آن جلوگیری به عمل می‌آورد.

راهنمایی تکمیلی: : مؤلفه نرم‌افزاری و ثابت‌افزاری مذکور، مواردی از جمله به‌روزرسانی‌های نرم‌افزاری و ثابت‌افزاری، بسته‌های تعمیری، بسته‌های خدماتی، درایورهای دستگاه، و به‌روزرسانی‌های سیستم‌های ورودی و خروجی (BIOS) را شامل می‌شوند. سازمان‌ها می‌توانند مؤلفه‌های نرم‌افزاری و ثابت‌افزاری قابل استفاده را با توجه به نوع، آیتم، یا ترکیبی از هر دو شناسایی نمایند. امضای سازمان و تأیید این امضاها توسط سازمان، روشی است برای احراز هویت کدها. کنترل‌های مربوطه: CM-7, SC-13, SI-7.

[171] abstract layers

(۴) محدودیت‌های دسترسی برای اعمال تغییر / صدور مجوز توسط دو فرد مجاز

سازمان برای اعمال تغییر در [اختصاص: اطلاعات سیستمی و مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان]، از فرایند صدور مجوز توسط دو فرد مجاز استفاده می‌کند.

راهنمایی تکمیلی: : سازمان با استفاده از فرایند صدور مجوز توسط دو فرد مجاز، اطمینان حاصل می‌نماید که هیچ تغییری را نمی‌توان در مؤلفه‌های تعیین‌شده سیستم‌های اطلاعاتی صورت داد، مگر این که دو فرد مجاز آن را تأیید کرده باشند. این دو نفر از تخصص لازم برای تشخیص مناسب بودن تغییر مورد نظر برخوردار هستند. صدور مجوز توسط دو فرد مجاز، با نام کنترل دونفری نیز شناخته می‌شود. کنترل‌های مربوطه: AC-5, CM-3.

(۵) محدودیت‌های دسترسی برای اعمال تغییر / محدود کردن اختیارات عملیاتی و تولیدی

سازمان:

الف. اختیار تغییر مؤلفه‌های سیستم اطلاعاتی و اطلاعات سیستمی در محیط عملیاتی یا تولیدی را محدود می‌کند؛ و

ب. این اختیارات را در [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] مجددا بازبینی و ارزیابی می‌کند.

راهنمایی تکمیلی: در بسیاری از سازمان‌ها، سیستم‌های اطلاعاتی از چند عملکرد مختلف در زمینه مأموریت و کسب‌وکار سازمان پشتیبانی می‌کنند. محدود کردن اختیار تغییر مؤلفه‌های سیستم اطلاعاتی از این جهت حائز اهمیت است که تغییر مؤلفه‌ها ممکن است اثرات قابل توجهی بر مأموریت‌ها و فرایندهای کسب‌وکار داشته باشد. گاهی اوقات، توسعه‌دهندگان از رابطه پیچیده و تنگاتنگ بین سیستم‌ها و مأموریت‌ها و فرایندهای کسب‌وکار آگاهی ندارند. کنترل مربوطه: AC-2.

(۶) محدودیت‌های دسترسی برای اعمال تغییر / محدود کردن اختیارات مربوط به کتابخانه‌های نرم‌افزار

سازمان، اختیار تغییر نرم‌افزارهای موجود در کتابخانه نرم‌افزار را محدود می‌کند.

راهنمایی تکمیلی: کتابخانه‌های نرم‌افزار، شامل برنامه‌هایی با اختیارات ویژه هستند. کنترل مربوطه: AC-2.

(۷) محدودیت‌های دسترسی برای اعمال تغییر / پیاده‌سازی خودکار ابزارهای امنیتی

[حذف شد: به بخش SI-7 منتقل شد].

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	CM-5 اولویت متوسط	CM-5(1)(2)(3) اولویت بالا

CM-6: تنظیمات پیکربندی

کنترل: سازمان:

الف. تنظیمات پیکربندی محصولات IT به کار گرفته شده در سیستم اطلاعاتی را با استفاده از [اختصاص: چک‌لیست پیکربندی امنیتی تعیین‌شده توسط سازمان] ایجاد و مستندسازی می‌کند. این تنظیمات مطابق محدودترین الزامات عملیاتی هستند؛

ب. تنظیمات پیکربندی را پیاده‌سازی می‌کند؛

پ. هرگونه انحراف از تنظیمات پیکربندی مربوط به [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] را بر اساس [اختصاص: الزامات عملیاتی تعیین‌شده توسط سازمان] شناسایی، مستندسازی و تأیید می‌کند؛ و

ت. اعمال تغییرات در تنظیمات پیکربندی را کنترل و نظارت می‌کند تا مطابق رویه‌ها و خط‌مشی‌های سازمان صورت گیرند.

راهنمایی تکمیلی: تنظیمات پیکربندی شامل مجموعه‌ای از پارامترها هستند که می‌توان آن‌ها را در مؤلفه‌های سخت‌افزاری، نرم‌افزاری و ثابت‌افزاری سیستم اطلاعاتی تغییر داد. این امر نیز به نوبه خود بر وضعیت و عملکرد امنیتی سیستم تأثیر می‌گذارد. آن دسته از محصولات IT که می‌توان تنظیمات پیکربندی امنیتی را برای آن‌ها تعریف کرد، مواردی از جمله کامپیوترها، سرورها (مانند سرور پایگاه داده، ایمیل، احراز هویت، وب، پراکسی، فایل، یا نام دامنه)، ایستگاه‌های کاری، دستگاه‌های ورودی و خروجی (مانند اسکنرها، دستگاه‌های کپی و پرینترها)، مؤلفه‌های شبکه (مانند فایروال‌ها، مسیریاب‌ها، گیت‌وی‌ها، سوئیچ‌های صوت و داده، نقاط دسترسی بی‌سیم، دستگاه‌های شبکه و حسگرها)، سیستم‌عامل‌ها، میان‌افزارها، و برنامه‌های کاربردی را در بر می‌گیرند. پارامترهای امنیتی، پارامترهایی هستند که بر وضعیت امنیتی سیستم اطلاعاتی تأثیر می‌گذارند (مانند پارامترهای مورد نیاز برای حصول اطمینان از رعایت سایر الزامات کنترل‌های امنیتی). به عنوان مثالی از پارامترهای امنیتی می‌توان به این موارد اشاره کرد: (۱) تنظمیات رجیستری؛ (۲) تنظیمات مجوز دسترسی به

حساب کاربری، فایل‌ها و دایرکتوری‌ها؛ و (۳) تنظیمات مربوط به توابع، پورت‌ها، پروتکل‌ها، خدمات و اتصلات راه دور. سازمان‌ها از تنظیمات پیکربندی کلی در سطح سازمان استفاده می‌کنند و سپس تنظیمات خاصی را برای سیستم‌های اطلاعاتی در نظر می‌گیرند. این تنظیمات تبدیل به بخشی از پیکربندی اولیه سیستم‌ها می‌شوند.

پیکربندی‌های امن معمول (که به آن‌ها چک‌لیست‌های پیکربندی امنیتی، راهنمای ارتقای امنیت سیستم، راهنمای مرجع امنیت، و راهنمای پیاده‌سازی فنی امنیتی نیز گفته می‌شود)، شاخص‌های استاندارد و شناخته‌شده‌ای را در اختیار سازمان‌ها قرار می‌دهند که تنظیمات پیکربندی امن پلت‌فرم‌ها و محصولات IT و دستورالعمل‌هایی در زمینه پیکربندی این مؤلفه‌ها را شامل می‌شوند. پیکربندی‌های امن معمول می‌توانند توسط سازمان‌ها و موجودیت‌های مختلفی ارائه شوند که از آن میان می‌توان به تولیدکنندگان محصولات IT، توسعه دهندگان، فروشندگان، کنسرسیوم‌ها، نهادهای آکادمیک، صنعت، ادارات فدرال، و سایر سازمان‌های فعال در بخش‌های عمومی و خصوصی اشاره کرد. پیکربندی‌های امن معمول، پیکربندی اولیه دولت امریکا (USGCB) را نیز شامل می‌شوند که بر پیاده‌سازی CM-6 و کنترل‌های دیگری مانند AC-19 و CM-7 تأثیر می‌گذارد. پروتکل خودکارسازی محتوای امنیتی (SCAP) و استانداردهای تعریف‌شده در این پروتکل، ابزارهای مناسبی برای شناسایی، پیگیری و کنترل یکنواخت تنظیمات پیکربندی به شمار می‌آیند. OMB مجموعه‌ای از خط‌مشی‌های فدرال را در زمینه الزامات پیکربندی برای سیستم‌های اطلاعاتی فدرال تهیه و ارائه کرده است. کنترل‌های مربوطه: AC-19, CM-2, CM-3, CM-7, SI-4.

کنترل‌های پیشرفته:

(۱) تنظیمات پیکربندی / تأیید، کاربرد و مدیریت مرکزی خودکار

سازمان با استفاده از سازوکارهای خودکار، تنظیمات پیکربندی [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] را به طور خودکار تأیید، استفاده و مدیریت می‌کند.

راهنمایی تکمیلی: کنترل‌های مربوطه: CA-7, CM-4.

(۲) تنظیمات پیکربندی / پاسخ به تغییرات غیر مجاز

سازمان با استفاده از [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] به تغییرات غیر مجاز در [اختصاص: تنظیمات پیکربندی تعیین‌شده توسط سازمان] پاسخ می‌دهد.

راهنمایی تکمیلی: پاسخ به تغییرات غیر مجاز در تنظیمات پیکربندی، مواردی از جمله هشدار به کارکنان سازمان، بازگشت به تنظیمات پیکربندی اولیه، یا متوقف کردن فعالیت‌های سیستم اطلاعاتی (در حالت بحرانی) را شامل می‌شود. کنترل‌های مربوطه: IR-4, SI-7.

(۳) تنظیمات پیکربندی / شناسایی تغییرات غیر مجاز

[حذف شد: به بخش SI-7 منقل شد].

(۴) تنظیمات پیکربندی / نشان دادن انطباق با الزامات

[حذف شد: به بخش CM-4 منقل شد].

مراجع: تفاهم‌نامه OMB 07-11, 07-18, 08-22؛ شماره‌های ویژه NIST 800-70, 800-128؛ آدرس‌های اینترنتی: http://www.nsa.gov, http://checklists.nist.gov, http://nvd.nist.gov

اولویت و تخصیص به مجموعه‌های پایه:

P1	CM-6 اولویت پایین	CM-6 اولویت متوسط	CM-6(1)(2) اولویت بالا

CM-7: **حداقل قابلیت‌ها**

کنترل: سازمان:

الف. به گونه‌ای سیستم اطلاعاتی را پیکربندی می‌کند تا تنها قابلیت‌های ضروری و واجب را داشته باشد.

ب. استفاده از [اختصاص: کارکردها، پورت‌ها، پروتکل‌ها و خدماتی که توسط سازمان ممنوع یا محدود شده‌اند] را ممنوع یا محدود می‌کند.

راهنمایی تکمیلی: سیستم اطلاعاتی می‌تواند مجموعه گسترده‌ای از عملکردها و خدمات را ارائه کند. برخی از این عملکردها و خدمات، که به صورت پیش فرض ارائه می‌شوند، برای پشتیبانی از عملیات اصلی سازمان ضرورتی ندارند. علاوه بر این، گاهی اوقات راحت‌تر است که خدمات مختلف از طریق یک مؤلفه واحد ارائه شوند، اما این کار میزان خدمات قابل ارائه را محدود می‌کند. در صورت امکان، سازمان‌ها برای هر دستگاه تنها یک عملکرد را در نظر می‌گیرند (مثلا از سرورهای ایمیل یا سرورهای وب استفاده می‌کنند، نه از هر دو). سازمان‌ها، عملکردها و خدمات ارائه‌شده توسط سیستم‌های اطلاعاتی یا مؤلفه‌های این سیستم‌ها را بازبینی می‌کنند تا مشخص شود که کدام عملکردها و خدمات را می‌توان حذف کرد (مثلا پروتکل صوت روی اینترنت، پیام‌دهی

آنی، اجرای خودکار، و اشتراک‌گذاری فایل). سازمان‌ها، پورت‌ها یا پروتکل‌های منطقی یا فیزیکی بلا استفاده را غیر فعال می‌کنند تا خطر اتصال غیر مجاز دستگاه‌ها، انتقال غیر مجاز اطلاعات، یا برقراری ارتباطات غیر مجاز از بین برود. به منظور شناسایی و جلوگیری از به‌کارگیری عملکردها، پورت‌ها، پروتکل‌ها و خدمات غیر مجاز، سازمان‌ها از ابزارهای اسکن شبکه، سیستم‌های شناسایی و جلوگیری از ورود غیر مجاز، و حفاظت نقطه پایانی استفاده کنند. کنترل‌های مربوطه: AC-6, CM-2, RA-5, SA-5, SC-7.

کنترل‌های پیشرفته:

(۱) حداقل قابلیت‌ها / بازبینی دوره‌ای

سازمان:

الف. سیستم اطلاعاتی را در [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند تا عملکردها، پورت‌ها، پروتکل‌ها، و خدمات غیر امن یا غیر ضروری را شناسایی نماید؛ و

ب. [عملکردها، پورت‌ها، پروتکل‌ها، و خدمات غیر امن یا غیر ضروری تعیین‌شده توسط سازمان] را غیر فعال می‌کند.

راهنمایی تکمیلی: سازمان می‌تواند امنیت نسبی عملکردهای، پورت‌ها، پروتکل‌ها، و خدمات را تعیین کند یا این که تصمیمم خود را بر اساس ارزیابی سایر نهادها و سازمان‌ها اتخاذ نماید. بلوتوث، FTP و شبکه همتا به همتا، نمونه‌هایی از پروتکل‌های غیر امن هستند. کنترل‌های مربوطه: AC-18, CM-7, IA-2.

(۲) حداقل قابلیت‌ها / جلوگیری از اجرای برنامه‌ها

سیستم اطلاعاتی بر اساس [انتخاب (یک یا چند مورد): [خط‌مشی‌های تعیین‌شده توسط سازمان در زمینه به‌کارگیری و محدودیت‌های برنامه‌های نرم‌افزاری]؛ قوانین مربوط به شرایط و ضوابط استفاده از برنامه‌های نرم‌افزاری]، از اجرای برنامه‌ها جلوگیری به عمل می‌آورد.

راهنمایی تکمیلی: کنترل‌های مربوطه: CM-8, PM-5.

(۳) حداقل قابلیت‌ها / انطباق با قوانین ثبت نام

سیستم اطلاعاتی اطمینان حاصل می‌نماید که [اختصاص: الزامات تعیین‌شده توسط سازمان در زمینه ثبت نام عملکردها، پورت‌ها، پروتکل‌ها، و خدمات] رعایت شده‌اند.

راهنمایی تکمیلی: سازمان‌ها با استفاده از فرایند ثبت نام، سیستم‌های اطلاعاتی و عملکردها، پورت‌ها، پروتکل‌ها، و خدمات را مدیریت و پیگیری می‌کند.

(۴) حداقل قابلیت‌ها / تهیه لیست سیاه نرم‌افزارهای غیر مجاز

سازمان:

الف. [اختصاص: برنامه‌های نرم‌افزاری تعیین‌شده توسط سازمان که اجازه اجرای آن‌ها در سیستم اطلاعاتی وجود ندارد] را شناسایی می‌کند؛

ب. خط‌مشی «اجازه دادن به همه، به جز موارد استثنا»[۱۷۲] را به کار می‌گیرد تا از اجرای برنامه‌های نرم‌افزاری غیر مجاز در سیستم اطلاعاتی جلوگیری به عمل آورد؛ و

پ. لیست برنامه‌های نرم‌افزاری غیر مجاز را در [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند.

راهنمایی تکمیلی: فرایند مورد استفاده برای شناسایی برنامه‌های نرم‌افزاری غیر مجاز، به عنوان «تهیه لیست سیاه» شناخته می‌شود. اگر از خط‌مشی تهیه لیست سفید (که از این خط‌مشی قدرتمندتر است) استفاده شود، سازمان می‌تواند به جای این کنترل پیشرفته از CM-7(5) استفاده کند. کنترل‌های مربوطه: CM-6, CM-8, PM-5.

(۵) حداقل قابلیت‌ها / تهیه لیست سفید نرم‌افزارهای مجاز

سازمان:

الف. [اختصاص: برنامه‌های نرم‌افزاری تعیین‌شده توسط سازمان که اجازه اجرای آن‌ها در سیستم اطلاعاتی وجود دارد] را شناسایی می‌کند؛

ب. خط‌مشی «منع همه، به جز موارد استثنا»[۱۷۳] را به کار می‌گیرد تا اجازه اجرای برنامه‌های نرم‌افزاری مجاز در سیستم اطلاعاتی را صادر کند؛ و

پ. لیست برنامه‌های نرم‌افزاری مجاز را در [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند.

راهنمایی تکمیلی: فرایند مورد استفاده برای شناسایی برنامه‌های نرم‌افزاری مجاز، به عنوان «تهیه لیست سیاه» شناخته می‌شود. علاوه بر تهیه لیست سفید، سازمان‌ها اقدام به تأیید صحت و یکپارچگی نرم‌افزارهای موجود در لیست نیز می‌نمایند. بدین منظور، از روش‌هایی مانند رمزنگاری، امضای دیجیتال، یا توابع درهم‌ساز استفاده می‌شود. تأیید نرم افزارهای موجود در لیست سفید می‌تواند هم

[172] allow-all, deny-by-exception policy

[173] deny-all, permit-by-exception policy

قبل از اجرا و هم در زمان راه‌اندازی سیستم انجام شود. کنترل‌های مربوطه: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.

مراجع: دستورالعمل DoD 8551.01

اولویت و تخصیص به مجموعه‌های پایه:

P1	CM-7 اولویت پایین	CM-7(1)(2)(4) اولویت متوسط	CM-7(1)(2)(5) اولویت بالا

CM-8: لیست مؤلفه‌های موجود سیستم اطلاعاتی

کنترل: سازمان:

الف. لیستی از مؤلفه‌های موجود سیستم اطلاعاتی تهیه و مستند می‌کند، به گونه‌ای که:

۱. وضعیت کنونی سیستم اطلاعاتی را به خوبی نشان دهد؛
۲. تمام مؤلفه‌های موجود در محدوده سیستم اطلاعاتی را شامل شود؛
۳. جزئیات مورد نیاز برای پیگیری و گزارش‌دهی را شامل باشد؛ و
۴. [اختصاص: اطلاعات تعیین‌شده توسط سازمان که برای دسترسی به اطلاعات لازم جهت پاسخگویی مؤلفه‌ها، ضروری هستند] را شامل باشد؛ و

ب. لیست مؤلفه‌های موجود سیستم اطلاعاتی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] مرور و به‌روز می‌کند.

راهنمایی تکمیلی: ممکن است سازمان‌ها از سیستم موجودی‌های متمرکز برای مؤلفه‌های سیستم اطلاعاتی استفاده کنند، که شامل مؤلفه‌های تمام سیستم‌های اطلاعاتی سازمان باشد. در این شرایط، سازمان اطمینان حاصل می‌نماید که موجودی حاصله، شامل تمام اطلاعات سیستمی مورد نیاز برای پاسخگو نمودن مؤلفه‌ها است (مانند انجمن‌های مرتبط با سیستم اطلاعاتی، و مالک سیستم اطلاعاتی). اطلاعات مورد نیاز برای پاسخگو نمودن مؤلفه‌های سیستم اطلاعاتی، مواردی از جمله ویژگی‌های موجودی سخت‌افزار، اطلاعات مربوط به مجوز نرم‌افزارها، شماره نسخه نرم‌افزار، مالکان مؤلفه‌ها، و نام دستگاه یا آدرس شبکه مربوط به دستگاه‌ها یا مؤلفه‌های شبکه را شامل می‌شود. ویژگی‌های موجودی، مواردی از جمله تولیدکننده، نوع، مدل، شماره سریال، و مکان فیزیکی دستگاه را در بر می‌گیرد. کنترل‌های مربوطه: CM-2, CM-6, PM-5.

کنترل‌های پیشرفته:

(۱) لیست مؤلفه‌های موجود سیستم اطلاعاتی / به‌روزرسانی در جریان نصب و حذف

سازمان، موجودی مؤلفه‌های سیستم اطلاعاتی را به عنوان بخشی از فرایند نصب و حذف مؤلفه‌ها و به‌روزرسانی سیستم اطلاعاتی، به‌روز می‌کند.

(۲) لیست مؤلفه‌های موجود سیستم اطلاعاتی / حفظ و نگهداری خودکار

سازمان با استفاده از سازوکارهای خودکار، موجودی مؤلفه‌های سیستم اطلاعاتی را به‌روز و تکمیل می‌کند و در دسترس قرار می‌دهد.

راهنمایی تکمیلی: سازمان‌ها، لیست مؤلفه‌های موجود سیستم اطلاعاتی را تا حد امکان حفظ می‌کنند و به‌روز می‌نمایند. به عنوان مثال، پایش ماشین‌های مجازی کار ساده‌ای نیست، زیرا این ماشین‌ها هنگامی که در حال کار نباشند، قابل مشاهده نیستند. در این موارد، سازمان‌ها لیست مؤلفه‌های موجود سیستم اطلاعاتی را به دقیق‌ترین و به‌روزترین شکل ممکن تهیه و نگهداری می‌کنند. سازمان‌هایی که می‌خواهند لیست مؤلفه‌های موجود سیستم اطلاعاتی را با پیکربندی اولیه ترکیب کنند، می‌توانند به جای این کنترل پیشرفته از CM-2(2) استفاده نمایند. کنترل مربوطه: SI-7.

(۳) لیست مؤلفه‌های موجود سیستم اطلاعاتی / شناسایی خودکار مؤلفه‌های غیر مجاز

سازمان:

الف. سازوکارهای خودکاری را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] به کار می‌گیرد تا با استفاده از آن‌ها، وجود مؤلفه‌های سخت‌افزاری، نرم‌افزاری و ثابت‌افزاری غیر مجاز در سیستم اطلاعاتی را شناسایی نماید؛ و

ب. در صورت شناسایی مؤلفه‌های غیر مجاز، اقدامات روبرو را انجام می‌دهد: [انتخاب (یک یا چند مورد): غیر فعال سازی دسترسی به شبکه برای این مؤلفه‌ها؛ جدا کردن مؤلفه از سیستم؛ اطلاع‌رسانی به [اختصاص: کارکنان و نقش‌های تعیین‌شده توسط سازمان]].

راهنمایی تکمیلی: این کنترل پیشرفته، در کنار پایش اتصالات راه دور و دستگاه‌های همراه غیر مجاز به کار گرفته می‌شود. پایش مؤلفه‌های غیر مجاز سیستم ممکن است به صورت منظم یا دوره‌ای صورت گیرد. سازوکارهای خودکار را می‌توان در سیستم اطلاعاتی یا در دستگاه‌های مجزا مورد استفاده قرار داد. برای جدا کردن مؤلفه غیر مجاز از سیستم، می‌توان آن را در دامنه یا شبکه فرعی جداگانه‌ای قرار

داد یا آن را قرنطینه نمود. به این نوع جداسازی مؤلفه‌ها، روش جعبه شنی[۱۷۴] گفته می‌شود. کنترل‌های مربوطه: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.

(۴) لیست مؤلفه‌های موجود سیستم اطلاعاتی / اطلاعات مورد نیاز برای پاسخگو نمودن افراد مسئول

سازمان، لیست مؤلفه‌های موجود سیستم اطلاعاتی را به گونه‌ای تهیه می‌کند که اطلاعات مورد نیاز برای شناسایی افراد مسئول مؤلفه‌های مذکور بر اساس [انتخاب (یک یا چند مورد): نام، پست، نقش] در آن وجود داشته باشد.

راهنمایی تکمیلی: سازمان‌ها با شناسایی افراد پاسخگو یا مسئول مؤلفه‌ها، اطمینان حاصل خواهند که مؤلفه‌ها به درستی راهبری شده‌اند و خواهند توانست اقدامات لازم را انجام دهند.

(۵) لیست مؤلفه‌های موجود سیستم اطلاعاتی / جلوگیری از تکرار مؤلفه‌ها در لیست‌های مختلف

سازمان تأیید می‌کند که هیچ یک از مؤلفه‌های موجود در محدوده سیستم اطلاعاتی، در سایر لیست‌های موجودی تکرار نشده‌اند.

راهنمایی تکمیلی: سازمان‌ها با استفاده از این کنترل پیشرفته، اطمینان حاصل خواهند کرد که مؤلفه‌های سیستم‌های اطلاعاتی پیچیده و به‌هم‌پیوسته، در لیست‌های مختلف تکرار نشده‌اند.

(۶) لیست مؤلفه‌های موجود سیستم اطلاعاتی / پیکربندی‌های بررسی‌شده و انحرافات تأییدشده

سازمان، اطلاعات مربوط به بررسی پیکربندی‌ها و موارد انحراف را در لیست مؤلفه‌های موجود سیستم اطلاعاتی وارد می‌کند.

راهنمایی تکمیلی: این کنترل پیشرفته، درباره تنظیمات پیکربندی سازمان‌ها و مؤلفه‌های سیستم اطلاعاتی است و مشخص می‌نماید که آیا الزامات پیکربندی به درستی رعایت شده‌اند و آیا انحرافی در این زمینه وجود دارد یا خیر. کنترل‌های مربوطه: CM-2, CM-6.

(۷) لیست مؤلفه‌های موجود سیستم اطلاعاتی / مخزن مرکزی

سازمان، یک مخزن مرکزی را برای مؤلفه‌های موجود سیستم اطلاعاتی در نظر می‌گیرد.

راهنمایی تکمیلی: ممکن است سازمان‌ها تصمیم بگیرند که یک موجودی متمرکز را برای مؤلفه‌های تمام سیستم‌های اطلاعاتی سازمان مورد استفاده قرار دهند. با استفاده از چنین مخزن متمرکزی، می‌توان موجودی سخت‌افزار، نرم‌افزار و ثابت‌افزار را به شکل بهتر و مؤثرتری مدیریت کرد. این مخازن همچنین سازمان‌ها را یاری می‌کنند تا هویت و مکان افراد مسئول راهبری مؤلفه‌ها را به سرعت شناسایی نمایند. با استفاده از این مخازن، سازمان‌ها می‌توانند اطمینان داشته باشند که اطلاعات

[174] sandboxing

سیستمی لازم برای پاسخگو نمودن افراد مسئول (مانند انجمن سیستم اطلاعاتی یا مالک سیستم اطلاعاتی) را در اختیار دارند.

(۸) لیست مؤلفه‌های موجود سیستم اطلاعاتی / پیگیری خودکار مکان

سازمان با استفاده از سازوکارهای خودکار، از پیگیری مکان جغرافیایی مؤلفه‌های سیستم اطلاعاتی پشتیبانی می‌نماید.

راهنمایی تکمیلی: استفاده از سازوکارهای پیگیری خودکار مکان جغرافیایی مؤلفه‌های سیستم اطلاعاتی، دقت سیستم موجودی مؤلفه‌ها را افزایش می‌دهد. این قابلیت همچنین سازمان‌ها را یاری می‌کند تا مکان و افراد مسئول مؤلفه‌هایی که در معرض خطر یا مورد حمله قرار گرفته‌اند را شناسایی نمایند.

(۹) لیست مؤلفه‌های موجود سیستم اطلاعاتی / تخصیص مؤلفه‌ها به سیستم‌ها

سازمان:

الف. [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] را به یک سیستم اطلاعاتی تخصیص می‌دهد؛ و

ب. تأییدیه مربوطه را از مالک سیستم اطلاعاتی دریافت می‌کند.

راهنمایی تکمیلی: سازمان‌ها، معیارها یا انواع مؤلفه‌های سیستم اطلاعاتی (مانند ریزپردازنده‌ها، مادربوردها، نرم‌افزارها، کنترل‌گرهای منطقی قابل برنامه‌ریزی، یا دستگاه‌های شبکه) مربوط به این کنترل پیشرفته را تعیین می‌کنند. کنترل مربوطه: SA-4.

مراجع: شماره ویژه NIST 800-128.

اولویت و تخصیص به مجموعه‌های پایه:

P1	CM-8 اولویت پایین	CM-8(1)(3)(5) اولویت متوسط	CM-8(1)(2)(3)(4)(5) اولویت بالا

CM-9: طرح مدیریت پیکربندی

کنترل: سازمان یک طرح مدیریت پیکربندی برای سیستم اطلاعاتی تهیه، مستند و پیاده‌سازی می‌کند که ویژگی‌های زیر را دارا باشد:

الف. نقش‌ها، مسئولیت‌ها و فرایندها و رویه‌های مربوط به مدیریت پیکربندی را توضیح دهد؛

ب. فرایندی جهت شناسایی آیتم‌های پیکربندی در سرتاسر چرخه توسعه سیستم ایجاد کند که قابلیت مدیریت پیکربندی آیتم‌ها را نیز داشته باشد؛

پ. آیتم‌های پیکربندی سیستم اطلاعاتی و مکان این آیتم‌ها را تعریف کند؛ و

ت. برنامه مدیریت پیکربندی را از فاش شدن و دستکاری‌های غیر مجاز مصون دارد.

راهنمایی تکمیلی: طرح مدیریت پیکربندی، مبتنی بر الزامات خط‌مشی مدیریت پیکربندی است که البته برای هر سیستم اطلاعاتی اندکی تعدیل شده‌اند. این طرح‌ها، فرایند و رویه مربوط به استفاده از مدیریت پیکربندی برای پشتیبانی از توسعه سیستم اطلاعاتی را تشریح می‌کنند. طرح‌های مدیریت پیکربندی معمولا در مرحله توسعه یا اکتساب از زنجیره توسعه سیستم، تهیه و تدوین می‌شوند. این طرح‌ها تشریح می‌کنند که چگونه باید تغییرات را با توج به فرایندهای مدیریت تغییر اعمال کرد، چگونه باید تنظیمات پیکربندی را به‌روز نمود، چگونه باید محیط‌های توسعه، آزمون و عملیات را کنترل کرد، و چگونه باید اسناد مهم را توسعه داد، منتشر نمود و به‌روز کرد. سازمان‌ها می‌توانند برای حصول اطمینان از توسعه و پیاده‌سازی صحیح و به‌هنگام طرح‌های مدیریت پیکربندی، از قالب‌های آماده استفاده کنند. این قالب‌ها می‌توانند یک طرح مرجع مدیریت پیکربندی را در اختیار سازمان قرار دهند، که به صورت گام به گام در مورد هر سیستم اطلاعاتی قابل استفاده است. برای تأیید طرح‌های مدیریت پیکربندی، افراد اصلی مسئول بازبینی و تأیید تغییرات پیشنهادی و افراد مسئول تجزیه و تحلیل اثرات امنیتی، پیش از اعمال تغییرات در سیستم‌ها مشخص می‌گردند. منظور از آیتم‌های پیکربندی، آن دسته از آیتم‌های سیستم اطلاعاتی (سخت‌افزار، نرم‌افزار، ثابت‌افزار و مستندات) است که قرار است از لحاظ پیکربندی مدیریت شوند. با پیشروی در چرخه توسعه سیستم، ممکن است آیتم‌های پیکربندی جدیدی شناسایی شوند یا برخی از آیتم‌های پیکربندی پیشین، کنار گذاشته شوند. کنترل‌های مربوطه: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.

کنترل‌های پیشرفته:

(۱) طرح مدیریت پیکربندی / تخصیص مسئولیت‌ها

سازمان، مسئولیت تهیه فرایند مدیریت پیکربندی را به کارکنانی واگذار می‌کند که مستقیما در فرایند توسعه سیستم اطلاعاتی نقش ندارند.

راهنمایی تکمیلی: در صورتی که گروه مدیریت پیکربندی خاصی توسط سازمان تعیین نشده باشد، ممکن است این وظیفه به توسعه‌دهندگان سیستم واگذار شود و آن‌ها نیز از کارکنانی استفاده کنند که مستقیما در فرایند توسعه سیستم اطلاعاتی نقش ندارند. این تفکیک وظایف، سبب می‌شود که سطح مناسبی از استقلال بین فرایند توسعه سیستم اطلاعاتی و فرایند مدیریت پیکربندی وجود داشته باشد، کنترل کیفیت تهیل شود، و نظارت مؤثرتری صورت گیرد.

مراجع: شماره ویژه NIST 800-128.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	CM-9 اولویت متوسط	CM-9 اولویت بالا

CM-10: محدودیت‌های استفاده از نرم‌افزار

کنترل: سازمان:

الف. از نرم‌افزارها و مستندات مربوطه مطابق توافقات قرارداد و حقوق کپی‌رایت استفاده می‌کند؛

ب. استفاده از نرم‌افزارها و مستندات مربوطه که تنها افراد محدودی مجوز دسترسی به آن‌ها دارند را پیگیری می‌کند تا کپی و انتشار آن‌ها را کنترل کند؛ و

پ. استفاده از فناوری اشتراک‌گذاری فایل همتابه‌همتا را کنترل و ثبت می‌کند تا مطمئن شود از این فناوری در جهت انتشار غیرمجاز، نمایش، اجرا یا تولید دوباره کارهایی که حق کپی‌رایت دارند، استفاده نمی‌شود.

راهنمایی تکمیلی: پیگیری مجوز نرم‌افزارها می‌تواند با توجه به نیازهای سازمان، با روش‌های دستی (مثلاً صفحات گسترده ساده) یا با روش‌های خودکار (مثل نرم‌افزارهای پیگیری تخصصی) انجام شود. کنترل‌های مربوطه: AC-17، CM-8 و SC-7.

کنترل‌های پیشرفته:

(۱) محدودیت‌های استفاده از نرم‌افزار | نرم‌افزارهای کدباز

سازمان محدودیت‌های زیر را برای استفاده از نرم‌افزارهای کدباز ایجاد می‌کند:

راهنمایی تکمیلی: نرم‌افزار کدباز به نرم‌افزاری گفته می‌شود که کدهای اصلی آن در دسترس است. برخی امتیازات نرم‌افزارها که معمولاً در اختیار دارندگان حق کپی‌رایت است، معمولا از طریق موافقت‌نامه‌ها و مجوزها در اختیار سایر افراد قرار می‌گیرند، تا آن‌ها نیز بتوانند اقدام به بررسی، تغییر و ارتقای نرم‌افزارها نمایند. از چشم‌انداز امنیتی، مزیت اصلی نرم‌افزارهای کدباز این است که سازمان‌ها را قادر به بررسی کدهای اصلی آن‌ها می‌نماید. با این حال، الزاماتی برای دریافت مجوز استفاده از این نرم‌افزارها نیز وجود دارد، که از آن میان می‌توان به محدودیت‌هایی در زمینه استفاده فرعی از آن‌ها اشاره کرد.

مراجع: ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	CM-10 اولویت پایین	CM-10 اولویت متوسط	CM-10 اولویت بالا

CM-11: **نرم‌افزارهای نصب‌شده توسط کاربر**

کنترل: سازمان:

الف. سیاست‌هایی جهت نظارت بر نصب نرم‌افزار توسط کاربران، تدوین می‌کند.

ب. از طریق [اختصاص: روش‌های تعیین‌شده توسط سازمان] این سیاست‌ها را اجرا می‌کند.

پ. [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] پیروی از سیاست‌های نصب نرم‌افزار را نظارت می‌کند.

راهنمایی تکمیلی: تنها در صورتی که امتیازات لازم به کاربران داده شود، آن‌ها می‌توانند در سیستم‌های اطلاعاتی نرم‌افزار نصب کنند. برای داشتن کنترل بر نوع نرم‌افزارهایی که نصب می‌شوند نیز، سازمان‌ها یک سری اقدامات مجاز و غیزمجاز در زمینه نصب نرم‌افزار تعیین می‌کنند. یک اقدام مجاز می‌تواند به‌روزرسانی و نصب بسته‌های تعمیری برای نرم‌افزارهای موجود باشد. نمونه دیگر دانلود نرم‌افزار از «app store» های مورد تأیید سازمان است. اقدامات ممنوع در زمینه نصب نرم‌افزار نیز می‌تواند نصب نرم‌افزار از منابع ناشناخته یا مشکوک باشد. نصب نرم‌افزارهایی که از نظر سازمان‌ها به طور بالقوه مخرب تلقی می‌شوند نیز می‌تواند اقدامی غیرمجاز باشد. سیاست‌هایی که سازمان‌ها برای نظارت و کنترل بر نرم‌افزارهای نصب‌شده توسط کاربران انتخاب می‌کنند،

ممکن است توسط خود سازمان یا برخی سازمان‌های خارجی تدوین شده باشند. روش‌های اجرای سیاست نیز شامل روش‌های رویه‌ای (مثل بررسی دوره‌ای حساب کاربران)، روش‌های خودکار (مثل تنظیمات پیکربندی که در سیستم‌های اطلاعاتی پیاده‌سازی می‌شوند) یا جفت آن‌هاست. کنترل‌های مربوطه: AC-3، CM-2، CM-3، CM-5، CM-6، CM-7 و PL-4.

کنترل‌های پیشرفته:

(۱) نرم‌افزارهای نصب‌شده توسط کاربران | هشدارهایی برای نصب‌های غیرمجاز

وقتی نصب غیرمجاز نرم‌افزار شناسایی شود، سیستم اطلاعاتی به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] هشدار می‌دهد.

راهنمایی تکمیلی: کنترل‌های مربوطه: CA-7 و SI-4.

(۲) نرم‌افزارهای نصب‌شده توسط کاربران | نصب غیرمجاز بدون داشتن اختیار این کار

سیستم اطلاعاتی نصب نرم‌افزار توسط کاربرانی که اختیار این کار ندارند را ممنوع می‌کند.

راهنمایی تکمیلی: اختیار نصب نرم‌افزار می‌تواند اکتسابی باشد، مثلاً از طریق راهبر سیستم. کنترل مربوطه: AC-6.

مراجع: ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	CM-11 اولویت پایین	CM-11 اولویت متوسط	CM-11 اولویت بالا

خانواده: برنامه‌ریزی برای رویدادهای آینده

CP-1: خط‌مشی و رویه‌های برنامه‌ریزی برای رویدادهای آینده

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۹. خط‌مشی برنامه‌ریزی برای رویدادهای آینده شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و
۱۰. رویه‌های تسهیل پیاده‌سازی خط‌مشی برنامه‌ریزی برای رویدادهای آینده و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۹. خط‌مشی برنامه‌ریزی برای رویدادهای آینده؛ و
۱۰. رویه‌های برنامه‌ریزی برای رویدادهای آینده.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده CP را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: رهنمود شماره ۱ فدرال در مورد برنامه‌ریزی برای رویدادهای آینده؛ شماره‌های ویژه NIST 800-12, 800-34, 800-100.

اولویت و تخصیص به مجموعه‌های پایه:

P1	CP-1 اولویت پایین	CP-1 اولویت متوسط	CP-1 اولویت بالا

CP-2: طرح برنامه‌ریزی برای رویدادهای آینده

کنترل: سازمان:

الف. یک طرح برنامه‌ریزی برای رویدادهای آینده را برای سیستم اطلاعاتی تهیه می‌کند که کارکردهای زیر را داشته باشد:

۱. شناسایی مأموریت‌ها و فرایندهای کسب‌وکار و الزامات موجود در زمینه برنامه‌ریزی برای رویدادهای آینده؛
۲. ارائه معیارها، اولویت‌های ترمیمی، و اهداف بازیابی؛
۳. تعیین افراد، نقش‌ها و مسئولیت‌های برنامه‌ریزی برای رویدادهای آینده؛
۴. ارائه طرح‌هایی برای ادامه دادن مأموریت‌ها و فرایندهای ضروری کسب‌وکار در شرایطی که کارکرد سیستم اطلاعاتی مختل شده باشد؛
۵. بازیابی کامل سیستم اطلاعاتی، بدون از دست رفتن ابزارها و ضمانت‌های امنیتی که از ابتدا در نظر گرفته شده‌اند؛ و
۶. بازبینی و تأیید توسط [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان].

ب. نسخه‌هایی از طرح برنامه‌ریزی برای رویدادهای آینده را بین [اختصاص: کارکنان اصلی مسئول برنامه‌ریزی برای رویدادهای آینده (تعیین‌شده بر اساس نام یا نقش آن‌ها) و عناصر سازمانی تعیین‌شده توسط سازمان] توزیع می‌کند؛

پ. فعالیت‌های مربوط به برنامه‌ریزی برای رویدادهای آینده را با فعالیت‌های مربوط به مدیریت رخدادها هماهنگ می‌کند؛

ت. طرح برنامه‌ریزی برای رویدادهای آینده مربوط به سیستم اطلاعاتی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند؛

ث. طرح برنامه‌ریزی برای رویدادهای آینده را بر اساس تغییرات صورت گرفته در سازمان، سیستم اطلاعاتی و محیط کاری، و همچنین بر اساس مشکلات مشاهده‌شده در مرحله پیاده‌سازی، اجرا یا آزمایش طرح، به‌روزرسانی می‌کند؛

ج. تغییرات صورت گرفته در طرح برنامه‌ریزی برای رویدادهای آینده را به [اختصاص: کارکنان اصلی مسئول برنامه‌ریزی برای رویدادهای آینده (تعیین‌شده بر اساس نام یا نقش آن‌ها) و عناصر سازمانی تعیین‌شده توسط سازمان] اطلاع می‌دهد؛ و

چ. طرح برنامه‌ریزی برای رویدادهای آینده را در برابر افشا یا تغییرات غیرمجاز محافظت می‌کند.

راهنمایی‌های تکمیلی: برنامه‌ریزی برای رویدادهای آینده سیستم‌های اطلاعاتی، بخشی از برنامه کلی سازمان برای استمرار مأموریت‌ها و فرایندهای کسب‌وکار است. در برنامه‌ریزی برای رویدادهای آینده تعیین می‌شود که در صورت اخلال در فعالیت‌های سیستم‌های اطلاعاتی، چگونه باید این سیستم‌ها را بازیابی نمود یا مأموریت‌ها و فرایندهای کسب‌وکار جایگزینی را پیاده‌سازی کرد. برای افزایش اثربخشی برنامه‌ریزی برای رویدادهای آینده، باید برنامه‌ریزی‌های مذکور را در تمام چرخه عمر توسعه سیستم در نظر داشت. برنامه‌ریزی برای رویدادهای آینده در هنگام توسعه نرم‌افزارها، سخت‌افزارها و ثابت‌افزارها می‌تواند راه مناسبی برای ایجاد انعطاف مطلوب در سیستم‌های اطلاعاتی باشد. در برنامه‌ریزی برای رویدادهای آینده تعیین می‌شود که سیستم اطلاعاتی سازمان باید چه سطحی از قابلیت انعطاف و بازیابی را داشته باشد. برای این که سیستم اطلاعاتی بتواند به فعالیت‌های خود ادامه دهد، لازم نیست که تمام مؤلفه‌ها به طور کامل بازیابی شوند. اهداف تعیین‌شده در زمینه بازیابی سیستم‌های اطلاعاتی، مبتنی بر دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. علاوه بر مسئله در دسترس بودن سیستم‌های اطلاعاتی، در برنامه‌ریزی برای رویدادهای آینده به موارد امنیتی دیگری که سبب وقفه در مأموریت‌ها و فرایندهای کسب‌وکار سازمان می‌شوند نیز پرداخته می‌شود. از جمله این موارد می‌توان به حملات مخربی اشاره کرد که محرمانگی و یکپارچگی سیستم‌های اطلاعاتی را در معرض خطر قرار می‌دهند. در برنامه‌ریزی برای رویدادهای آینده به مواردی همچون توقف عملیات سیستم‌های اطلاعاتی، بازگشت به حالت عملیات دستی، تغییر جریان‌های اطلاعات، و فعالیت سیستم در حالتی مشابه آنچه در شرایط حمله رخ می‌دهد اشاره کرد. سازمان‌ها می‌توانند با ایجاد هماهنگی بین

برنامه‌ریزی برای رویدادهای آینده و فعالیت‌های برنامه‌ریزی‌شده برای مدیریت رخدادها، اطمینان حاصل کنند که در صورت اتفاق افتادن موارد امنیتی، ابزارها و قابلیت‌های لازم برای ادامه فعالیت‌ها را دارند. کنترل‌های مربوطه: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

کنترل‌های پیشرفته:

(۱) طرح برنامه‌ریزی برای رویدادهای آینده / ایجاد هماهنگی با سایر طرح‌های مربوطه

سازمان، در زمینه توسعه برنامه‌ریزی برای رویدادهای آینده، هماهنگی لازم را با عناصر سازمانی فعال در زمینه طرح‌های مربوطه انجام می‌دهد.

راهنمایی‌های تکمیلی: طرح‌های مربوطه شامل مواردی از جمله طرح‌های رویدادهای آینده در زمینه کسب‌وکار، طرح‌های بازیابی سیستم پس از فاجعه، طرح‌های استمرار عملیات، طرح‌های ارتباط در شرایط بحران، طرح‌های زیرساخت‌های اصلی، طرح‌های پاسخ به رخدادهای سایبری، طرح پیاده‌سازی تهدیدات داخلی، و طرح‌های شرایط اضطراری هستند.

(۲) طرح برنامه‌ریزی برای رویدادهای آینده / برنامه‌ریزی ظرفیت‌ها

سازمان، برنامه‌ریزی ظرفیت‌ها را انجام می‌دهد تا اطمینان حاصل کند که ظرفیت‌های پردازشی، مخابراتی و محیطی لازم در صورت اتفاق افتادن رویدادهای آینده وجود دارند.

راهنمایی‌های تکمیلی: برنامه‌ریزی ظرفیت‌ها به این دلیل لازم است که تهدیدات مختلف (از جمله بلایای طبیعی و حملات سایبری) می‌توانند سبب کاهش ظرفیت‌های پردازشی، مخابراتی و محیطی شوند و مأموریت‌ها و فرایندهای کسب‌وکار سازمان را در شرایط بحران به خطر اندازند. سازمان‌ها باید انتظار داشته باشند که در چنین شرایطی، برخی ظرفیت‌های خود را از دست بدهند.

(۳) طرح برنامه‌ریزی برای رویدادهای آینده / استمرار مأموریت‌ها و عملکردهای اصلی کسب‌وکار

سازمان، خود را آماده می‌کند تا در صورت رخ دادن اتفاقاتی در آینده، مأموریت‌ها و عملکردهای اصلی کسب‌وکار را برای [اختصاص: مدت زمان تعیین‌شده توسط سازمان] ادامه دهد.

راهنمایی‌های تکمیلی: ممکن است سازمان‌ها تصمیم بگیرند که برنامه‌ریزی برای رویدادهای آینده را به عنوان بخشی از برنامه‌ریزی استمرار عملیات انجام دهند. به عنوان مثال، برنامه‌ریزی برای رویدادهای آینده می‌تواند بخشی از تحلیل تأثیرات کسب‌وکار باشد. مدت زمان تعیین‌شده برای بازیابی و استمرار مأموریت‌ها و فرایندهای کسب‌وکار سازمان، به عواملی همچون شدت و مدت زمان وقفه‌های ایجادشده در سیستم اطلاعاتی و زیرساخت‌های آن بستگی دارد. کنترل مربوطه: PE-12.

(۴) طرح برنامه‌ریزی برای رویدادهای آینده / استمرار تمام مأموریت‌ها و عملکردهای کسب‌وکار

سازمان، خود را آماده می‌کند تا در صورت رخ دادن اتفاقاتی در آینده، تمام مأموریت‌ها و عملکردهای کسب‌وکار را برای [اختصاص: مدت زمان تعیین‌شده توسط سازمان] ادامه دهد.

راهنمایی‌های تکمیلی: ممکن است سازمان‌ها تصمیم بگیرند که برنامه‌ریزی برای رویدادهای آینده را به عنوان بخشی از برنامه‌ریزی استمرار عملیات انجام دهند. به عنوان مثال، برنامه‌ریزی برای رویدادهای آینده می‌تواند بخشی از تحلیل تأثیرات کسب‌وکار باشد. مدت زمان تعیین‌شده برای بازیابی و استمرار مأموریت‌ها و فرایندهای کسب‌وکار سازمان، به عواملی همچون شدت و مدت زمان وقفه‌های ایجادشده در سیستم اطلاعاتی و زیرساخت‌های آن بستگی دارد. کنترل مربوطه: PE-12.

(۵) طرح برنامه‌ریزی برای رویدادهای آینده / ادامه یافتن مأموریت‌ها و عملکردهای اصلی کسب‌وکار

سازمان، خود را آماده می‌کند تا در صورت رخ دادن اتفاقاتی در آینده، مأموریت‌ها و عملکردهای اصلی کسب‌وکار را بدون وقفه ادامه دهد و این شرایط را حفظ کند تا زمانی که سیستم اطلاعاتی در سایت پردازش و/یا ذخیره‌سازی اولیه بازیابی شود.

راهنمایی‌های تکمیلی: ممکن است سازمان‌ها تصمیم بگیرند که برنامه‌ریزی برای رویدادهای آینده را به عنوان بخشی از برنامه‌ریزی استمرار عملیات انجام دهند. به عنوان مثال، برنامه‌ریزی برای رویدادهای آینده می‌تواند بخشی از تحلیل تأثیرات کسب‌وکار باشد. سایت‌های پردازش و/یا ذخیره‌سازی اولیه ممکن است در اثر رویدادهای آینده تغییر کنند (مثلاً ممکن است سایت‌های پشتیبان تبدیل به سایت‌های اولیه شوند). کنترل مربوطه: PE-12.

(۶) طرح برنامه‌ریزی برای رویدادهای آینده / سایت‌های پردازش و/یا ذخیره‌سازی جایگزین

سازمان، خود را آماده می‌کند تا در صورت رخ دادن اتفاقاتی در آینده، مأموریت‌ها و عملکردهای اصلی کسب‌وکار را بدون ایجاد وقفه در عملیات به سایت‌های پردازش و/یا ذخیره‌سازی جایگزین انتقال دهد و این شرایط را حفظ کند تا زمانی که سیستم اطلاعاتی در سایت پردازش و/یا ذخیره‌سازی اولیه بازیابی شود.

راهنمایی‌های تکمیلی: ممکن است سازمان‌ها تصمیم بگیرند که برنامه‌ریزی برای رویدادهای آینده را به عنوان بخشی از برنامه‌ریزی استمرار عملیات انجام دهند. به عنوان مثال، برنامه‌ریزی برای رویدادهای آینده می‌تواند بخشی از تحلیل تأثیرات کسب‌وکار باشد. سایت‌های پردازش و/یا ذخیره‌سازی اولیه ممکن است در اثر رویدادهای آینده تغییر کنند (مثلاً ممکن است سایت‌های پشتیبان تبدیل به سایت‌های اولیه شوند). کنترل مربوطه: PE-12.

(۷) طرح برنامه‌ریزی برای رویدادهای آینده / ایجاد هماهنگی با تأمین‌کنندگان خدمات خارجی

سازمان، برنامه‌ریزی برای رویدادهای آینده را بر اساس برنامه‌های متناظر تأمین‌کنندگان خدمات خارجی انجام می‌دهد تا اطمینان حاصل نماید که الزامات مربوطه رعایت شده‌اند.

راهنمایی‌های تکمیلی: هنگامی که قابلیت یک سازمان برای انجام موفقیت‌آمیز مأموریت‌ها و فرایندهای کسب‌وکار خود وابسته به تأمین‌کنندکان خدمات خارجی باشد، تهیه یک طرح برنامه‌ریزی برای رویدادهای آینده تبدیل به امری دشوار و چالش‌برانگیز خواهد شد. در این شرایط، سازمان برنامه‌ریزی برای رویدادهای آینده را بر اساس برنامه‌های متناظر تأمین‌کنندگان خدمات خارجی انجام می‌دهد تا اطمینان حاصل نماید که طرح تهیه‌شده بازتاب‌دهنده نیازهای سازمان است. کنترل مربوطه: SA-9.

(۸) طرح برنامه‌ریزی برای رویدادهای آینده / شناسایی سرمایه‌های اصلی

سازمان، سرمایه‌های اصلی سیستم‌های اطلاعاتی برای پشتیبانی از مأموریت‌ها و عملکردهای اصلی کسب‌وکار را شناسایی می‌کند.

راهنمایی‌های تکمیلی: ممکن است سازمان‌ها تصمیم بگیرند که برنامه‌ریزی برای رویدادهای آینده را به عنوان بخشی از برنامه‌ریزی استمرار عملیات انجام دهند. در این شرایط، سازمان‌ها وظیفه شناسایی سرمایه‌های اصلی سیستم‌های اطلاعاتی را به گونه‌ای انجام می‌دهند که بتوان ابزارهای دیگری به جز ابزارهای معمول را نیز به کار گرفت و در شرایط بحران، مأموریت‌ها و عملکردهای کسب‌وکار را ادامه داد. علاوه بر این، شناسایی سرمایه‌های اطلاعاتی اصلی سبب می‌شود که سازمان‌ها راحت‌تر بتوانند منابع خود را اولویت‌بندی کنند. سرمایه‌های اصلی سیستم‌های اطلاعاتی، شامل سرمایه‌های عملیاتی و فنی هستند. به عنوان مثالی از سرمایه‌های فنی می‌توان به خدمات IT، مؤلفه‌های سیستم‌های اطلاعاتی، محصولات IT، و سازوکارها اشاره کرد. سرمایه‌های عملیاتی نیز مواردی از جمله رویه‌ها (عملیاتی که به صورت دستی انجام می‌شوند) و کارکنان (افرادی که ابزارهای فنی را به کار می‌گیرند یا رویه‌های دستی را انجام می‌دهند) را در بر می‌گیرد. طرح‌های حفاظت از برنامه‌های سازمانی، می‌توانند سازمان‌ها را در امر شناسایی سرمایه‌های اصلی یاری کنند. کنترل‌های مربوطه: SA-14, SA-15.

مراجع: رهنمود شماره ۱ فدرال در مورد ادامه یافتن عملیات سازمانی؛ شماره ویژه NIST 800-34.

اولویت و تخصیص به مجموعه‌های پایه:

P1	CP-2 اولویت پایین	CP-2(1)(3)(8) اولویت متوسط	CP-2(1)(2)(3)(4)(5)(8) اولویت بالا

CP-3: آموزش برای مواجهه با رویدادهای آینده

کنترل: سازمان، آموزش‌های متناسب با نقش‌ها و مسئولیت‌ها را با توجه به موارد زیر به کاربران سیستم‌های اطلاعاتی ارائه می‌کند:

الف. در [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] که انتظار می‌رود کاربران مذکور همچنان مسئولیت‌های خود را در زمینه برنامه‌ریزی برای رویدادهای آینده داشته باشند؛

ب. در صورتی که به موجب تغییر سیستم‌های اطلاعاتی، این آموزش‌ها ضروری شوند؛ و

پ. [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: آموزش برای مواجهه با رویدادهای آینده، بر اساس نقش‌ها و مسئولیت‌های کارکنان سازمان به آن‌ها ارائه می‌شود تا اطمینان حاصل شود که محتوا و اطلاعات مناسبی در اختیار آن‌ها قرار گرفته است. به عنوان مثال، ممکن است کاربران معمولی تنها به آموزش زمان و مکان گزارش‌دهی رویدادها نیاز داشته باشند، یا این که آموزش داده شوند که در گزارشات خود قید کنند که رویداد بر کاربران معمولی نیز تأثیر گذاشته است یا خیر. اما راهبران سیستم به آموزش‌های بیشتری نیاز دارند. آن‌ها باید بدانند که چه هنگام از سایت‌های پردازش و ذخیره‌سازی جایگزین استفاده کنند. آموزش مدیران ارشد حتی از این هم دقیق‌تر خواهد بود. آن‌ها باید بدانند که چگونه عملیات اصلی سازمان را در مکان‌های خارج از سازمان انجام دهند و چگونه ارتباطات و هماهنگی‌های لازم در زمینه رویدادهای آینده را با سایر مؤسسات دولتی صورت دهند. آموزش‌های متناسب با نقش‌ها و مسئولیت‌ها، بازتاب‌دهنده الزامات مورد اشاره در طرح‌های آماده‌سازی برای رویدادهای آینده هستند. کنترل‌های مربوطه: AT-2, AT-3, CP-2, IR-2.

کنترل‌های پیشرفته:

(۱) آموزش برای مواجهه با رویدادهای آینده / رویدادهای شبیه‌سازی‌شده

سازمان، به منظور آموزش برای مواجهه با رویدادهای آینده از شبیه‌سازی رویدادها استفاده می‌کند تا کارکنان بتوانند در شرایط بحران، واکنش‌های بهتری از خود نشان دهند.

(۲) آموزش برای مواجهه با رویدادهای آینده / محیط‌های آموزشی خودکار

سازمان از سازوکارهای خودکار استفاده می‌کند تا محیط‌های آموزشی کامل‌تر و واقع‌گرایانه‌تری را برای کارکنان فراهم آورد.

مراجع: رهنمود شماره ۱ فدرال در مورد برنامه‌ریزی برای رویدادهای آینده؛ شماره‌های ویژه NIST 800-16, 800-50.

اولویت و تخصیص به مجموعه‌های پایه:

P2	CP-3 اولویت پایین	CP-3 اولویت متوسط	CP-3(1) اولویت بالا

CP-4: آزمون کردن طرح‌های برنامه‌ریزی برای رویدادهای آینده

کنترل: سازمان:

الف. طرح‌های برنامه‌ریزی برای رویدادهای آینده مربوط به سیستم اطلاعاتی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] با استفاده از [اختصاص: آزمون‌های تعیین‌شده توسط سازمان] آزمون می‌کند تا اثربخشی این طرح‌ها و آمادگی سازمان برای اجرای آن‌ها مشخص شود؛

ب. نتایج آزمون‌های صورت‌گرفته را بازبینی می‌کند؛ و

پ. در صورت لزوم، اقدامات اصلاحی را آغاز می‌کند.

راهنمایی‌های تکمیلی: از جمله روش‌های مورد استفاده برای انجام آزمون‌های مذکور می‌توان به آزمون گام به گام[۱۷۵]، آزمون tabletop، استفاده از چک‌لیست‌ها، روش‌های شبیه‌سازی (شبیه‌سازی موازی، شبیه‌سازی اختلال کامل) و آزمون‌های جامع اشاره کرد. سازمان‌ها، آزمون‌های خود را بر اساس الزامات تعیین‌شده در زمینه استمرار عملکرد و همچنین بر اساس اثرات به جای مانده بر عملیات سازمانی، سرمایه‌ها و افراد انجام می‌دهند. سازمان‌ها در زمینه گستردگی، عمق و زمان‌بندی فعالیت‌های اصلاحی، دارای آزادی عمل هستند. کنترل‌های مربوطه: CP-2, CP-3, IR-3.

کنترل‌های پیشرفته:

(۱) آزمون کردن طرح‌های برنامه‌ریزی برای رویدادهای آینده / ایجاد هماهنگی با طرح‌های مرتبط سازمان، بین آزمون‌های مربوط به طرح‌های برنامه‌ریزی برای رویدادهای آینده و آن دسته از عناصر سازمانی که مسئول این آزمون‌ها هستند، هماهنگی‌های لازم را ایجاد می‌کند.

[175] walk-through exercise

راهنمایی‌های تکمیلی: طرح‌های مربوط به برنامه‌ریزی برای رویدادهای آینده شامل مواردی از جمله طرح‌های رویدادهای آینده در زمینه کسب‌وکار، طرح‌های بازیابی سیستم پس از فاجعه، طرح‌های استمرار عملیات، طرح‌های ارتباط در شرایط بحران، طرح‌های زیرساخت‌های اصلی، طرح‌های پاسخ به رخدادهای سایبری، طرح پیاده‌سازی تهدیدات داخلی، و طرح‌های شرایط اضطراری هستند. این کنترل پیشرفته، سازمان‌ها را ملزم به ایجاد عناصر سازمانی برای مدیریت طرح‌ها یا اختصاص طرح‌ها به عناصر خاص نمی‌کند. با این حال، در صورتی که تعدادی عناصر سازمانی وجود دارند که مسئول طرح‌های مذکور هستند، سازمان‌ها باید هماهنگی‌های لازم را با آن عناصر به عمل آورند. کنترل‌های مربوطه: IR-8, PM-8.

(۲) آزمون کردن طرح‌های برنامه‌ریزی برای رویدادهای آینده / سایت پردازش جایگزین

سازمان، طرح‌های برنامه‌ریزی برای رویدادهای آینده را در سایت پردازش جایگزین آزمون می‌کند تا اهداف زیر را محقق سازد:

(الف) آشنا کردن کارکنان مربوط به این طرح‌ها با تأسیسات و منابع موجود؛ و

(ب) ارزیابی قابلیت سایت پردازش جایگزین برای پشتیبانی از عملیات مربوط به طرح‌های برنامه‌ریزی برای رویدادهای آینده.

راهنمایی‌های تکمیلی: کنترل مربوطه: CP-7.

(۳) آزمون کردن طرح‌های برنامه‌ریزی برای رویدادهای آینده / آزمون خودکار

سازمان، سازوکارهای خودکار را به کار می‌گیرد تا طرح‌های برنامه‌ریزی برای رویدادهای آینده را به گونه‌ای جامع‌تر و مؤثرتر آزمون کند.

راهنمایی‌های تکمیلی: سازوکارهای خودکار، امکاناتی از قبیل موارد روبرو را فراهم می‌آورند و می‌توان با استفاده از آن‌ها، طرح‌های برنامه‌ریزی برای رویدادهای آینده را به گونه‌ای جامع‌تر و مؤثرتر آزمون کرد: (۱) پوشش دادن بهتر مسائل مربوط به برنامه‌ریزی برای رویدادهای آینده؛ (۲) انتخاب محیط‌ها و سناریوهای واقع‌گرایانه‌تر برای آزمون‌ها؛ و (۳) تأکید بر سیستم اطلاعاتی و مأموریت‌های آن.

(۴) آزمون کردن طرح‌های برنامه‌ریزی برای رویدادهای آینده / بازسازی و بازیابی کامل

سازمان، به عنوان بخشی از آزمون طرح‌های برنامه‌ریزی برای رویدادهای آینده، سیستم اطلاعاتی را به طور کامل بازیابی می‌کند یا تا حد تعیین‌شده بازسازی می‌نماید.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: CP-10, SC-24.

مراجع: رهنمود شماره ۱ فدرال در مورد برنامه‌ریزی برای رویدادهای آینده؛ FIPS 199؛ شماره‌های ویژه NIST 800-34, 800-85.

اولویت و تخصیص به مجموعه‌های پایه:

P2	CP-4 اولویت پایین	CP-4(1) اولویت متوسط	CP-4(1)(2) اولویت بالا

CP-5: به‌روزرسانی طرح‌های برنامه‌ریزی برای رویدادهای آینده

[حذف شد: به بخش CP-2 منتقل شد].

CP-6: سایت ذخیره‌سازی جایگزین

کنترل: سازمان:

الف. یک سایت ذخیره‌سازی جایگزین را ایجاد می‌کند و هماهنگی‌های لازم را برای ذخیره‌سازی و بازیابی نسخه پشتیبان اطلاعات مربوط به سیستم اطلاعاتی انجام می‌دهد؛ و

ب. اطمینان حاصل می‌نماید که امنیت اطلاعات در این سایت نیز درست مانند سایت اولیه تضمین شده است.

راهنمایی‌های تکمیلی: سایت‌های ذخیره‌سازی جایگزین، از لحاظ جغرافیایی در موقعیتی مجزا از سایت ذخیره‌سازی اولیه قرار دارند. نسخه پشتیبان داده‌ها و اطلاعات در سایت ذخیره‌سازی جایگزین نگهداری می‌شوند تا در صورتی که سایت اولیه در دسترس نباشد، از آن‌ها استفاده شود. مواردی که در موافقت‌نامه‌های سایت ذخیره‌سازی جایگزین به آن‌ها اشاره می‌شود شامل شرایط محیطی سایت‌های جایگزین، قوانین دسترسی، الزامات حفاظت محیطی و فیزیکی، و هماهنگی در زمینه تحویل و بازیابی رسانه‌های پشتیبان هستند. الزامات طرح‌های برنامه‌ریزی برای رویدادهای آینده، در سایت‌های ذخیره‌سازی جایگزین رعایت می‌شوند، تا سازمان‌ها بتوانند در صورت بروز اخلال یا از کار افتادن سیستم‌های اطلاعات خود، مأموریت‌ها و فرایندهای کسب‌وکار را ادامه دهند. کنترل‌های مربوطه: CP-2, CP-7, CP-9, CP-10, MP-4.

کنترل‌های پیشرفته:

(۱) سایت ذخیره‌سازی جایگزین / مجزا بودن از سایت اولیه

سازمان، مکانی را به عنوان سایت ذخیره‌سازی جایگزین در نظر می‌گیرد که مجزا از سایت اولیه باشد، به گونه‌ای که یک تهدید واحد هر دو سایت را هدف قرار ندهد.

راهنمایی‌های تکمیلی: تهدیداتی که ممکن است سایت ذخیره‌سازی جایگزین را تحت تأثیر قرار دهند، در بررسی‌های مخاطرات سازمانی تعیین می‌شوند. به عنوان مثال‌هایی از این تهدیدات می‌توان به بلایای طبیعی، شکست‌های ساختاری، حملات سایبری خصمانه، و خطاهای صورت‌گرفته در کنارگذاشتن یا به‌کارگماری کارکنان اشاره کرد. بر اساس نوع تهدیدات، سازمان‌ها تعیین می‌کنند که چه فاصله‌ای باید بین سایت اولیه و سایت جایگزین وجود داشته باشد. در مورد یکی از انواع تهدیداتی که به آن اشاره شد (یعنی حملات سایبری خصمانه)، فاصله بین سایت‌ها اهمیت چندانی ندارد. کنترل مربوطه: RA-3.

(۲) سایت ذخیره‌سازی جایگزین / اهداف و زمان بازیابی

سازمان، سایت ذخیره‌سازی جایگزین را به گونه‌ای پیکربندی می‌کند که عملیات بازیابی با توجه به اهداف و زمان، به شکل ساده‌تری انجام شود.

(۳) سایت ذخیره‌سازی جایگزین / دسترسی

سازمان، احتمال اخلال و بلایای گسترده را در نظر می‌گیرد و با شناسایی مشکلات بالقوه در زمینه دسترسی به سایت ذخیره‌سازی جایگزین، اقداماتی را برای کاهش خسارت‌ها تعیین می‌کند.

راهنمایی‌های تکمیلی: منظور از اخلال گسترده، اخلالی است که در یک محدوده جغرافیایی گسترده رخ دهد (مانند طوفان، قطع برق گسترده). این انواع اخلال، بر اساس بررسی‌های مخاطرات سازمانی تعیین می‌شوند. به عنوان مثال‌هایی از اقدامات کاهش خسارات، می‌توان به این موارد اشاره کرد: (۱) قرار دادن نسخه‌هایی از اطلاعات در مجموعه‌ای دیگر از سایت‌های ذخیره‌سازی جایگزین، در صورتی که مشکل دسترسی به سایت‌های اولیه ذخیره‌سازی جایگزین وجود داشته باشد؛ یا (۲) برنامه‌ریزی برای دسترسی فیزیکی، به منظور بازیابی اطلاعات پشتیبان، در صورتی که دسترسی الکترونیک به سایت‌های جایگزین دچار وقفه شده باشد. کنترل‌های مربوطه: RA-3.

مراجع: شماره ویژه NIST 800-34.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	CP-6(1)(3) اولویت متوسط	CP-6(1)(2)(3) اولویت بالا

CP-7: سایت پردازش جایگزین

کنترل: سازمان:

الف. یک سایت ذخیره‌سازی جایگزین را ایجاد می‌کند و هماهنگی‌های لازم را انجام می‌دهد تا در صورت از دست رفتن قابلیت‌های پردازشی اولیه، [اختصاص: عملیات سیستم اطلاعاتی که توسط سازمان تعیین شده‌اند] مربوط به مأموریت‌ها و فرایندهای اصلی کسب‌وکار [اختصاص: در بازه زمانی تعیین‌شده توسط سازمان، متناسب با زمان و اهداف بازیابی] ادامه یابند؛

ب. اطمینان حاصل می‌نماید که تجهیزات و وسایل مورد نیاز برای انتقال و ادامه فعالیت‌ها، در سایت پردازش جایگزین وجود دارند، و یا این که در قراردادها شرایط و ضوابطی در نظر گرفته شده است که این تجهیزات و وسایل در بازه زمانی تعیین‌شده توسط سازمان فراهم شوند؛ و

پ. اطمینان حاصل می‌نماید که امنیت اطلاعات در این سایت نیز درست مانند سایت اولیه تضمین شده است.

راهنمایی‌های تکمیلی: سایت‌های پردازش جایگزین، از لحاظ جغرافیایی در موقعیتی مجزا از سایت پردازش اولیه قرار دارند. در صورتی که اتفاقی رخ دهد و امکان استفاده از سایت پردازش اولیه وجود نداشته باشد، از این سایت‌های جایگزین استفاده می‌شود. در موافقت‌نامه‌های مربوط به سایت‌های پردازش جایگزین، به مواردی همچون شرایط محیطی در این سایت‌ها، قوانین دسترسی، الزامات حفاظت فیزیکی و محیطی، و هماهنگی برای انتخاب و اختصاص کارکنان پرداخته می‌شود. الزامات مربوط به این سایت‌ها به گونه‌ای در نظر گرفته می‌شوند که در صورت رخ دادن اتفاقاتی در آینده و از دسترسی خارج شدن سایت و سیستم‌های اطلاعاتی اولیه، امکان ادامه فعالیت‌ها وجود داشته باشد. کنترل‌های مربوطه: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.

کنترل‌های پیشرفته:

(۱) سایت پردازش جایگزین / مجزا بودن از سایت اولیه

سازمان، سایت پردازش جایگزین را به گونه‌ای انتخاب می‌کند که از لحاظ جغرافیایی مجزا از سایت اولیه باشد و تهدیداتی که سایت اولیه را تحت تأثیر قرار داده‌اند، بر آن تأثیری نداشته باشند.

راهنمایی‌های تکمیلی: تهدیداتی که ممکن است سایت ذخیره‌سازی جایگزین را تحت تأثیر قرار دهند، در بررسی‌های مخاطرات سازمانی تعیین می‌شوند. به عنوان مثال‌هایی از این تهدیدات می‌توان به

بلایای طبیعی، شکست‌های ساختاری، حملات سایبری خصمانه، و خطاهای صورت‌گرفته در کنارگذاشتن یا به‌کارگماری کارکنان اشاره کرد. بر اساس نوع تهدیدات، سازمان‌ها تعیین می‌کنند که چه فاصله‌ای باید بین سایت اولیه و سایت جایگزین وجود داشته باشد. در مورد یکی از انواع تهدیداتی که به آن اشاره شد (یعنی حملات سایبری خصمانه)، فاصله بین سایت‌ها اهمیت چندانی ندارد. کنترل مربوطه: RA-3.

(۲) سایت پردازش جایگزین / دسترسی

سازمان، احتمال اخلال و بلایای گسترده را در نظر می‌گیرد و با شناسایی مشکلات بالقوه در زمینه دسترسی به سایت پردازش جایگزین، اقداماتی را برای کاهش خسارت‌ها تعیین می‌کند.

راهنمایی‌های تکمیلی: منظور از اخلال گسترده، اخلالی است که در یک محدوده جغرافیایی گسترده رخ دهد (مانند طوفان، قطع برق گسترده). این انواع اخلال، بر اساس بررسی‌های مخاطرات سازمانی تعیین می‌شوند. کنترل‌های مربوطه: RA-3.

(۳) سایت پردازش جایگزین / اولویت خدمات

سازمان، موافقت‌نامه‌هایی را در زمینه سایت پردازش جایگزین تهیه می‌کند که شامل مفادی در خصوص اولویت خدمات با توجه به الزامات سازمانی دسترسی (شامل اهداف مربوط به زمان بازیابی) هستند.

راهنمایی‌های تکمیلی: موافقت‌نامه‌های مربوط به اولویت خدمات، موافقت‌نامه‌هایی هستند که با تأمین‌کنندگان خدمات امضا می‌شوند تا اطمینان حاصل شود که الزامات رعایت می‌شوند و منابع اطلاعاتی در سایت پردازش جایگزین در اختیار سازمان قرار می‌گیرند.

(۴) سایت پردازش جایگزین / آماده‌سازی برای استفاده

سازمان، سایت پردازش جایگزین را آماده عملیات می‌کند تا بتوان برای پشتیبانی از فرایندهای کسب‌وکار و مأموریت‌های اصلی سازمان از آن استفاده کرد.

راهنمایی‌های تکمیلی: برای آماده‌سازی سایت باید اقداماتی از این قبیل را انجام داد: پیکربندی مؤلفه‌های سیستم اطلاعاتی در سایت پردازش جایگزین بر اساس الزامات پیکربندی سایت اولیه، و حصول اطمینان از این که منابع لازم و سایر ملاحظات تدارکاتی در نظر گرفته شده‌اند. کنترل‌های مربوطه: CM-2, CM-6.

(۵) سایت پردازش جایگزین / تأمین امنیت اطلاعات

[حذف شد: به بخش CP-7 منتقل شد].

(۶) سایت پردازش جایگزین / عدم امکان بازگشت به سایت اولیه

سازمان، خود را برای شرایطی که امکان بازگشت به سایت اولیه وجود نداشته باشد مهیا می‌کند.

مراجع: شماره ویژه NIST 800-34.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	CP-7(1)(2)(3) اولویت متوسط	CP-7(1)(2)(3)(4) اولویت بالا

CP-8: خدمات مخابراتی

کنترل: سازمان، خدمات مخابراتی جایگزین را تدارک می‌بیند و موافقت‌نامه‌های لازم را تهیه می‌کند تا در صورت از دسترس خارج شدن خدمات مخابراتی اولیه در سایت‌های ذخیره‌سازی و پردازش اولیه یا جایگزین، امکان ادامه [اختصاص: عملیات سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] و مأموریت‌ها و فرایندهای کسب‌وکار در [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] وجود داشته باشد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، در مورد خدمات مخابراتی (صوت و داده) برای سایت‌های ذخیره‌سازی و پردازش اولیه و جایگزین مصداق دارد. خدمات مخابراتی جایگزین با توجه به برنامه‌ریزی رویدادهای آینده تدارک دیده می‌شوند. این خدمات بدیمن منظور فراهم می‌آیند که در صورت اخلال در عملکرد خدمات مخابراتی اولیه، بتوان از آن‌ها برای ادامه دادن مأموریت‌ها و فرایندهای اصلی کسب‌وکار استفاده کرد. ممکن است سازمان‌ها بازه‌های زمانی مختلفی را برای سایت‌های اولیه و جایگزین تعیین کنند. خدمات مخابراتی جایگزین مواردی از جمله خطوط مخابراتی زمینی جایگزین یا ارتباطات ماهواره‌ای را در بر می‌گیرند. در هنگام تهیه موافقت‌نامه‌های مربوط به خدمات مخابراتی جایگزین، مواردی از جمله در دسترس بودن، کیفیت خدمات و دسترسی در نظر گرفته می‌شوند. کنترل‌های مربوطه: CP-2, CP-6, CP-7.

کنترل‌های پیشرفته:

(۱) خدمات مخابراتی / مفاد مربوط به اولویت خدمات

سازمان:

(الف) موافقت‌نامه‌هایی را در زمینه خدمات مخابراتی جایگزین تهیه می‌کند که شامل مفادی در خصوص اولویت خدمات با توجه به الزامات سازمانی دسترسی (شامل اهداف مربوط به زمان بازیابی) هستند؛ و

(ب) در صورتی که خدمات مخابراتی اولیه و/یا جایگزین توسط یک تأمین‌کننده مشترک فراهم آمده باشند، درخواست اولویت‌بندی تمام خدمات مخابراتی مورد استفاده در موارد اضطراری مربوط به مسائل امنیت ملی را می‌نماید.

راهنمایی‌های تکمیلی: در صورتی که تأمین‌کنندگان خدمات مخابراتی سازمان، خدماتی را به سازمان‌های دیگر با مفاد اولویت یکسان نیز ارائه می‌کنند، سازمان‌ها بررسی می‌کنند که این امر چه تأثیری بر مأموریت‌ها و فرایندهای کسب‌وکار آن‌ها خواهد داشت.

(۲) خدمات مخابراتی / نقطه شکست[۱۷۶]

سازمان‌ها خدمات مخابراتی جایگزین را در نظر می‌گیرند تا احتمال وجود نقطه شکست مشترک با خدمات مخابراتی اولیه را کاهش دهند.

(۳) خدمات مخابراتی / مجزا بودن تأمین‌کنندگان خدمات مخابراتی اولیه و جایگزین

سازمان‌ها خدمات مخابراتی جایگزین را از تأمین‌کنندگانی مجزا از تأمین‌کنندگان خدمات مخابراتی اولیه دریافت می‌کنند، تا احتمال وجود یک تهدید مشترک بر علیه این دو نوع خدمات کاهش یابد.

راهنمایی‌های تکمیلی: تهدیداتی که ممکن است سایت ذخیره‌سازی جایگزین را تحت تأثیر قرار دهند، در بررسی‌های مخاطرات سازمانی تعیین می‌شوند. به عنوان مثال‌هایی از این تهدیدات می‌توان به بلایای طبیعی، شکست‌های ساختاری، حملات سایبری خصمانه، و خطاهای صورت‌گرفته در کنارگذاشتن یا به‌کارگماری کارکنان اشاره کرد. سازمان‌ها برای کاهش نقاط ضعف و آسیب‌پذیری‌ها، اقداماتی را انجام می‌دهند. به عنوان مثال، زیرساخت‌های مشترک بین تأمین‌کنندگان خدمات مخابراتی را کاهش می‌دهند و فاصله جغرافیایی مناسبی را بین آن‌ها در نظر می‌گیرند. در صورتی که یک تأمین‌کننده واحد بتواند خدمات اولیه و جایگزین را با سطح تفکیک تعیین‌شده در بررسی مخاطرات ارائه نماید، ممکن است سازمان‌ها از یک تأمین‌کننده واحد برای فراهم آوردن خدمات مذکور استفاده کنند.

(۴) خدمات مخابراتی / تهیه طرح آمادگی برای رویدادهای آینده توسط تأمین کنندگان سازمان:

[176] single point of failure

(الف) از تأمین‌کنندگان خدمات مخابراتی اولیه و جایگزین می‌خواهد تا طرح آمادگی برای رویدادهای آینده را تهیه کنند؛

(ب) طرح‌های مذکور را بازبینی می‌کند تا اطمینان حاصل شود که مطابق با الزامات سازمان در زمینه آمادگی برای رویدادهای آینده هستند؛ و

(پ) [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] مدارک مربوط به آموزش و آزمایش طرح‌های آمادگی برای رویدادهای آینده را از تأمین‌کنندگان دریافت می‌کند.

راهنمایی‌های تکمیلی: در فرایند بازبینی طرح‌های آمادگی برای رویدادهای آینده، به این امر توجه می‌شود که طرح‌های مذکور ماهیت مناسبی داشته باشند. در برخی شرایط، ممکن است دریافت خلاصه‌ای از طرح‌های تأمین‌کنندگان نیز برای سازمان کفایت کند. ممکن است تأمین‌کنندگان خدمات مخابراتی، برنامه‌های مستمر بازیابی از بحران را نیز با همکاری سازمان امنیت داخلی، دولت و سازمان‌های دولتی تدارک ببینند. این اقدامات نیز می‌توانند مدرکی برای تأیید طرح‌های تأمین‌کنندگان به شمار آیند.

(۵) خدمات مخابراتی / آزمایش خدمات مخابراتی جایگزین

سازمان، خدمات مخابراتی جایگزین را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] آزمایش می‌کند.

مراجع: شماره ویژه NIST 800-34؛ رهنمود سیستم‌های ارتباطات ملی ۳-۱۰؛ آدرس اینترنتی: http://www.dhs.gov/telecommunications-service-priority-tsp

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	CP-8(1)(2) اولویت متوسط	CP-8(1)(2)(3)(4) اولویت بالا

CP-9: نسخه پشتیبان سیستم اطلاعاتی

کنترل: سازمان:

الف. نسخه‌های پشتیبانی را از اطلاعات کاربری موجود در سیستم‌های اطلاعاتی [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان و با توجه به زمان بازیابی و نقطه بازیابی] تهیه می‌کند؛

ب. نسخه‌های پشتیبانی را از اطلاعات سیستمی موجود در سیستم‌های اطلاعاتی [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان و با توجه به زمان بازیابی و نقطه بازیابی] تهیه می‌کند؛

پ. نسخه‌های پشتیبانی را از اسناد سیستم‌های اطلاعاتی از جمله اسناد امنیتی [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان و با توجه به زمان بازیابی و نقطه بازیابی] تهیه می‌کند؛ و

ت. محرمانگی، یکپارچگی، و موجود بودن اطلاعات پشتیبان را در مکان‌های ذخیره‌سازی تضمین می‌کند.

راهنمایی‌های تکمیلی: اطلاعات سیستمی شامل مواردی از جمله اطلاعات مربوط به وضعیت سیستم، سیستم‌های عامل و نرم‌افزارهای کاربردی، و مجوزها هستند. اطلاعات کاربری، تمامی انواع دیگر اطلاعات متفاوت از اطلاعات سیستمی را در بر می‌گیرند. سازوکارهای مورد استفاده سازمان‌ها برای حفاظت از یکپارچگی نسخه‌های پشتیبان اطلاعات، شامل امضاهای دیجیتال و درهم‌سازهای رمزنگاری هستند. حفاظت از نسخه‌های پشتیبان اطلاعات در حال انتقال، در حیطه شمول این کنترل نیست. برای تهیه نسخه‌های پشتیبان از اطلاعات موجود در سیستم‌های اطلاعاتی، باید به الزامات مذکور در طرح‌های آمادگی برای رویدادهای آینده و سایر الزامات سازمانی مربوط به تهیه نسخه‌های پشتیبان اطلاعات توجه نمود. کنترل‌های مربوطه: CP-2, CP-6, MP-4, MP-5, SC-13.

کنترل‌های پیشرفته:

(۱) نسخه پشتیبان سیستم اطلاعاتی / آزمون یکپارچگی و قابلیت اعتماد

سازمان، نسخه‌های پشتیبان اطلاعات را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] آزمون می‌کند تا یکپارچگی اطلاعات و قابلیت اعتماد رسانه‌ها را تأیید نماید.

راهنمایی‌های تکمیلی: کنترل مربوطه: CP-4.

(۲) نسخه پشتیبان سیستم اطلاعاتی / بازیابی آزمون با استفاده از نمونه‌گیری

سازمان، به عنوان بخشی از فرایند آزمون طرح آمادگی برای رویدادهای آینده، از نمونه‌ای از نسخه پشتیبان اطلاعات در فرایند بازیابی اطلاعات منتخب استفاده می‌کند.

راهنمایی‌های تکمیلی: کنترل مربوطه: CP-4.

(۳) نسخه پشتیبان سیستم اطلاعاتی / حافظه مجزا برای اطلاعات مهم

سازمان، نسخه‌های پشتیبانی از [اختصاص: نرم‌افزارهای مهم سیستم اطلاعاتی و سایر اطلاعات امنیتی تعیین‌شده توسط سازمان] را در یک تأسیسات مجزا و یا در حافظه‌ای ذخیره می‌کند که در مکانی جدا از سیستم اطلاعاتی قرار دارد.

راهنمایی‌های تکمیلی: به عنوان مثالی از نرم‌افزارهای مهم سیستم اطلاعاتی، می‌توان به سیستم‌های عامل، سیستم‌های مدیریت کلید رمزنگاری، و سیستم‌های شناسایی ورود غیرمجاز و جلوگیری از این ورودها اشاره کرد. اطلاعات امنیتی نیز مواردی از جمله موجودی سخت‌افزارها، نرم‌افزارها و ثابت‌افزارهای سازمان را در بر می‌گیرند. سایت‌های ذخیره‌سازی جایگزین معمولاً به عنوان حافظه مجزا توسط سازمان به کار گرفته می‌شوند. کنترل‌های مربوطه: CM-2, CM-8.

(۴) نسخه پشتیبان سیستم اطلاعاتی / حفاظت در برابر تغییرات غیرمجاز

[حذف شد: به بخش CP-9 منتقل شد].

(۵) نسخه پشتیبان سیستم اطلاعاتی / انتقال به سایت ذخیره‌سازی جایگزین

سازمان، نسخه پشتیبان اطلاعات سیستم اطلاعاتی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان و با توجه به زمان بازیابی و نقطه بازیابی] به سایت ذخیره‌سازی جایگزین منتقل می‌کند.

راهنمایی‌های تکمیلی: نسخه پشتیبان اطلاعات سیستم اطلاعاتی را می‌توان به صورت الکترونیکی یا از طریق انتقال فیزیکی رسانه ذخیره‌سازی، به سایت ذخیره‌سازی جایگزین منتقل کرد.

(۶) نسخه پشتیبان سیستم اطلاعاتی / سیستم ثانویه جایگزین

به منظور تهیه نسخه پشتیبان از سیستم اطلاعاتی، سازمان یک سیستم ثانویه را در جایی مجزا از سیستم اولیه ایجاد می‌کند که می‌تواند بدون از دست رفتن اطلاعات یا توقف در عملیات سازمان فعال شود.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: CP-7, CP-10.

(۷) نسخه پشتیبان سیستم اطلاعاتی / نیاز به تأیید مجدد

به منظور پاک کردن یا نابودی [اختصاص: اطلاعات پشتیبان تعیین‌شده توسط سازمان]، سازمان نیاز به تأیید مجدد از سوی کاربران را لازم می‌دارد.

راهنمایی‌های تکمیلی: با تأیید مجدد، اطمینان حاصل می‌شود که بدون تأیید دو نفر از کارکنان مجاز، امکان پاک کردن یا نابودی نسخه‌های پشتیبان اطلاعات وجود نخواهد داشت. افرادی که نسخه‌های پشتیبان اطلاعات را پاک یا نابود می‌کنند، دارای مهارت و تخصص لازم هستند و می‌توانند تشخیص

دهند که آیا این کار مطابق با رویه‌ها و خط‌مشی‌های سازمان هست یا خیر. نیاز به تأیید مجدد گاهی به عنوان کنترل دونفری نیز شناخته می‌شود. کنترل‌های مربوطه: AC-3, MP-2.

مراجع: شماره ویژه NIST 800-34.

اولویت و تخصیص به مجموعه‌های پایه:

P1	CP-9 اولویت پایین	CP-9(1) اولویت متوسط	CP-9(1)(2)(3)(5) اولویت بالا

CP-10: بازسازی[177] و بازیابی[178] سیستم اطلاعاتی

کنترل: سازمان، اقدامات لازم برای بازسازی و بازیابی سیستم اطلاعاتی به حالت عادی پس از اخلال یا شکست در سیستم را انجام می‌دهد.

راهنمایی‌های تکمیلی: بازیابی یعنی انجام فعالیت‌های مورد اشاره در طرح آمادگی برای رویدادهای آینده با هدف ادامه یافتن مأموریت‌ها و فرایندهای کسب‌وکار سازمان. بازسازی پس از بازیابی اتفاق می‌افتد و شامل فعالیت‌هایی است که برای بازگرداندن سیستم اطلاعاتی به حالت عملکرد کامل انجام می‌گیرد. بازسازی و بازیابی بر اساس مأموریت و اولویت‌های کسب‌وکار سازمان، زمان و نقطه بازیابی و اهداف بازسازی، معیارهای سازمان و الزامات مورد اشاره در طرح آمادگی برای رویدادهای آینده انجام می‌شوند. در بازسازی، تمامی قابلیت‌های سیستم اطلاعاتی که در حالت بازیابی مورد نیاز هستند، غیر فعال می‌شوند. در این حالت همچنین قابلیت‌های حالت عملکرد کامل سیستم اطلاعاتی بررسی می‌شوند، فعالیت‌های پایش پیوسته از سر گرفته می‌شوند، موارد لازم مجدداً تأیید می‌شوند، و فعالیت‌هایی صورت می‌گیرند تا سیستم اطلاعاتی برای اخلال‌ها و شکست‌های آینده آماده شود. بازیابی و بازسازی ممکن است به صورت خودکار یا به صورت دستی انجام شوند. کنترل‌های مربوطه: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24.

کنترل‌های پیشرفته:

(۱) بازسازی و بازیابی سیستم اطلاعاتی / آزمایش کردن طرح‌های آمادگی برای رویدادهای آینده
[حذف شد: به بخش CP-4 منتقل شد].

[177] reconstitution
[178] recovery

(۲) بازسازی و بازیابی سیستم اطلاعاتی / بازیابی تراکنش

سیستم اطلاعاتی، فرایند بازیابی تراکنش را در مورد سیستم‌های مبتنی بر تراکنش انجام می‌دهد.

راهنمایی‌های تکمیلی: سیستم‌های اطلاعاتی مبتنی بر تراکنش شامل سیستم‌های مدیریت پایگاه‌های داده، سیستم‌های پردازش تراکنش و موارد دیگری از این دست هستند. سازوکارهای پشتیبانی از بازیابی تراکنش نیز مواردی از جمله سازوکارهای ثبت تراکنش و سازوکارهای بازگشت به حالت اولیه را در بر می‌گیرند.

(۳) بازسازی و بازیابی سیستم اطلاعاتی / کنترل‌های امنیتی جبرانی

[حذف شد: این مورد در بخش مربوط به رویه‌های اختصاصی تشریح شده است].

(۴) بازسازی و بازیابی سیستم اطلاعاتی / بازیابی در بازه زمانی مشخص

سازمان، امکان بازیابی مؤلفه‌ای سیستم اطلاعاتی را [اختصاص: در بازه زمانی تعیین‌شده توسط سازمان] فراهم می‌آورد تا پیکربندی و یکپارچگی اطلاعات حفظ شوند و مؤلفه‌های مذکور به حالت عملکرد عادی و شناخته‌شده خود بازگردند.

راهنمایی‌های تکمیلی: بازیابی مؤلفه‌های سیستم اطلاعاتی شامل تعیین اقداماتی است که مؤلفه‌ها را به حالت عملکرد عادی و شناخته‌شده خود بازمی‌گردانند. کنترل مربوطه: CM-2.

(۵) بازسازی و بازیابی سیستم اطلاعاتی / قابلیت انتقال به سیستم جایگزین

[حذف شد: به بخش SI-13 منتقل شد].

(۶) بازسازی و بازیابی سیستم اطلاعاتی / حفاظت از مؤلفه‌ها

سازمان، از نرم‌افزارها، سخت‌افزارها و ثابت‌افزارهای بازیابی و پشتیبان محافظت می‌نماید.

راهنمایی‌های تکمیلی: حفاظت از نرم‌افزارها، سخت‌افزارها و ثابت‌افزارهای بازیابی و پشتیبان می‌تواند از طریق روش‌های فنی یا فیزیکی صورت گیرد. نرم‌افزارهای بازیابی و پشتیبان شامل جداول مسیریابی، کامپایلرها، و سایر نرم‌افزارهای امنیتی سیستم هستند. کنترل‌های مربوطه: AC-3, AC-6, PE-3.

مراجع: رهنمود شماره اول استمرار عملیات فدرال؛ شماره ویژه NIST 800-34.

اولویت و تخصیص به مجموعه‌های پایه:

P1	CP-10 اولویت پایین	CP-10(2) اولویت متوسط	CP-10(2)(4) اولویت بالا

CP-11: پروتکل‌های ارتباطی جایگزین

کنترل: سیستم اطلاعاتی، امکان استفاده از [اختصاص: پروتکل‌های ارتباطی جایگزین تعیین‌شده توسط سازمان] را برای پشتیبانی از استمرار عملیات فراهم می‌آورد.

راهنمایی‌های تکمیلی: طرح‌های آمادگی برای رویدادهای آینده و آزمایش‌ها و آموزش‌های مربوط به آن‌ها، در مجموع یک پروتکل ارتباطی جایگزین را تشکیل می‌دهند که قابلیت انعطاف سیستم اطلاعات سازمان را افزایش می‌دهد. پروتکل‌های ارتباطی جایگزین شامل مواردی از جمله انتقال از نسخه چهارم پروتکل TCP/IP به نسخه ششم این پروتکل هستند. انتقال از یک پروتکل ارتباطی به یک پروتکل دیگر می‌تواند بر برنامه‌های کاربردی تأثیر بگذارد. در نتیجه، پیش از انجام این کار معمولاً تحلیل‌هایی در زمینه این پروتکل‌های ارتباطی جایگرین صورت می‌گیرند.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

CP-12: **حالت امن**

کنترل: در صورت رخ دادن [اختصاص: شرایط تعیین‌شده توسط سازمان]، سیستم اطلاعاتی حالت امن عملیات را با [اختصاص: محدودیت‌های تعیین‌شده توسط سازمان در زمینه حالت امن عملیات] را فعال می‌کند.

راهنمایی‌های تکمیلی: در مورد آن دسته از سیستم‌های اطلاعاتی که از مأموریت‌ها و فرایندهای اصلی کسب‌وکار مانند عملیات نظامی و سیستم‌های تسلیحاتی، عملیات نیروگاه‌های هسته‌ای، و عملیات کنترل ترافیک هوایی (به ویژه محیط‌های عملیاتی بلادرنگ) پشتیبانی می‌کنند، ممکن است سازمان‌ها شرایطی را در نظر گیرند که در صورت رخ دادن آن‌ها، سیستم به یک حالت امن از پیش تعریف‌شده بازگردد. حالت امن عملیات، که می‌توان آن را به صورت خودکار یا دستی فعال کرد، نوع فعالیت‌های قابل انجام توسط سیستم‌های اطلاعاتی در شرایط مشخص‌شده را محدود می‌کند. به عنوان مثال، تنها مجموعه محدودی از عملیات در شرایط توان مصرفی کم و پهنای باند پایین قابل انجام هستند.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

CP-13: سازوکارهای امنیتی جایگزین

کنترل: در صورتی که ابزارهای امنیتی اولیه در دسترس نباشند یا در معرض خطر قرار گرفته باشند، سازمان [اختصاص: سازوکارهای امنیتی تکمیلی یا جایگزین تعیین‌شده توسط سازمان] را به کار می‌گیرد تا [اختصاص: عملکردهای امنیتی تعیین‌شده توسط سازمان] را انجام دهند.

راهنمایی‌های تکمیلی: این کنترل سبب افزایش قابلیت انعطاف و همچنین برنامه‌ریزی بهتر جهت آمادگی برای رویدادهای آینده و استمرار عملیات سازمان می‌شود. سازمان‌ها می‌توانند برای حصول اطمینان از استمرار مأموریت‌ها و فرایندهای کسب‌وکار خود، از سازوکارهای امنیتی تکمیلی یا جایگزین استفاده کنند. ممکن است این سازوکارها نسبت به سازوکارهای اولیه اثربخشی کمتری داشته باشند (مثلاً استفاده از آن‌ها دشوارتر باشد، مقیاس‌پذیر نباشند، یا امنیت کمتری داشته باشند). با این حال، قابلیت به کار گیری این سازوکارها می‌تواند سبب جلوگیری از ایجاد وقفه در عملیات سازمان و استمرار مأموریت‌ها و فرایندهای کسب‌وکار شود. با توجه به هزینه و منابع مورد نیاز برای فراهم آوردن این قابلیت‌های تکمیلی و جایگزین، این کنترل تنها در مورد قابلیت‌های امنیتی مهم ارائه‌شده توسط سیستم‌های اطلاعاتی، مؤلفه‌های این سیستم‌ها، یا خدمات این سیستم‌ها به کار گرفته می‌شود. کنترل مربوطه: CP-2.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

خانواده: شناسایی و احراز هویت

IA-1: خط‌مشی و رویه‌های شناسایی و احراز هویت

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۱۱. خط‌مشی شناسایی و احراز هویت شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و
۱۲. رویه‌های تسهیل پیاده‌سازی خط‌مشی شناسایی و احراز هویت و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۱۱. خط‌مشی شناسایی و احراز هویت؛ و
۱۲. رویه‌های شناسایی و احراز هویت.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده IA را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور همچنین می‌تواند مجموعه‌ای از خط‌مشی‌های مختلف باشد که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص تهیه نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در تدوین این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: FIPS 201؛ شماره‌های ویژه NIST 800-12, 800-800-63, 800-73, 800-76, 800-78, 800-100.

اولویت و تخصیص به مجموعه‌های پایه:

P1	IA-1 اولویت پایین	IA-1 اولویت متوسط	IA-1 اولویت بالا

IA-2: شناسایی و احراز هویت (کاربران سازمانی)

کنترل: سیستم اطلاعاتی، کاربران سازمانی (یا فرایندهایی که از سوی آن‌ها اجرا می‌شوند) را به صورت منحصر به فرد شناسایی و احراز هویت می‌کند.

راهنمایی‌های تکمیلی: کاربران سازمانی شامل کارکنان و سایر افرادی هستند که از دید سازمان، موقعیتی مشابه کارکنان دارند (مانند پیمانکاران و پژوهشگران مهمان). این کنترل در مورد تمام دسترسی‌ها به جز موارد روبرو اعمال می‌شود: (الف) دسترسی‌هایی که به طور آشکار در AC-14 تعیین و مستندسازی شده‌اند؛ و (ب) دسترسی‌هایی که از طریق استفاده مجاز از ابزارهای احراز هویت گروهی و بدون استفاده از احراز هویت فردی حاصل می‌شوند. سازمان‌ها ممکن است از کاربران حساب‌های گروهی بخواهند که هر یک به صورت مجزا احراز هویت شوند. این الزام ممکن است برای پاسخگویی هر یک از افراد در قبال فعالیت‌های خود باشد. سازمان‌ها برای احراز هویت کاربران از گذرواژه‌ها، ژتون[۱۷۹]، یا داده‌های بیومتریک استفاده می‌کنند. در برخی موارد نیز از چند روش مختلف احراز هویت به صورت ترکیبی استفاده می‌شود. دسترسی به سیستم‌های اطلاعاتی سازمانی، به صورت دسترسی محلی یا دسترسی شبکه صورت می‌گیرد. دسترسی محلی عبات است از هر گونه دسترسی به سیستم‌های اطلاعاتی سازمانی توسط کاربران (یا فرایندهایی که از سوی آن‌ها اجرا می‌شوند)، از طریق اتصال مستقیم و بدون استفاده از شبکه. دسترسی شبکه عبارت است از دسترسی به سیستم‌های اطلاعاتی سازمانی توسط کاربران (یا فرایندهایی که از سوی آن‌ها اجرا می‌شوند)، از طریق اتصال شبکه (یعنی دسترسی غیر محلی). دسترسی از راه دور نوعی از دسترسی شبکه است که ارتباطات آن از طریق شبکه‌های خارجی (مانند اینترنت) صورت می‌گیرد. شبکه‌های اینترنتی به دو دسته شبکه‌های محلی و شبکه‌های گسترده تقسیم می‌شوند. علاوه بر این، استفاده از شبکه‌های خصوصی مجازی (VPN) رمزگذاری‌شده برای برقراری اتصال شبکه بین نقاط پایانی تحت کنترل سازمان و سایر نقاط پایانی، می‌تواند نوعی شبکه داخلی به وجود آورد که از محرمانگی و یکپارچگی اطلاعات منتقل‌شده در شبکه محافظت می‌کند.

[179] token

سازمان‌ها می‌توانند برای حصول اطمینان از رعایت الزامات مربوط به شناسایی و احراز هویت، از الزاماتی که در رهنمود شماره ۱۲ ریاست جمهوری در زمینه امنیت داخلی تبعیت کنند. این الزامات، مطابق با طرح‌های اجرایی سازمانی هستند. احراز هویت چندعاملی[۱۸۰] نیازمند استفاده از چند عامل مختلف برای احراز هویت است. این عوامل عبارتند از: (لف) چیزی که می‌دانید (مانند گذرواژه یا شماره شناسایی شخصی (PIN))؛ (ب) چیزی که در اختیار دارید (مانند دستگاه شناسایی رمزنگاری یا ژتون)؛ یا (پ) چیزی که هستید، یا به عبارت دیگر، چیزی که نشان‌دهنده هویت شما است (مانند اطلاعات بیومتریک). به عنوان مثالی از روش‌های چندعاملی که نیازمند دستگاه‌های جداگانه هستند، می‌توان به این موارد اشاره کرد: ژتون‌های سخت‌افزاری که ابزارهای احراز هویت را ارائه می‌کنند، یا کارت‌های هوشمندی مانند کارت تأیید هویت فردی دولت امریکا و کارت‌های DoD معمولی. علاوه بر شناسایی و احراز هویت کاربران در سطح سیستم اطلاعاتی (مثلا در هنگام ورود به سیستم)، سازمان‌ها در صورت لزوم در سطح برنامه کاربردی نیز از سازوکارهایی برای شناسایی و احراز هویت استفاده می‌کنند، تا امنیت اطلاعات را افزایش دهند. الزامات شناسایی و احراز هویت برای موجودیت‌های به جز کاربران سازمانی، در IA-8 تشریح شده‌اند. کنترل‌های مربوطه: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.

کنترل‌های پیشرفته:

(۱) شناسایی و احراز هویت / دسترسی شبکه به حساب‌های دارای امتیاز ویژه

سیستم اطلاعاتی، از احراز هویت چندعاملی برای دسترسی شبکه به حساب‌های دارای امتیاز ویژه استفاده می‌کند.

راهنمایی‌های تکمیلی: کنترل مربوطه: AC-6.

(۲) شناسایی و احراز هویت / دسترسی شبکه به حساب‌هایی که امتیاز ویژه ندارند

سیستم اطلاعاتی، از احراز هویت چندعاملی برای دسترسی شبکه به حساب‌هایی که امتیاز ویژه ندارند استفاده می‌کند.

(۳) شناسایی و احراز هویت / دسترسی محلی به حساب‌های دارای امتیاز ویژه

سیستم اطلاعاتی، از احراز هویت چندعاملی برای دسترسی محلی به حساب‌های دارای امتیاز ویژه استفاده می‌کند.

راهنمایی‌های تکمیلی: کنترل مربوطه: AC-6.

(۴) شناسایی و احراز هویت / دسترسی شبکه به حساب‌هایی که امتیاز ویژه ندارند

[180] multifactor authentication

سیستم اطلاعاتی، از احراز هویت چندعاملی برای دسترسی محلی به حساب‌هایی که امتیاز ویژه ندارند استفاده می‌کند.

(۵) شناسایی و احراز هویت / احراز هویت گروهی

هنگامی که یک ابزار احراز هویت گروهی به کار گرفته می‌شود، سیستم اطلاعاتی از تک تک کاربران می‌خواهد که با استفاده از ابزارهای احراز هویت فردی خود احراز هویت نمایند.

راهنمایی‌های تکمیلی: ملزم کردن افراد به استفاده از ابزارهای احراز هویت فردی به عنوان سطح دوم احراز هویت، سازمان را قادر می‌سازد تا مخاطره استفاده از ابزارهای احراز هویت گروهی را کاهش دهد.

(۶) شناسایی و احراز هویت / دسترسی شبکه به حساب‌های دارای امتیاز ویژه – دستگاه‌های مجزا

سیستم اطلاعاتی، از احراز هویت چندعاملی برای دسترسی شبکه به حساب‌های دارای امتیاز ویژه استفاده می‌کند، به گونه‌ای که یکی از عوامل توسط یک دستگاه مجزا از سیستم ارائه می‌شود و این دستگاه از [اختصاص: الزامات سازوکار تعیین‌شده توسط سازمان] پیروی می‌کند.

راهنمایی‌های تکمیلی: کنترل مربوطه: AC-6.

(۷) شناسایی و احراز هویت / دسترسی شبکه به حساب‌هایی که امتیاز ویژه ندارند – دستگاه‌های مجزا

سیستم اطلاعاتی، از احراز هویت چندعاملی برای دسترسی شبکه به حساب‌هایی که امتیاز ویژه ندارند استفاده می‌کند، به گونه‌ای که یکی از عوامل توسط یک دستگاه مجزا از سیستم ارائه می‌شود و این دستگاه از [اختصاص: الزامات سازوکار تعیین‌شده توسط سازمان] پیروی می‌کند.

(۸) شناسایی و احراز هویت / دسترسی شبکه به حساب‌های دارای امتیاز ویژه – مقاومت در برابر حملات بازپخش[۱۸۱]

سیستم اطلاعاتی، از سازوکار احراز هویت مقاوم در برابر حملات بازپخش برای دسترسی شبکه به حساب‌های دارای امتیاز ویژه استفاده می‌کند.

راهنمایی‌های تکمیلی: فرایندهای احراز هویت مقاوم در برابر حملات بازپخش به گونه‌ای طراحی شده‌اند که از احراز هویت موفق با استفاده از روش بازپخش پیام‌های احراز هویت جلوگیری به عمل می‌آورند. روش‌های مقاومت در برابر حملات بازپخش شامل چنین مواردی هستند: پروتکل‌هایی که از نانس‌ها[۱۸۲] یا چالش‌ها استفاده می‌کنند، مانند امنیت لایه انتقال (TLS)، و همچنین ابزارهای احراز هویت یک بار مصرف یا چالش‌محور دارای تقارن زمانی.

---

[181] replay-resistance

[182] nonce

(۹) شناسایی و احراز هویت / دسترسی شبکه به حساب‌هایی که امتیاز ویژه ندارند – مقاومت در برابر حملات بازپخش

سیستم اطلاعاتی، از سازوکار احراز هویت مقاوم در برابر حملات بازپخش برای دسترسی شبکه به حساب‌هایی که امتیاز ویژه ندارند استفاده می‌کند.

راهنمایی‌های تکمیلی: فرایندهای احراز هویت مقاوم در برابر حملات بازپخش به گونه‌ای طراحی شده‌اند که از احراز هویت موفق با استفاده از روش بازپخش پیام‌های احراز هویت جلوگیری به عمل می‌آورند. روش‌های مقاومت در برابر حملات بازپخش شامل چنین مواردی هستند: پروتکل‌هایی که از نانس‌ها[۱۸۳] یا چالش‌ها استفاده می‌کنند، مانند امنیت لایه انتقال (TLS)، و همچنین ابزارهای احراز هویت یک بار مصرف یا چالش‌محور دارای تقارن زمانی.

(۱۰) شناسایی و احراز هویت / یک‌بار ورود[۱۸۴]

سیستم اطلاعاتی، قابلیت یک‌بار ورود را برای [اختصاص: خدمات و حساب‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] فراهم می‌آورد.

راهنمایی‌های تکمیلی: امکان یک‌بار ورود، کاربران را قادر می‌سازد تا یک بار وارد سیستم شوند و به چند منبع سیستم اطلاعاتی دسترسی پیدا کنند. البته سازمان‌ها در کنار بهره بردن از کارایی این روش، به این نکته نیز توجه دارند که روش مذکور مخاطراتی را برای آن‌ها به همراه دارد. با استفاده از این روش، در صورتی که یک ابزار احراز هویت به سرقت برود، فرد مهاجم می‌تواند به طور همزمان به چند منبع دسترسی پیدا نماید.

(۱۱) شناسایی و احراز هویت / دسترسی از راه دور – دستگاه‌های مجزا

سیستم اطلاعاتی، از احراز هویت چندعاملی برای دسترسی از راه دور به حساب‌های دارای امتیاز ویژه و حساب‌هایی که امتیاز ویژه ندارند استفاده می‌کند، به گونه‌ای که یکی از عوامل توسط یک دستگاه مجزا از سیستم ارائه می‌شود و این دستگاه از [اختصاص: الزامات سازوکار تعیین‌شده توسط سازمان] پیروی می‌کند.

راهنمایی‌های تکمیلی: ارائه یکی از عوامل احراز هویت توسط دستگاه مجزا به منظور دسترسی از راه دور به حساب‌های دارای امتیاز ویژه و حساب‌هایی که امتیاز ویژه ندارند، برای کاهش احتمال به خطر افتادن اطلاعات احراز هویت ذخیره‌شده روی سیستم است. در غیر این صورت، مهاجمانی که از کدهای

---

183 nonce

184 single sign-on

مخرب در سیستم اطلاعاتی سازمان استفاده می‌کنند، می‌توانند به اطلاعات احراز هویت سیستم دست یابند و خود را به جای کاربران مجاز جا بزنند. کنترل مربوطه: AC-6.

(۱۲) شناسایی و احراز هویت / پذیرفتن اطلاعات تأیید هویت فردی (PIV)

راهنمایی‌های تکمیلی: این کنترل پیشرفته در مورد سازمان‌هایی اعمال می‌شود که از سیستم‌های کنترل دسترسی منطقی (LACS) و سیستم‌های کنترل دسترسی فیزیکی (PACS) استفاده می‌کنند. اطلاعات تأیید هویت فردی (PIV)، توسط ادارات فدرالی صادر می‌شوند که FIPS 201 و اسناد راهنمای مربوطه را تأیید می‌کنند. تفاهم‌نامه OMB 11-11 ادارات فدرال را ملزم می‌کند که الزامات تعیین‌شده در HSPD-12 را به کار گیرند و از اطلاعات تأیید هویت فردی استفاده نمایند. کنترل‌های مربوطه: AU-2, PE-3, SA-4.

(۱۳) شناسایی و احراز هویت / احراز هویت دومسیری[۱۸۵]

سیستم اطلاعاتی در [اختصاص: شرایط تعیین‌شده توسط سازمان] از [اختصاص: احراز هویت دومسیری تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: احراز هویت دومسیری (OOBA) یعنی استفاده از دو مسیر ارتباطی مجزا برای شناسایی و احراز هویت کاربران در یک سیستم اطلاعاتی. مسیر اول (یعنی مسیر داخلی[۱۸۶]) برای شناسایی و احراز هویت کاربران و دستگاه‌ها به کار می‌رود و معمولا اطلاعات از طریق آن جریان می‌یابند. مسیر دوم (یعنی مسیر خارجی[۱۸۷]) برای تأیید مستقل هویت و/یا انجام اقدامات درخواست‌شده مورد استفاده قرار می‌گیرد. به عنوان مثال، یک کاربر از طریق کامپیوتر نوت‌بوک خود در یک سرور راه دور احراز هویت می‌کند، و درخواست انجام اقداماتی را توسط سرور و از طریق مسیر ارتباطی می‌نماید. در ادامه، سرور از طریق گوشی کاربر با وی ارتباط برقرار می‌کند تا تأیید شود که درخواست از طرف وی صادر شده است. کاربر می‌تواند اقدام را تأیید کند یا کد احراز هویت را ارائه نماید. سازمان‌ها می‌توانند با استفاده از این روش احراز هویت، خطر حملات کسی در میانه را کاهش دهند. شرایطی نیز برای فعال‌سازی این سازوکار در نظر گرفته می‌شود که به عنوان نمونه می‌توان به فعالیت‌های مشکوک، مشاهده شاخص جدید تهدید یا بالا رفتن سطح تهدید، یا سطح تأثیر یا سطح دسته‌بندی اطلاعات در تراکنش درخواستی اشاره کرد. کنترل‌های مربوطه: IA-10, IA-11, SC-37.

---

[185] out-of-band authentication
[186] in-band path
[187] out-of-band path

مراجع: HSPD-12؛ تفاهم‌نامه 11-11 ,06-16 ,04-04 OMB؛ FIPS 201؛ شماره‌های ویژه NIST 800-63, 800-78 ,800-76 ,800-73؛ نقشه راه و راهنمای پیاده‌سازی FICAM؛ آدرس اینترنتی http://idmanagement.gov

اولویت و تخصیص به مجموعه‌های پایه:

P1	IA-2(1)(12) اولویت پایین	IA-2(1)(2)(3)(8)(11)(12) اولویت متوسط	IA-2(1)(2)(3)(4)(8)(9)(11)(12) اولویت بالا

IA-3: شناسایی و احراز هویت دستگاه

کنترل: سیستم اطلاعاتی، [اختصاص: ویژگی‌ها و/یا انواع دستگاه‌های تعیین‌شده توسط سازمان] را پیش از ایجاد یک اتصال [انتخاب (یک یا چند مورد): محلی، راه دور، شبکه]، به صورت منحصر به فرد شناسایی و احراز هویت می‌نماید.

راهنمایی‌های تکمیلی: دستگاه‌های سازمان که باید شناسایی و احراز هویت شوند، بر اساس نوع، دستگاه، یا ترکیبی از نوع و دستگاه دسته‌بندی می‌شوند. سیستم‌های اطلاعاتی معمولا از اطلاعات معلوم اشتراک‌گذاری‌شده (مانند کنترل دسترسی به رسانه‌ها (MAC) یا آدرس‌های TCP/IP) برای شناسایی و احراز هویت دستگاه‌ها استفاده می‌کنند یا روش‌های احراز هویت سازمانی (مانند IEEE 802.1x و پروتکل احراز هویت بسط‌پذیر (EAP) و احراز هویت سرور Radius با امنیت لایه انتقال (TLS)) را برای شناسایی و احراز هویت دستگاه‌ها در شبکه‌های محلی یا گسترده مورد استفاده قرار می‌دهند. سازمان‌ها، قدرت مورد نیاز سازوکاهای احراز هویت را بر اساس دسته‌بندی امنیتی سیستم‌های اطلاعاتی تعیین می‌کنند. به دلیل چالش‌های به‌کارگیری گسترده این کنترل در ابعاد وسیع، از سازمان‌ها درخواست می‌شود که کنترل حاضر را تنها در مورد دستگاه‌هایی اعمال کنند که واقعا نیازمند داشتن این قابلیت هستند. کنترل‌های مربوطه: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.

کنترل‌های پیشرفته:

(۱) شناسایی و احراز هویت دستگاه / احراز هویت دوسویه مبتنی بر رمزنگاری

سیستم اطلاعاتی، [اختصاص: ویژگی‌ها و/یا انواع دستگاه‌های تعیین‌شده توسط سازمان] را پیش از ایجاد یک اتصال [انتخاب (یک یا چند مورد): محلی، راه دور، شبکه]، با استفاده از روش دوسویه مبتنی بر رمزنگاری، احراز هویت می‌نماید.

راهنمایی‌های تکمیلی: اتصال محلی، اتصالی است که بدون استفاده از شبکه با دستگاه برقرار می‌شود. اتصال شبکه، اتصالی است که از طریق شبکه با دستگاه برقرار می‌شود (مانند شبکه محلی، شبکه گسترده، یا اینترنت). اتصال از راه دور، اتصالی است که از طریق یک شبکه خارجی با دستگاه برقرار می‌شود (مانند اینترنت). احراز هویت دوسویه، شاخص‌های امنیتی قدرتمندتری را برای شناسایی دستگاه‌ها در اتصالات دارای مخاطره بیشتر (مانند اتصالات از راه دور) فراهم می‌آورد. کنترل‌های مربوطه: SC-8, SC-12, SC-13.

(۲) شناسایی و احراز هویت دستگاه / احراز هویت دوسویه شبکه مبتنی بر رمزنگاری

[حذف شد: به بخش IA-3(1) منتقل شد].

(۳) شناسایی و احراز هویت دستگاه / تخصیص آدرس پویا[۱۸۸]

سازمان:

(الف) اطلاعات اجازه و مدت زمان اجاره مربوط به تخصیص آدرس پویا را بر اساس [اختصاص: اطلاعات اجازه و زمان اجاره تعیین‌شده توسط سازمان]، استانداردسازی می‌کند؛ و

(ب) اطلاعات اجاره اختصاص داده شده به دستگاه را ممیزی می‌کند.

راهنمایی‌های تکمیلی: به عنوان نمونه‌ای از فرایند تخصیص آدرس پویا، می‌توان به کلاینت‌هایی با DHCP فعال اشاره کرد که آدرس IP خود را از سرورهای DHCP اجاره می‌کنند. کنترل‌های مربوطه: AU-2, AU-3, AU-6, AU-12.

(۴) شناسایی و احراز هویت دستگاه / تصدیق دستگاه

سازمان اطمینان حاصل می‌نماید که شناسایی و احراز هویت دستگاه بر اساس تصدیق دریافت‌شده از [اختصاص: فرایند مدیریت پیکربندی تعیین‌شده توسط سازمان] انجام می‌شود.

راهنمایی‌های تکمیلی: تصدیق دستگاه یعنی شناسایی و احراز هویت دستگاه بر اساس پیکربندی و وضعیت عملیاتی آن. تصدیق دستگاه را می‌توان از طرق برخی درهم‌سازهای رمزنگاری دستگاه انجام داد. اگر تصدیق دستگاه ابزاری برای شناسایی و احراز هویت دستگاه باشد، تعمیر و به‌روزرسانی دستگاه

[188] dynamic address allocation

باید از طریق فرایند مدیریت پیکربندی مقتضی انجام شود، به نحوی که تعمیر و به‌روزرسانی به صورت امن انجام گیرد و اخلالی در شناسایی و احراز هویت سایر دستگاه‌ها پدید نیاورد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	IA-3 اولویت متوسط	IA-3 اولویت بالا

IA-4: مدیریت شناسه[۱۸۹]

کنترل: سازمان، به روش‌های زیر اقدام به مدیریت شناسه‌های سیستم اطلاعاتی می‌کند:

الف. دریافت فرم احراز هویت از [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] برای تخصیص یک شناسه به دستگاه، نقش، گروه یا فرد؛

ب. انتخاب شناسه‌ای که یک فرد، گروه، نقش یا دستگاه را شناسایی کند؛

پ. تخصیص شناسه به دستگاه، نقش، گروه یا فرد؛

ت. جلوگیری از استفاده مجدد از شناسه‌ها در [اختصاص: مدت زمان تعیین‌شده توسط سازمان]؛ و

ث. غیر فعال کردن شناسه پس از [اختصاص: مدت زمان عدم فعالیت تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: به عنوان نمونه‌هایی از شناسه‌های معمول دستگاه، می‌توان به کنترل دسترسی به رسانه (MAC)، آدرس پروتکل اینترنتی (IP)، یا شناسه‌های ژتون منحصر به فرد دستگاه اشاره کرد. روش‌های مدیریت شناسه‌های فردی را نمی‌توان برای حساب‌های اشتراک‌گذاری‌شده سیستم اطلاعاتی (مانند حساب‌های مهمان یا ناشناس) مورد استفاده قرار داد. شناسه‌های افراد، معمولا نام کاربری حساب‌های سیستم‌های اطلاعاتی هستند که به آن‌ها تخصیص داده شده‌اند. در چنین مواردی، برای مدیریت حساب‌های AC-2 از نام‌های کاربری ارائه‌شده توسط IA-4 استفاده می‌شود. کنترل حاضر در مورد آن دسته از شناسه‌های فردی که الزاما مربوط به حساب‌های سیستم اطلاعاتی نیستند نیز اعمال می‌شود (مانند شناسه‌های مورد استفاده در پایگاه‌های داده

[189] identifier

کنترل امنیت فیزیکی که توسط سیستم‌های علامت‌خوان[۱۹۰] برای دسترسی به سیستم‌های اطلاعاتی مورد استفاده قرار می‌گیرند). منع استفاده مجدد از شناسه‌ها بدین معنی است که نمی‌توان شناسه‌های پیشر استفاده شده افراد، گروه‌ها، نقش‌ها یا دستگاه‌ها را برای افراد، گروه‌ها، نقش‌ها یا دستگاه‌های دیگر مورد استفاده قرار داد. کنترل‌های مربوطه: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

کنترل‌های پیشرفته:

(۱) مدیریت شناسه / منع استفاده از شناسه‌های حساب‌ها به عنوان شناسه‌های عمومی

سازمان، استفاده از شناسه‌های حساب‌های سیستم اطلاعاتی که مشابه شناسه‌های عمومی ایمیل‌های افراد هستند را ممنوع می‌کند.

راهنمایی‌های تکمیلی: منع استفاده از شناسه‌های حساب‌ها به عنوان شناسه‌های عمومی (مانند شناسه‌های ایمیل‌های افراد)، سبب می‌شود که حدس زدن شناسه‌ها برای مهاجمان دشوارتر شود. کنترل مربوطه: AT-2.

(۲) مدیریت شناسه / صدور مجوز نظارت

سازمان ملزم می‌دارد که یک شناسه فردی شامل مجوز نظارت، در فرایند ثبت دریافت شود.

(۳) مدیریت شناسه / استفاده از چند نوع گواهی‌نامه

سازمان ملزم می‌دارد که چند نوع گواهی‌نامه برای شناسایی افراد، به مسئول ثبت ارائه شود.

راهنمایی‌های تکمیلی: ارائه چند نوع گواهی‌نامه هویتی (مانند مدارک مختلف یا ترکیبی از اسناد و اطلاعات بیومتریک)، سبب می‌شود که احتمال استفاده از شناسه‌های هویتی جعلی از سوی مهاجمان کمتر شود یا این که مهاجمان حداقل نیاز به سعی و تلاش بیشتری برای دستیابی به این شناسه‌ها داشته باشند.

(۴) مدیریت شناسه / شناسه‌های وضعیت کاربر

سازمان، هر یک از افراد را به صورت منحصر به فرد و بر اساس [اختصاص: ویژگی‌های فردی تعیین‌شده توسط سازمان] شناسایی می‌کند و بدین ترتیب، شناسه‌های فردی را مدیریت می‌نماید.

راهنمایی‌های تکمیلی: به عنوان مثال، پیمانکار یا شهروند یک کشور دیگر، ویژگی‌هایی هستند که وضعیت افراد را نشان می‌دهند. استفاده از شناسه‌های تعیین وضعیت افراد، اطلاعات بیشتری را درباره افرادی که کارکنان سازمان با آن‌ها در ارتباط هستند، ارائه می‌کند. به عنوان مثال، یک کارمند دولتی

[190] badge reader system

متوجه خواهد شد که یکی از افرادی که از طریق ایمیل با وی در ارتباط بوده، یک پیمانکار است. کنترل مربوطه: AT-2.

(۵) مدیریت شناسه / مدیریت پویا

سیستم اطلاعاتی، شناسه‌ها را به صورت پویا مدیریت می‌کند.

راهنمایی‌های تکمیلی: بر خلاف روش‌های مرسوم شناسایی که حساب‌های کاربران در آن‌ها استاتیک یا ایستا در نظر گرفته می‌شوند، بسیاری از سیستم‌های اطلاعاتی توزیع‌شده (مانند معماری‌های خدمت‌محور)، برای موجودیت‌هایی که پیشتر شناخته‌شده نبوده‌اند، در زمان اجرا شناسه‌هایی را تولید می‌کنند. در این شرایط، سازمان‌ها خود را برای ایجاد شناسه‌ها به صورت دینامیک آماده می‌نمایند. برای استفاده از چنین فرایندی، لازم است که سازوکارها و روابط مورد اعتمادی با مسئولین مربوطه برقرار شود تا بتوان شناسه‌ها و اطلاعات آن‌ها را تأیید کرد. کنترل مربوطه: AC-16.

(۶) مدیریت شناسه / مدیریت بین‌سازمانی شناسه‌ها

سازمان، هماهنگی‌های لازم برای مدیریت بین‌سازمانی شناسه‌ها را با [اختصاص: سازمان‌های خارجی تعیین‌شده توسط سازمان] انجام می‌دهد.

راهنمایی‌های تکمیلی: مدیریت بین‌سازمانی شناسه‌ها این قابلیت را در اختیار سازمان‌ها قرار می‌دهد تا افراد، گروه‌ها، نقش‌ها و سازمان‌ها را در فعالیت‌های بین‌سازمانی مانند پردازش، ذخیره‌سازی و انتقال اطلاعات، به خوبی شناسایی نمایند.

(۷) مدیریت شناسه / ثبت نام حضوری

سازمان، افراد را ملزم می‌دارد که به صورت حضوری به مسئول ثبت نام مراجعه کنند و پس از انجام ثبت نام، شناسه فردی خود را دریافت نمایند.

راهنمایی‌های تکمیلی: ثبت نام حضوری، امکان صدور شناسه‌های متقلبانه را کاهش می‌دهد، زیرا در این فرایند لازم است که افراد به صورت حضوری به مسئول ثبت نام مراجعه کنند و پس از انجام ثبت نام، شناسه فردی خود را دریافت نمایند.

مراجع: FIPS 201؛ شماره‌های ویژه NIST 800-73, 800-76, 800-78.

اولویت و تخصیص به مجموعه‌های پایه:

P1	IA-4 اولویت پایین	IA-4 اولویت متوسط	IA-4 اولویت بالا

IA-5: مدیریت ابزارهای احراز هویت

کنترل: سازمان، ابزارهای احراز هویت را با استفاده از روش‌های زیر مدیریت می‌کند:

الف. تأیید هویت فرد، گروه، نقش یا دستگاه دریافت‌کننده ابزار احراز هویت، به عنوان بخشی از فرایند اولیه توزیع ابزارهای احراز هویت؛

ب. ایجاد محتوای احراز هویت اولیه برای ابزارهای احراز هویت تعیین‌شده توسط سازمان؛

پ. حصول اطمینان از این که ابزارهای احراز هویت قدرت کافی برای انجام درست وظیفه خود را دارند؛

ت. ایجاد و اجرای یک فرایند راهبری برای توزیع اولیه ابزارهای احراز هویت، مدیریت ابزارهای احراز هویتاز دست رفته یا به خطر افتاده، و بازیابی ابزارهای احراز هویت؛

ث. تغییر محتوای پیش فرض ابزارهای احراز هویت پیش از نصب سیستم اطلاعاتی؛

ج. تعیین محدودیت‌هایی در زمینه حداقل و حداکثر طول عمر و استفاده مجدد از شرایط برای ابزارهای احراز هویت؛

چ. تغییر یا بارگذاری مجدد[۱۹۱] ابزارهای احراز هویت در [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان بر اساس نوع ابزارهای احراز هویت]؛

ح. جلوگیری از تغییر و افشای غیر مجاز محتوای ابزارهای احراز هویت؛

خ. ملزم کردن افراد و دستگاه‌ها به استفاده از ابزارهای امنیتی برای حفاظت از ابزارهای احراز هویت؛

د. تغییر ابزارهای احراز هویت مربوط به حساب‌ها گروهی، در صورتی که اعضای گروه تغییر کنند.

راهنمایی‌های تکمیلی: به عنوان نمونه‌هایی از ابزارهای احراز هویت، می‌توان به گذرواژه، ژتون، اطلاعات بیومتریک، گواهی‌نامه‌های PKI، و کارت‌ها اشاره کرد. محتوای اولیه ابزارهای احراز هویت، عبارت است از محتوای اصلی (مانند گذرواژه اولیه) که با توجه به الزامات مربوطه (مانند حداقل طول گذرواژه) تعیین می‌شود. در بسیاری از موارد، مؤلفه‌های سیستم‌های اطلاعاتی با محتوای پیش فرض خود برای مشتری فرستاده می‌شوند، و مشتری می‌تواند پیکربندی مورد نظر خود را در زمان نصب انجام دهد. محتوای پیش فرض معمولا

[191] refresh

محتوایی ساده است که به راحتی می‌توان آن را حدس زد، و در نتیجه در معرض مخاطره امنیتی زیادی قرار دارد. الزامات مربوط به حفاظت از ابزارهای احراز هویت فردی در کنترل‌های PL-4 و PS-6، و الزامات مربوط به آن دسته از ابزارهای احراز هویت که در سیستم‌های اطلاعات سازمانی ذخیره شده‌اند (مانند گذرواژه‌های ذخیره‌شده در قالب‌های درهم‌سازی‌شده یا رمزگذاری‌شده، یا فایل‌هایی که گذرواژه‌های درهم‌سازی‌شده یا رمزگذاری‌شده دارند و تنها راهبر می‌تواند به این گذرواژه‌ها دسترسی داشته باشد)، در کنترل‌های AC-3 و AC-6 تشریح شده‌اند. سیستم‌های اطلاعاتی برای مدیریت ابزارهای احراز هویت از محدودیت‌ها و تنظیمات سازمانی استفاده می‌کنند. به عنوان مثال‌هایی از این محدودیت‌ها و تنظیمات، می‌توان به حداقل طول گذرواژه، ترکیب گذرواژه، پنجره زمان اعتبار برای ژتون‌های متقارن زمانی، و تعداد تلاش‌های ورود ناموفق در هنگام استفاده از اطلاعات بیومتریک اشاره کرد. برای حفاظت از ابزارهای احراز هویت می‌توان از روش‌ها و ابزارهای مختلفی استفاد کرد. به عنوان مثال، می‌توان تنظیمات را به گونه‌ای انجام داد که مالکیت ابزارهای فردی تنها در اختیار کاربر مورد نظر باشد، ابزارهای احراز هویت فردی را با سایر کاربران به اشتراک نگذاشت، و در صورت از دست رفتن یا به خطر افتادن ابزارهای احراز هویت، مراتب را در اسرع وقت اطلاع‌رسانی نمود. فرایند مدیریت ابزارهای احراز هویت شامل این موارد است: صدور ابزارهای احراز هویت، فسخ این ابزارها در صورتی که دیگر نیازی به آن‌ها نباشد، و صدور ابزارهای احراز هویت موقتی برای مواردی از جمله تعمیر و نگهداری از راه دور. ابزارهای احراز هویت دستگاه‌ها شامل مواردی از جمله گواهی‌نامه‌ها و گذرواژه‌ها هستند. کنترل‌های مربوطه: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

کنترل‌های پیشرفته:

(۱) مدیریت ابزارهای احراز هویت / احراز هویت مبتنی بر گذرواژه

سیستم اطلاعاتی، اقدامات زیر را برای تحقق احراز هویت مبتنی بر گذرواژه صورت می‌دهد:

(الف) رعایت حداقل پیچیدگی گذرواژه بر اساس [اختصاص: الزامات تعیین‌شده توسط سازمان در زمینه حساسیت به کوچک و بزرگ بودن حروف، تعداد کاراکترها، ترکیب حروف بزرگ و کوچک، حروف کوچک، اعداد، کاراکترهای ویژه، شامل حداقل الزامات در خصوص هر یک از این موارد]؛

(ب) تعیین حداقل این تعداد از کاراکترهای عوض‌شده در صورت تغییر گذرواژه: [اختصاص: تعداد تعیین‌شده توسط سازمان]؛

(پ) ذخیره‌سازی و انتقال صرفا آن دسته از گذرواژه‌ها که با روش‌های رمزنگاری از آن‌ها حفاظت شده است؛

(ت) تعیین محدودیت‌هایی در زمینه حداقل و حداکثر طول عمر، بر اساس: [اختصاص: حداقل طول عمر تعیین‌شده توسط سازمان، حداکثر طول عمر تعیین‌شده توسط سازمان]؛

(ث) جلوگیری از استفاده مجدد از گذرواژه برای [اختصاص: عدد تعیین‌شده توسط سازمان] بار؛ و

(ج) امکان استفاده از گذرواژه موقتی برای ورود به سیستم با تغییر سریع گذرواژه اصلی.

راهنمایی‌های تکمیلی: این کنترل پیشرفته در مواردی اعمال می‌شود که افراد می‌خواهند با استفاده از ابزارهای احراز هویت فردی یا گروهی، احراز هویت تک عاملی را انجام دهند، یا هنگامی که گذرواژه‌ها بخشی از ابزارهای احراز هویت چند عاملی هستند. کنترل حاضر در مواردی که گذرواژه‌ها برای باز کردن قفل ابزارهای احراز هویت سخت‌افزاری (مانند کارت‌های احراز هویت شخصی) مورد استفاده قرار می‌گیرند، اعمال نمی‌شود. استفاده از چنین سازوکارهایی، ممکن است مبتنی بر تمامی الزامات این کنترل پیشرفته نباشد. به عنوان مثال‌هایی از گذرواژه‌های مبتنی بر رمزنگاری، می‌توان به نسخه‌های رمزگذاری‌شده گذرواژه‌ها و درهم‌سازهای یک‌سویه گذرواژه‌ها اشاره کرد. تعداد کاراکترهای تغییریافته، یعنی تعداد تغییرهای مورد نیاز با توجه به تعداد کل مکان‌های موجود در گذرواژه فعلی. محدودیت‌های مربوط به طول عمر گذرواژه، در مورد گذرواژه‌های موقتی اعمال نمی‌شوند. برای کاهش مخاطره حملات جستجوی فراگیر[۱۹۲]، سازمان‌ها ممکن است از روش‌های رمزنگاری دیگری مانند salting نیز استفاده کنند. کنترل مربوطه: IA-6.

(۲) مدیریت ابزارهای احراز هویت / احراز هویت مبتنی بر PKI

سیستم‌های اطلاعاتی، اقدامات زیر را برای احراز هویت مبتنی بر PKI انجام می‌دهند:

(الف) تأیید گواهی‌نامه‌ها با ایجاد و تأیید یک مسیر گواهی‌نامه به مرجع اعتماد[۱۹۳] پذیرفته‌شده، شامل بررسی اطلاعات مربوط به وضعیت گواهی‌نامه؛

(ب) فراهم آوردن امکان دسترسی مجاز به کلید عمومی مربوطه؛

(پ) برقراری ارتباط بین یک هویت احرازشده و حساب کاربردی فرد یا گروه؛ و

(ت) استفاده از یک حافظه نهان[۱۹۴] محلی برای ذخیره‌سازی داده‌های مربوط به فسخ، به منظور تأیید و شناسایی مسیر در صورت ناتوانی در دسترسی به این داده‌ها از طریق شبکه.

راهنمایی‌های تکمیلی: اطلاعات مربوط به وضعیت مسیر گواهی‌نامه، شامل مواردی از جمله لیست فسخ گواهی‌نامه یا پاسخ پروتکل به وضعیت گواهی‌نامه‌ها است. در مورد کارت‌های PIV، تأیید گواهی‌نامه‌ها

---

[192] brute-force attack
[193] trust anchor
[194] cache

شامل ایجاد و تأیید یک مسیر گواهی‌نامه به مرجع اعتماد Common Policy Root است. کنترل مربوطه: IA-6.

(۳) مدیریت ابزارهای احراز هویت / ثبت نام حضوری یا ثبت نام از طریق شخص ثالث مورد اعتماد

سازمان، این الزام را تعیین می‌کند که فرایند ثبت نام برای دریافت [اختصاص: انواع ابزارهای احراز هویت و/یا یک ابزار احراز هویت خاص تعیین‌شده توسط سازمان] باید به صورت [انتخاب: حضوری، توسط شخص ثالث مورد اعتماد] نزد [اختصاص: مسئول ثبت نام تعیین‌شده توسط سازمان] و با مجوز [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] انجام شود.

(۴) مدیریت ابزارهای احراز هویت / پشتیبانی خودکار از تعیین قدرت گذرواژه

سازمان، ابزارهای خودکار را به کار می‌گیرد تا مشخص کند که آیا ابزارهای احراز هویت مبتنی بر گذرواژه به اندازه‌ای قدرتمند هستند که [اختصاص: الزامات تعیین‌شده توسط سازمان] را برآورده کنند یا خیر.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، درباره ایجاد یک گذرواژه قدرتمند و ویژگی‌های این گذرواژه‌ها (مانند پیچیدگی) پیش از استفاده، و اجرای موارد مطرح‌شده در مورد سیستم‌های اطلاعات سازمانی در IA-5(1) است. کنترل‌های مربوطه: CA-2, CA-7, RA-5.

(۵) مدیریت ابزارهای احراز هویت / تغییر ابزارهای احراز هویت پیش از تحویل

سازمان، توسعه‌دهندگان و نصب‌کنندگان مؤلفه‌های سیستم اطلاعاتی را ملزم می‌کند تا پیش از تحویل یا نصب این مؤلفه‌ها، ابزارهای احراز هویت منحصر به فردی را ارائه کنند یا ابزارهای احراز هویت پیش فرض را تغییر دهند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، الزامات سازمان در خصوص تغییر ابزارهای احراز هویت پیش فرض در زمان نصب سیستم اطلاعاتی را بسط و گسترش می‌دهد. بر اساس کنترل پیشرفته حاضر، توسعه‌دهندگان و نصب‌کنندگان مؤلفه‌های سیستم اطلاعاتی باید پیش از تحویل یا نصب این مؤلفه‌ها، ابزارهای احراز هویت منحصر به فردی را ارائه کنند یا ابزارهای احراز هویت پیش فرض را تغییر دهند. اما این الزام معمولد درباره توسعه‌دهندگان محصولات IT تجاری موجود در بازار صدق نمی‌کند. ممکن است در اسناد سازمانی ذکر شود که در هنگام تهیه و تدارک سیستم‌های اطلاعاتی یا مؤلفه‌های این سیستم‌ها، لازم است که ابزارهای احراز هویت منحصر به فردی ارائه شوند.

(۶) مدیریت ابزارهای احراز هویت / حفاظت از ابزارهای احراز هویت

سازمان بر اساس دسته امنیتی اطلاعاتی که برای دسترسی به آن‌ها نیاز به ابزارهای احراز هویت است، از این ابزارها حفاظت می‌نماید.

راهنمایی‌های تکمیلی: در مورد آن دسته از سیستم‌های اطلاعاتی که دسته‌های امنیتی متفاوتی از اطلاعات را شامل می‌شوند و تمایز فیزیکی یا منطقی قابل اعتمادی بین این دسته‌ها وجود دارد، ابزارهای احراز هویت مربوطه، بر اساس دسته امنیتی اطلاعاتی که برای دسترسی به آن‌ها نیاز به ابزارهای مذکور است، مورد محافظت قرار می‌گیرند.

(۷) مدیریت ابزارهای احراز هویت / تعبیه نشدن ابزارهای احراز هویت استاتیک رمزگذاری‌نشده در سیستم

سازمان اطمینان حاصل می‌نماید که ابزارهای احراز هویت استاتیک رمزگذاری‌نشده، در برنامه‌های کاربردی یا اسکریپت‌های دسترسی تعبیه نشده یا در کلیدهای تابعی[۱۹۵] ذخیره نشده‌اند.

راهنمایی‌های تکمیلی: سازمان‌ها برای تعیین این که آیا ابزارهای احراز هویت تعبیه‌شده یا ذخیره‌شده، رمزگذاری شده‌اند یا خیر، احتیاط لازم را به عمل می‌آورند. اگر ابزارهای احراز هویت به همان صورتی که ذخیره شده‌اند مورد استفاده قرار گیرند، به عنوان ابزارهای احراز هویت رمزگذاری‌نشده در نظر گرفته می‌شوند. این ابزارهای احراز هویت به عنوان رمزگذاری‌نشده در نظر گرفته خواهند شد، حتی اگر حالت رمزگذاری‌شده چیز دیگری باشند (مثلا حالت رمزگذاری‌شده یک گذرواژه باشند).

(۸) مدیریت ابزارهای احراز هویت / حساب‌های چندگانه در سیستم‌های اطلاعاتی

سازمان، [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] را برای محافظت از حساب‌های افرادی که چند حساب کاربری در سیستم‌های اطلاعاتی مختلف دارند، به کار می‌گیرد.

راهنمایی‌های تکمیلی: در صورتی که افراد چند حساب را در سیستم‌های اطلاعاتی مختلف داشته باشند و در همه آن‌ها از ابزارهای احراز هویت یکسان استفاده کرده باشند، به خطر افتادن یکی از این حساب‌ها می‌تواند بقیه آن‌ها را نیز در معرض خطر قرار دهد. برای مقابله با این خطر، می‌توان یکی از این اقدامات را انجام داد: (۱) استفاده از ابزارهای احراز هویت مختلف در سیستم‌های متفاوت، (۲) استفاده از سازوکار یک بار ورود[۱۹۶]، یا (۳) استفاده از گذرواژه‌های یک بار مصرف در تمام سیستم‌ها.

(۹) مدیریت ابزارهای احراز هویت / مدیریت بین‌سازمانی اطلاعات حساب‌های کاربری

سازمان، هماهنگی‌های لازم برای مدیریت بین‌سازمانی اطلاعات حساب کاربری را با [اختصاص: سازمان‌های خارجی تعیین‌شده توسط سازمان] انجام می‌دهد.

---

[195] function keys

[196] single sign-on

راهنمایی‌های تکمیلی: مدیریت بین‌سازمانی اطلاعات حساب‌های کاربری، این امکان را به سازمان‌ها می‌دهد که در فرایندهای بین‌سازمانی از جمله پردازش، ذخیره‌سازی و انتقال اطلاعات، افراد و گروه‌ها و نقش‌ها و سازمان‌ها را به خوبی احراز هویت کنند.

(۱۰) مدیریت ابزارهای احراز هویت / ایجاد ارتباط پویا بین اطلاعات حساب‌های کاربری

سیستم اطلاعاتی، شناسه‌ها و هویت‌های پویایی را فراهم می‌آورد.

راهنمایی‌های تکمیلی: برای احراز هویت، لازم است که نوع رابطه بین هویت و ابزارهای احراز هویت مورد استفاده برای تأیید آن هویت وجود داشته باشد. در روش‌های قدیمی، هم هویت و هم ابزارهای احراز هویت از قبل به سیستم اطلاعاتی فرستاده می‌شوند. به عنوان مثال، یک نام کاربری (یعنی هویت) و یک گذرواژه (یعنی ابزار احراز هویت) در کنار هم برای سیستم اطلاعاتی ارسال می‌شوند. روش‌های احراز هویت جدید این امکان را فراهم می‌آورند که رابطه بین هویت و ابزارهای احراز هویت در خارج از سیستم اطلاعاتی شکل گیرد. مثلا در کارت‌های هوشمند، ارتباط بین هویت و ابزار احراز هویت در کارت برقرار می‌شود. سیستم‌های اطلاعاتی می‌توانند با استفاده از این روش‌های جدید، هویت‌هایی را که از پیش ارسال نشده‌اند، احراز هویت نمایند و هویت را به صورت پویا پس از احراز ارائه نمایند. در این شرایط، سازمان‌ها باید انتظار ارائه پویای هویت را داشته باشند. برای تحقق این روش‌ها، لازم است که سازوکارها و روابط مبتنی بر اعتماد با مسئولان مربوطه شکل گرفته باشد تا بتوان هویت‌ها و اطلاعات حساب‌های کاربری را تأیید نمود.

(۱۱) مدیریت ابزارهای احراز هویت / احراز هویت سخت‌افزاری مبتنی بر ژتون

سیستم اطلاعاتی، برای احراز هویت سخت‌افزاری مبتنی بر ژتون از سازوکارهایی استفاده می‌کند که [اختصاص: الزامات تعیین‌شده توسط سازمان در زمینه کیفیت ژتون] را برآورده نمایند.

راهنمایی‌های تکمیلی: منظور از احراز هویت سخت‌افزاری مبتنی بر ژتون، استفاده از ژتون‌های مبتنی بر PKI از جمله کارت تأیید هویت فردی دولت امریکا (PIV) است. سازمان‌ها الزاماتی را نیز در مور این ژتون‌ها تعریف می‌کنند؛ مثلا این که ژتون مورد استفاده امکان کار با یک PKI خاص را داشته باشد.

(۱۲) مدیریت ابزارهای احراز هویت / احراز هویت مبتنی بر استفاده از اطلاعات بیومتریک

سیستم اطلاعاتی، برای احراز هویت مبتنی بر استفاده از اطلاعات بیومتریک، از سازوکارهایی استفاده می‌کند که [اختصاص: الزامات تعیین‌شده توسط سازمان در زمینه کیفیت اطلاعات بیومتریک] را برآورده نمایند.

راهنمایی‌های تکمیلی: بر خلاف روش احراز هویت مبتنی بر گذرواژه که در آن گذرواژه واردشده توسط کاربر با گذرواژه ذخیره‌شده مقایسه می‌شود، در احراز هویت مبتنی بر استفاده از اطلاعات بیومتریک نیازی نیست که چنین تطبیق دقیقی وجود داشته باشد. بسته به نوع اطلاعات بیومتریک و روش مورد استفاده برای گردآوری این اطلاعات، ممکن است مقدار خاصی اختلاف بین اطلاعات واردشده و اطلاعات ذخیره‌شده ایرادی نداشته باشد و در صورت بیشتر بودن اختلاف از حد مورد نظر، احراز هویت با موفقیت انجام نشود. در چنین مقایسه‌ای، امکان احراز هویت موفق در صورت نادرست بودن اطلاعات و همچنین امکان احراز هویت ناموفق در صورت درست بودن اطلاعات وجود دارد. نرخ برابر بودن این دو احتمال، به عنوان نرخ هم‌گذری[۱۹۷] شناخته می‌شود. به عنوان مثالی از الزامات مربوط به کیفیت اطلاعات بیومتریک، می‌توان به نرخ هم‌گذری اشاره کرد، زیرا این نرخ همواره نشان‌دهنده دقت اطلاعات بیومتریک است.

(۱۳) مدیریت ابزارهای احراز هویت / منقضی شدن ابزارهای احراز هویت ذخیره‌شده در حافظه نهان سیستم اطلاعاتی، استفاده از ابزارهای احراز هویت ذخیره‌شده در حافظه نهان را پس از [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] ممنوع می‌کند.

(۱۴) مدیریت ابزارهای احراز هویت / مدیریت محتوای فروشگاه‌های PKI مورد اعتماد

سازمان، برای احراز هویت مبتنی بر PKI، از روش‌های سازمانی مقتضی برای مدیریت محتوای فروشگاه‌های PKI مورد اعتماد نصب‌شده روی پلت‌فرم‌های مختلف (از جمله شبکه‌ها، سیستم‌عامل‌ها، مرورگرها و برنامه‌های کاربردی) استفاده می‌کند.

(۱۵) مدیریت ابزارهای احراز هویت / خدمات و ابزارهای حفاظتی تأییدشده توسط FICAM

سازمان، تنها از آن دسته از خدمات و محصولات شناسایی و تأیید مسیر استفاده می‌کند که توسط FICAM تأیید شده‌اند.

راهنمایی‌های تکمیلی: منظور از خدمات و محصولات شناسایی و تأیید مسیر تأییدشده توسط مدیریت هویت، اطلاعات حساب کاربری و دسترسی فدرال (FICAM)، محصولات و خدماتی هستند که با برنامه‌های FICAM انطباق داشته باشند.

مراجع: تفاهم‌نامه OMB 04-04, 11-11؛ FIPS 201؛ شماره‌های ویژه NIST 800-73, 800-63, 800-76, 800-78؛ نقشه راه و راهنمای پیاده‌سازی FICAM؛ آدرس اینترنتی http://idmanagement.gov

[197] crossover rate

اولویت و تخصیص به مجموعه‌های پایه:

P1	IA-5(1)(11) اولویت پایین	IA-5(1)(2)(3)(11) اولویت متوسط	IA-5(1)(2)(3)(11) اولویت بالا

IA-6: بازخوردهای مربوط به ابزارهای احراز هویت

کنترل: سیستم اطلاعاتی، بازخورد اطلاعات احراز هویت در جریان فرایند احراز هویت را به صورت مبهم و ناخوانا نشان می‌دهد، تا افراد غیر مجاز نتوانند به این اطلاعات دست یابند و از آن‌ها استفاده نمایند.

راهنمایی‌های تکمیلی: سیستم اطلاعاتی، بازخورد را به گونه‌ای ارائه می‌کند که افراد غیر مجاز نتوانند سازوکار احراز هویت را به خطر اندازند. این تهدید ممکن است در مورد برخی از انواع خاص سیستم‌های اطلاعاتی یا مؤلفه‌ها (مانند نوت‌بوک‌ها و کامپیوترهای رومیزی) بسیار زیاد باشد. در مورد برخی دیگر از سیستم‌های اطلاعاتی و مؤلفه‌ها (مانند دستگاه‌های همراه با صفحه نمایش ۲ تا ۴ اینچی)، این تهدید چندان زیاد نیست. در چنین مواردی، باید تعادل لازم را بین مبهم و ناخوانا بودن بازخورد و افزایش احتمال خطای در ورود اطلاعات (به دلیل کوچک بودن صفحه نمایش) برقرار نمود. در این حالت‌ها، ابزار مورد استفاده برای ناخوانا کردن بازخورد به گونه مقتضی انتخاب می‌شود. برا ناخوانا کردن بازخورد می‌توان از روش‌های مختلفی استفاده کرد. به عنوان مثال، ممکن است در هنگام تایپ کردن ابزار احراز هویت، به جای کاراکترها ستاره نمایش داده شود یا این که کاراکترها تنها برای مدت زمان بسیار کوتاهی نشان داده شوند و به سرعت محو گردند. کنترل مربوطه: PE-18.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	IA-6 اولویت پایین	IA-6 اولویت متوسط	IA-6 اولویت بالا

IA-7: احراز هویت در ماژول رمزنگاری

کنترل: سیستم اطلاعاتی، از سازوکارهایی برای احراز هویت در ماژول رمزنگاری استفاده می‌کند که مبتنی بر الزامات مورد اشاره در دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال مربوطه باشند.

راهنمایی‌های تکمیلی: ممکن است در یک ماژول رمزنگاری، نیاز به استفاده از سازوکارهای احراز هویت وجود داشته باشد تا اپراتور احراز هویت نماید و بتوان اطمینان حاصل نمود که اپراتور مذکور اجازه دسترسی به اطلاعات را دارد. کنترل‌های مربوطه: SC-12, SC-13.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: FIPS 140؛ آدرس اینترنتی http://csrc.nist.gov/groups/STM/cmvp/index.html

اولویت و تخصیص به مجموعه‌های پایه:

P1	IA-7 اولویت پایین	IA-7 اولویت متوسط	IA-7 اولویت بالا

IA-8: شناسایی و احراز هویت (برای کاربران غیر سازمانی)

کنترل: سیستم اطلاعاتی، کاربران غیر سازمانی (یا فرایندهایی که از سوی آن‌ها اجرا می‌شوند) را به صورت منحصر به فرد شناسایی و احراز هویت می‌کند.

راهنمایی‌های تکمیلی: به عنوان نمونه‌هایی از کاربران غیر سازمانی می‌توان به کاربران غیر سازمانی سیستم‌های اطلاعاتی اشاره کرد (الزامات مربوط به کارکنان سازمانی در بخش IA-2 آمده است). این افراد، برای دسترسی‌هایی به جز آن چه در بخش AC-14 ذکر شده است، به صورت منحصر به فرد شناسایی و احراز هویت می‌شوند. بر اساس پروژه احراز هویت الکترونیک در دولت الکترونیک، لازم است که کاربران غیر سازمانی برای دسترسی به سیستم‌های اطلاعاتی فدرال، احراز هویت شوند تا از اطلاعات خصوصی یا محرمانه فدرال محافظت شود (استثنائاتی در مورد سیستم‌های امنیت ملی در نظر گرفته شده است). سازمان‌ها با استفاده از روش‌های بررسی مخاطره، نیازها و الزامات احراز هویت را تعیین می‌کنند. سازمان‌ها برای انجام این کار، مقیاس‌پذیری، امکان‌پذیری و امنیت را مورد توجه قرار می‌دهند. کنترل‌های مربوطه: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.

کنترل‌های پیشرفته:

(۱) شناسایی و احراز هویت / پذیرفتن اطلاعات PIV حساب‌های کاربری از سایر ادارات

سیستم اطلاعاتی، اطلاعات PIV حساب‌های کاربری را از سایر ادارات فدرال می پذیرد و آن‌ها را به صورت الکترونیکی تأیید می‌نماید.

راهنمایی‌های تکمیلی: این کنترل پیشرفته در مورد سازمان‌هایی اعمال می‌شود که از سیستم‌های کنترل دسترسی منطقی (LACS) و سیستم‌های کنترل دسترسی فیزیکی (PACS) استفاده می‌کنند. اطلاعات تأیید هویت فردی (PIV)، توسط ادارات فدرالی صادر می‌شوند که FIPS 201 و اسناد راهنمای مربوطه را تأیید می‌کنند. تفاهم‌نامه OMB 11-11 ادارات فدرال را ملزم می‌کند که الزامات تعیین‌شده در HSPD-12 را به کار گیرند و از اطلاعات تأیید هویت فردی استفاده نمایند. کنترل‌های مربوطه: AU-2, PE-3, SA-4.

(۲) شناسایی و احراز هویت / پذیرفتن اطلاعات حساب‌های کاربری اشخاص ثالث

سیستم اطلاعاتی، تنها آن دسته از اطلاعات حساب‌های کاربری اشخاص ثالث را می پذیرد که مورد تأیید FICAM باشند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته در مورد آن دسته از سیستم‌های اطلاعاتی سازمانی اعمال می‌شود که در دسترس عموم مردم قرار دارند (مانند وب‌سایت‌هایی که همه به آن‌ها دسترسی دارند). منظور از اطلاعات حساب‌های کاربری اشخاص ثالث، آن دسته از اطلاعات حساب‌های کاربری است که توسط سازمان‌های غیر فدرال مورد تأیید FICAM فراهم آمده‌اند. این اطلاعات باید مطابق با الزامات سازمانی، حریم خصوصی، امنیتی و فنی فدرال باشند. بدین ترتیب، سازمان‌های وابسته به دولت فدرال می‌توانند از صحت و اعتبار اطلاعات حساب‌های کاربری اطمینان حاصل نمایند. کنترل مربوطه: AU-2.

(۳) شناسایی و احراز هویت / استفاده از محصولات تأییدشده توسط FICAM

سازمان، در [اختصاص: سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] تنها از مؤلفه‌های تأییدشده توسط FICAM برای پذیرفتن اطلاعات حساب‌های کاربری اشخاص ثالث استفاده می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته در مورد آن دسته از سیستم‌های اطلاعاتی سازمانی اعمال می‌شود که در دسترس عموم مردم قرار دارند (مانند وب‌سایت‌هایی که همه به آن‌ها دسترسی دارند). مؤلفه‌های تأییدشده توسط FICAM شامل مواردی از جمله محصولات IT و کتابخانه‌های نرم‌افزاری است که به تأیید FICAM رسیده‌اند. کنترل مربوطه: SA-4.

(۴) شناسایی و احراز هویت / استفاده از پروفایل‌های صادرشده توسط FICAM

سیستم اطلاعاتی، از پروفایل‌های صادرشده توسط FICAM پیروی می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته، به استانداردهای مدیریت هویت باز[۱۹۸] می‌پردازد. برای حصول اطمینان از کاربردی، قابل اعتماد و پایدار بودن این استانداردها و قابلیت همکاری آن‌ها، دولت امریکا آن‌ها را با توجه به قوانین، مقررات، رهنمودها، خط‌مشی‌ها و الزامات خود مورد بررسی قرار می‌دهد. نتیجه این فرایند، پروفایل‌های صادرشده توسط FICAM است که پروتکل‌های مورد تأیید را نشان می‌دهند. کنترل مربوطه: SA-4.

(۵) شناسایی و احراز هویت / پذیرفتن اطلاعات PIV-I حساب‌های کاربری

سیستم اطلاعاتی، اطلاعات PIV-I حساب‌های کاربری را می پذیرد و آن‌ها را به صورت الکترونیکی تأیید می‌نماید.

راهنمایی‌های تکمیلی: این کنترل پیشرفته: (۱) در مورد سیستم‌های کنترلی با دسترسی فیزیکی و منطقی اعمال می‌شود، و (۲) به مسائل مربوط به صادرکنندگان غیر فدرال (NFI) کارت‌های شناسایی می‌پردازد که می‌خواهند با سیستم‌های اطلاعاتی PIV دولت امریکا همکاری داشته باشند و سازمان‌های وابسته به دولت فدرال می‌توانند به آن‌ها اعتماد نمایند. خط‌مشی گواهی‌نامه X.509 برای FBCA، الزامات PIV-I را پوشش می‌دهد. کارت PIV-I برای سطح تضمینی ۴ (که در تفاهم‌نامه OMB 04-04 و NIST 800-63 تشریح شده است) و احراز هویت چند عاملی (که در NIST 800-116 تشریح شده است) مناسب است. منظور از اطلاعات PIV-I حساب‌های کاربری، آن دسته از اطلاعات حساب‌های کاربری است که توسط تأمین‌کننده PIV-I صادر شده‌اند که خط‌مشی PIV-I آن مبتنی بر خط‌مشی گواهی‌نامه PIV-I فدرال است. یک تأمین‌کننده PIV-I در صورتی توسط FBCA تأیید می‌شود (به صورت مستقیم یا از طریق یک PKI دیگر) که مطابق با الزامات تعریف‌شده در خط‌مشی FBCA باشد. کنترل مربوطه: AU-2.

مراجع: تفاهم‌نامه OMB 04-04, 11-11, 10-06-2011؛ FIPS 201؛ شماره‌های ویژه NIST 800-63, 800-116؛ نقشه راه و راهنمای پیاده‌سازی FICAM؛ راهبرد ملی هویت‌های قابل اعتماد در فضای مجازی؛ آدرس اینترنتی http://idmanagement.gov

اولویت و تخصیص به مجموعه‌های پایه:

P1	IA-8(1)(2)(3)(4) اولویت	IA-8(1)(2)(3)(4) اولویت	IA-8(1)(2)(3)(4) اولویت بالا

[198] open identity management standards

	پایین	متوسط	

IA-9: شناسایی و احراز هویت خدمات

کنترل: سازمان، [اختصاص: خدمات سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] را با استفاده از [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] شناسایی و احراز هویت می‌نماید.

راهنمایی‌های تکمیلی: این کنترل، از معماری‌های سیستم‌محور و سایر معماری‌های توزیع‌شده پشتیبانی می‌کند که نیازمند شناسایی و احراز هویت سیستم‌های اطلاعاتی هستند. در این معماری‌ها، خدمات خارجی معمولا به صورت پویا ارائه می‌شوند. بنابراین، سیستم‌های اطلاعاتی باید بتوانند به صورت پویا تعیین کنند که آیا تأمین‌کنندگان خارجی و خدمات ارائه‌شده توسط آن‌ها معتبر هستند یا خیر. ابزارهای امنیتی مورد استفاده سیستم‌های اطلاعاتی سازمانی برای تأیید اعتبار این تأمین‌کنندگان و خدمات آن‌ها، شامل مواردی از جمله امضای کد و اطلاعات، نمودارهای تأیید اصالت، و/یا امضای دیجیتال تأیید کننده منشأ خدمات هستند.

کنترل‌های پیشرفته:

(۱) شناسایی و احراز هویت خدمات / تبادل اطلاعات

سازمان اطمینان حاصل می‌نماید که تأمین‌کنندگان خدمات، اطلاعات مربوط به شناسایی و احراز هویت را دریافت می‌کنند، تأیید می‌نمایند و انتقال می‌دهند.

(۲) شناسایی و احراز هویت خدمات / انتقال تصمیمات

سازمان اطمینان حاصل می‌نماید که تصمیمات مربوط به شناسایی و احراز هویت، بین [اختصاص: خدمات تعیین‌شده توسط سازمان] سازگار با خط‌مشی‌های سازمانی انتقال پیدا می‌کنند.

راهنمایی‌های تکمیلی: در مورد معماری‌های توزیع‌شده (مانند معماری‌های خدمت‌محور)، تصمیمات مربوط به شناسایی و احراز هویت ممکن است توسط خدماتی که از سوی این تصمیمات عمل می‌کنند اتخاذ نشوند، بلکه از سوی خدمات دیگر اتخاذ گردند. در این شرایط، لازم است که تصمیمات مربوط به شناسایی و احراز هویت به خدماتی که از سوی این تصمیمات عمل می‌کنند، انتقال داده شوند. کنترل مربوطه: SC-8.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

IA-10: شناسایی و احراز هویت تطبیقی

کنترل: سازمان، افرادی که به سیستم اطلاعاتی دسترسی دارند را ملزم می‌نماید تا [اختصاص: سازوکارها و روش‌های تکمیلی احراز هویت تعیین‌شده توسط سازمان] را بر اساس [اختصاص: شرایط و موقعیت‌های تعیین‌شده توسط سازمان] به کار گیرند.

راهنمایی‌های تکمیلی: ممکن است که مهاجمان، سازوکارهای احراز هویت افراد را مورد هدف قرار دهند و سپس تلاش کنند تا خود را به جای کاربران مجاز، جا بزنند. این اتفاق می‌تواند در مورد تمام سازوکارهای مورد استفاده سازمان رخ دهد. برای مقابله با این تهدید، سازمان‌ها می‌توانند سازوکارها و روش‌های خاصی را برای بررسی رفتارهای مشکوک به کار گیرند یا پروتکل‌هایی را در این زمینه تهیه کنند. به عنوان نمونه‌هایی از رفتارهای مشکوک، می‌توان به این موارد اشاره کرد: دسترسی افراد به اطلاعاتی که ارتباطی با نقش‌ها و مسئولیت‌های آن‌ها ندارد، دسترسی افراد به حجم زیادی از اطلاعات که معمولا در شرایط عادی به این حجم دسترسی ندارند، یا تلاش برای دسترسی به اطلاعات از آدرس‌های اینترنتی مشکوک. در این شرایط، سازمان‌ها می‌توانند از چنین افرادی بخواهند که اطلاعات احراز هویت بیشتری را ارائه نمایند. یکی دیگر از کاربردهای شناسایی و احراز هویت تطبیقی، افزایش قدرت سازوکارها بر اساس تعداد و/یا نوع سوابق مورد دسترسی است.
کنترل‌های مربوطه: AU-6, SI-4.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

IA-11: احراز هویت مجدد

کنترل: در هنگامی که [اختصاص: شرایط و موقعیت‌های تعیین‌شده توسط سازمان، لزوم احراز هویت مجدد را نشان دهند]، سازمان از کاربران و دستگاه‌ها می‌خواهد که مجددا احراز هویت نمایند.

راهنمایی‌های تکمیلی: علاوه بر مواردی که در اثر قفل شدن نشست، نیاز به احراز هویت مجدد وجود دارد، در موارد دیگر نیز ممکن است سازمان از کاربران و دستگاه‌ها بخواهد که مجددا احراز هویت نمایند. به عنوان نمونه‌ای از این شرایط، می‌توان به موارد روبرو اشاره کرد: (۱) وقتی که ابزارهای احراز هویت تغییر می‌کنند؛ (۲) وقتی که نقش‌ها تغییر می‌کنند؛ (۳) وقتی که دسته‌های امنیتی سیستم‌های اطلاعاتی تغییر می‌کنند؛ (۴) وقتی توابه ویژه اجرا می‌شوند؛ (۵) پس از مدت زمان تعیین‌شده؛ یا (۶) به طور دوره‌ای. کنترل مربوطه: AC-11.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، اولویت پایین	انتخاب نشده، اولویت متوسط	انتخاب نشده، اولویت بالا

خانواده: واکنش به حوادث

IR-1: خط‌مشی و رویه‌های واکنش به حوادث

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۱۳. خط‌مشی واکنش به حوادث شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و

۱۴. رویه‌های تسهیل پیاده‌سازی خط‌مشی واکنش به حوادث و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۱۳. خط‌مشی واکنش به حوادث؛ و

۱۴. رویه‌های واکنش به حوادث.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده IR را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: نشریه‌های ویژه NIST 800-12، NIST 800-61، NIST800-83 و NIST800-100

اولویت و تخصیص به مجموعه‌های پایه:

P1	IR-1 اولویت پایین	IR-1 اولویت متوسط	IR-1 اولویت بالا

IR-2: آموزش‌های واکنش به حوادث

کنترل: سازمان، آموزش‌های واکنش به حوادث را متناسب با نقش‌ها و مسئولیت‌ها و با توجه به موارد زیر به کاربران سیستم‌های اطلاعاتی ارائه می‌کند:

الف. در [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] که انتظار می‌رود کاربران مذکور همچنان مسئولیت‌های خود را در زمینه برنامه‌ریزی برای رویدادهای آینده داشته باشند؛

ب. در صورتی که به موجب تغییر سیستم‌های اطلاعاتی، این آموزش‌ها ضروری شوند؛ و

پ. [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: آموزش‌های واکنش به حوادث، بر اساس نقش‌ها و مسئولیت‌های کارکنان سازمان به آن‌ها ارائه می‌شود تا اطمینان حاصل شود که محتوا و اطلاعات مناسبی در اختیار آن‌ها قرار گرفته است. به عنوان مثال، ممکن است برای کاربران ثابت تنها نیاز باشد که بدانند با چه کسی تماس بگیرند یا چگونه یک حادثه در سیستم‌های اطلاعاتی را تشخیص دهد. راهبران سیستم‌ها ممکن است به آموزش‌های بیشتری در خصوص نحوه مهار حوادث و جبران و اصلاح حوادث نیاز داشته باشند. افراد مسئول واکنش به حوادث نیز ممکن است آموزش‌های ویژه بیشتری در ارتباط با ممیزی قانونی، گزارش دادن و بازیابی و بازگردانی سیستم دریافت نمایند. آموزش‌های واکنش به حوادث شامل آموزش کاربران برای شناسایی و گزارش کردن فعالیت‌های مشکوک هم از جانب منابع داخلی و هم از جانب منابع خارجی می‌شود. کنترل‌های مربوطه: AT-3، CP-3 و IR-8.

کنترل‌های پیشرفته:

(۱) آموزش‌های واکنش به حوادث / رویدادهای شبیه‌سازی‌شده

سازمان در آموزش‌های واکنش به حوادث، از رویدادهای شبیه‌سازی‌شده استفاده می‌کند تا واکنش مؤثر از جانب کارکنان در شرایط بحرانی را تسهیل نماید.

(۲) آموزش‌های واکنش به حوادث / محیط‌های آموزشی خودکار

سازمان از سازوکارهای خودکار برای فراهم کردم یک محیط واقعی‌تر و جامع‌تر برای آموزش‌های واکنش به حوادث استفاده می‌کند.

مراجع: نشریه‌های ویژه NIST 800-16 و NIST 800-50

اولویت و تخصیص به مجموعه‌های پایه:

P2	IR-2 اولویت پایین	IR-2 اولویت متوسط	IR-2 (1)(2) اولویت بالا

IR-3: تست‌های واکنش به حوادث

کنترل: سازمان سامانه واکنش به حوادث را برای سیستم‌های اطلاعاتی [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] با استفاده از [اختصاص: تست‌های تعیین‌شده توسط سازمان] می‌آزماید تا میزان اثربخشی واکنش به حوادث را مشخص کند و نتایج را مستند می‌نماید.

راهنمایی تکمیلی: سازمان‌ها سامانه‌های واکنش به حوادث را می‌آزمایند تا اثربخشی کلی این سامانه‌ها را مشخص نمایند و ضعف‌ها و ناکارامدی‌های احتمالی را شناسایی کنند. چک‌لیست‌ها، بازبینی فیزیکی و میزگردهای شبیه‌سازی، شبیه‌سازی‌های موازی و توقف کامل[۱۹۹] و اقدامات جامع نمونه‌هایی از تست‌های واکنش به حوادث هستند. تست‌های واکنش به حوادث می‌تواند شامل بررسی تأثیرات ناشی از واکنش به حوادث روی عملیات‌های سازمانی (نظیر کاهش توانایی‌های مأموریتی)، دارایی‌های سازمانی و افراد نیز بشود. کنترل‌های مربوطه: CP-4 و IR-8.

کنترل‌های پیشرفته:

(۱) تست‌های واکنش به حوادث / تست‌های خودکار

سازمان از سازوکارهای خودکار برای انجام مؤثرتر و جامع‌تر تست‌های سامانه واکنش به حوادث استفاده می‌کند.

راهنمایی تکمیلی: سازمان‌ها از سازوکارهای خودکار برای انجام مؤثرتر و جامع‌تر تست‌های مربوط به سامانه‌های واکنش به حوادث استفاده می‌کند. نمونه‌هایی از این سازوکارها عبارتند از: (۱) ارائه پوشش کامل‌تر از مسائل مرتبط با واکنش به حوادث (۲) انتخاب برنامه‌ها و محیط‌های تست واقعی‌تر (۳) انجام تست‌های شدید روی توانایی و امکانات واکنش‌ها. کنترل مربوطه: AT-2.

[199] Full Interrupt

(۲) تست‌های واکنش به حوادث / هماهنگی با برنامه‌ریزی‌های مربوطه

سازمان تست‌های واکنش به حوادث را عناصر و عوامل سازمانی مسئول برنامه‌ریزی‌های مربوطه هماهنگ می‌نماید.

راهنمایی تکمیلی: برنامه‌ریزی‌های تداوم کسب‌وکار[۲۰۰]، برنامه‌ریزی برای رویدادهای آینده[۲۰۱]، برنامه‌ریزی‌های بازیابی پس از وقوع حادثه[۲۰۲]، برنامه‌های تداوم عملیات‌ها[۲۰۳]، برنامه‌ریزی‌های مربوط به ارتباطات هنگام بحران‌ها[۲۰۴]، برنامه‌ریزی‌های مربوط به زیرساخت‌های اساسی و حیاتی[۲۰۵] و برنامه‌ریزی‌های مربوط به ساکنان و حاضرین در ساختمان‌ها در شرایط اضطراری[۲۰۶]، نمونه‌هایی از برنامه‌ریزی‌های سازمانی مربوط به تست‌های واکنش به حوادث هستند.

مراجع: نشریه‌های ویژه NIST 800-84 و NIST 800-115

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب‌نشده، اولویت پایین	IR-3 (2) اولویت متوسط	IR-3 (2) اولویت بالا

IR-4: مهار حوادث

کنترل: سازمان:

الف. یک سیستم مهار حوادث برای حوادث امنیتی پیاده‌سازی می‌کند که شامل آماده‌سازی، شناسایی و تجزیه و تحلیل، محصور کردن، ریشه‌کنی و بازیابی می‌شود.

ب. فعالیت‌های مهار حوادث را با فعالیت‌های برنامه‌ریزی برای رویدادهای آینده هماهنگ می‌کند.

پ. نکات درس‌گرفته‌شده از فعالیت‌های در حال انجام مهار حوادث را در رویه‌ها، آموزش‌ها و تست‌های واکنش به حوادث تلفیق می‌کند و تغییرات به‌وجودآمده را به تناسب پیاده‌سازی می‌کند.

[200] Business Continuity Plans
[201] Contingency Plans
[202] Disaster Recovery Plans
[203] Continuity of Operations Plans
[204] Crisis Communications Plans
[205] Critical Infrastructure Plans
[206] Occupant Emergency Plans

راهنمایی تکمیلی: سازمان‌ها می‌دانند که سامانه واکنش به حوادث، به قابلیت‌های سیستم‌های اطلاعاتی سازمانی و فرایندهای مأموریتی و کسب‌وکاری مورد پشتیبانی این سیستم‌ها بستگی دارد. بنابراین، سازمان‌ها واکنش به حوادث را به عنوان بخشی از تعریف، طراحی و توسعه فرایندهای مأموریتی و کسب‌وکاری و سیستم‌های اطلاعاتی به حساب می‌آورند. اطلاعات مربوط به حوادث را می‌توان از منابع مختلفی به دست آورد؛ نظیر پایش ممیزی‌ها، پایش شبکه، پایش دسترسی فیزیکی، گزارش‌های کاربران و راهبران و رویدادهای گزارش‌شده از زنجیره تدارکات. سامانه مهار مؤثر حوادث شامل هماهنگی میان بسیاری از موجودیت‌های سازمانی می‌شود؛ نظیر صاحبان مأموریت‌ها و کسب‌وکار، صاحبان سیستم‌های اطلاعاتی، مقامات صدور مجوز، اداره‌های منابع انسانی، اداره‌های امنیت فیزیکی و امنیت کارکنان، دپارتمان‌های حقوقی، کارکنان عملیاتی، اداره‌های تهیه و تدارکات و بخش مدیریت (عملکردی) مخاطرات. کنترل‌های مربوطه: AU-6، CM-6، CP-2، CP-4، IR-2، IR-3، IR-8، PE-6، SC-5، SC-7، SI-3، SI-4 و SI-7.

کنترل‌های پیشرفته:

(۱) مهار حوادث / فرایندهای خودکار مهار حوادث

سازمان از سازوکارهای خودکار برای پشتیبانی فرایند مهار حوادث استفاده می‌کند.

راهنمایی تکمیلی: سیستم‌های آنلاین مدیریت حوادث، نمونه‌ای از سازوکارهای خودکاری هستند که از فرایندهای مهار حوادث پشتیانی می‌کنند.

(۲) مهار حوادث / پیکربندی دوباره و پویا

سازمان پیکربندی دوباره و پویای [اختصاص: مؤلفه‌ی سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] را به عنوان بخشی از سامانه مهار حوادث تعبیه می‌کند.

راهنمایی تکمیلی: تغییرات قوانین مسیریاب‌ها، لیست‌های کنترل دسترسی، تغییرات پارامترهای سیستم‌های شناسایی و پیشگیری از نفوذ و تغییرات قوانین فیلترینگ برای فایروال‌ها و گیت‌وی‌ها نمونه‌هایی از پیکربندی دوباره و پویا هستند. سازمان‌ها را برای اهداف مختلفی، پیکربندی دوباره و پویا را در سیستم‌های اطلاعاتی انجام می‌دهند؛ از جمله متوقف ساختن حملات، گمراه نمودن مهاجمان و جدا نگهداشتن مؤلفه‌های سیستم‌ها و به این ترتیب، محدود ساختن شدت آسیب‌های ناشی از رخنه‌ها یا حملات. با توجه به نیاز احتمالی برای واکنش سریع به منظور رسیدگی مؤثر به تهدیدات پیشرفته سایبری، سازمان‌ها چارچوب‌های زمانی برای پیکربندی دوباره سیستم‌های اطلاعاتی را در تعریف پیکربندی دوباره لحاظ می‌کنند. کنترل‌های مربوطه: AC-2، AC-4، AC-16، CM-2، CM-3 و CM-4.

(۳) مهار حوادث / تداوم عملیات‌ها

سازمان [اختصاص: دسته‌های حوادث را که توسط سازمان تعیین می‌شوند] و [اختصاص: اقدامات تعیین‌شده توسط سازمان را که باید در واکنش به دسته‌های مختلف حوادث انجام داد]، مشخص می‌نماید تا اطمینان حاصل کند که مأموریت‌های سازمانی و عملکردهای کسب‌وکار تداوم می‌یابند.

راهنمایی تکمیلی: عملکرد ناقص به دلیل خطا یا کوتاهی در طراحی و پیاده‌سازی، حملات مخرب و هدفمند و حملات مخرب و بدون هدف‌گیری نمونه‌هایی از دسته‌های حوادث هستند. تنزل‌های محترمانه، خاموشی سیستم‌های اطلاعاتی، بازگشت به حالت دستی یا فناوری‌های جایگزین که در آن‌ها، سیستم به صورتی متفاوت عمل می‌کند، به‌کارگیری تمهیدات فریبنده، جریان‌های فرعی اطلاعات یا عمل کردن در حالتی که فقط برای مواقعی در نظر گرفته شده است که سیستم‌ها تحت حمله هستند، نمونه‌هایی از اقدامات مناسب برای واکنش به حوادث هستند.

(۴) مهار حوادث / برقراری ارتباط میان اطلاعات

سازمان اطلاعات حوادث را به هر یک از واکنش‌های صورت‌گرفته مرتبط می‌سازد تا نمایی کامل از سرتاسر سازمان در خصوص آگاهی از حوادث و واکنش به حوادث به دست بیاورد.

راهنمایی تکمیلی: گاهی، ماهیت یک رویداد تهدیدآمیز، برای مثال یک حمله سایبری خصمانه، به گونه‌ای است که تنها با جمع‌آوری و کنار هم قرار دادن اطلاعات از منابع مختلف، از جمله گزارش‌های متنوع و رویه‌های گزارشی وضع‌شده توسط سازمان‌ها، می‌توان آن را تشخیص داد.

(۵) مهار حوادث / غیرفعال‌سازی خودکار سیستم‌های اطلاعاتی

سازمان یک ویژگی قابل پیکربندی را به منظور غیرفعال‌سازی خودکار سیستم‌های اطلاعاتی در صورت شناسایی [اختصاص: تخلفات امنیتی تعیین‌شده توسط سازمان] پیاده‌سازی می‌نماید.

(۶) مهار حوادث / تهدیدات خودی؛ سامانه‌های مشخص

سازمان، سامانه مهار حوادث را برای تهدیدات خودی پیاده‌سازی می‌نماید.

راهنمایی تکمیلی: با این که بسیاری از سازمان‌ها به حوادث مربوط به تهدیدات خودی در قالب بخشی از برنامه سازمانی خود برای واکنش به حوادث رسیدگی می‌کنند، این کنترل پیشرفته تأکید بیشتری روی این نوع تهدید و نیز ضرورت وجود سامانه‌های مشخص و خاص مهار حوادث (همان طوری که داخل سازمان‌ها تعیین می‌شود) برای انجام واکنش‌های مناسب و به‌موقع دارد.

(۷) مهار حوادث / تهدیدات خودی؛ هماهنگی درون‌سازمانی

سازمان سامانه مهار حوادث مربوط به تهدیدات خودی را در سراسر [اختصاص: مؤلفه‌ها یا عناصری از سازمان که توسط خود سازمان تعیین می‌شوند] هماهنگ می‌کند.

راهنمایی تکمیلی: اقدامات مهار حوادث مربوط به تهدیدات خودی (شامل آماده‌سازی، شناسایی و تجزیه و تحلیل، محصور کردن، ریشه‌کنی و بازیابی) برای مؤثر بودن، نیازمند هماهنگی نزدیک و دقیق میان مؤلفه‌ها و عناصر سازمانی مختلفی است. صاحبان مأموریت‌ها و کسب‌وکار، صاحبان سیستم‌های اطلاعاتی، مقامات صدور مجوز، اداره‌های منابع انسانی، اداره‌های امنیت فیزیکی و امنیت کارکنان، دپارتمان‌های حقوقی، کارکنان عملیاتی، اداره‌های تهیه و تدارکات و بخش مدیریت (عملکردی) مخاطرات نمونه‌هایی از این مؤلفه‌ها و عناصر هستند. به علاوه، ممکن است سازمان‌ها نیازمند حمایت خارجی از جانب آژانس‌های فدرال، آژانس‌های دولتی و آژانس‌های محلی اعمال قانون باشند.

(۸) مهار حوادث / ارتباط با سازمان‌های خارجی

سازمان خودش را با [اختصاص: سازمان‌های خارجی تعیین‌شده توسط سازمان] به منظور برقراری ارتباط میان [اختصاص: اطلاعات تعیین‌شده توسط سازمان و مربوط به حوادث] و اشتراک‌گذاری آن‌ها هماهنگ می‌نماید تا نمایی کامل و سراسری از سازمان‌های متخلف در خصوص آگاهی از حوادث و واکنش‌های مؤثرتر به حوادث به دست بیاورد.

راهنمایی تکمیلی: هماهنگی اطلاعات حوادث با سازمان‌های خارجی، نظیر شرکای مأموریتی و کسب‌وکاری، شرکای نظامی و ائتلافی، مشتریان و توسعه‌دهندگان چندرتبه‌ای، می‌تواند مزایایی چشمگیری داشته باشد. هماهنگی میان سازمان‌های مختلف با در نظر گرفتن سامانه مهار حوادث، می‌تواند به عنوان یک سامانه مهم مدیریت مخاطرات عمل نماید. این سامانه به سازمان‌ها اجازه می‌دهد تا از اطلاعات حیاتی و مهم به‌دست‌آمده از منابع مختلف، به منظور واکنش مؤثر به آن دسته از حوادث مربوط به امنیت اطلاعات که احتمالاً روی عملیات‌ها، دارایی‌ها و افراد سازمان تأثیر می‌گذارند، بهره بگیرند.

(۹) مهار حوادث / سامانه واکنش پویا

سازمان از [اختصاص: سامانه‌های واکنش پویا که توسط سازمان تعیین می‌شوند] برای واکنش مؤثر به حوادث امنیتی استفاده می‌کند.

راهنمایی تکمیلی: این کنترل پیشرفته به استقرار سامانه‌های جایگزین یا سامانه‌های جدید در زمان‌های درست و در واکنش به حوادث امنیتی (نظیر اقدامات مهاجمان در هنگام حملات سایبری خصمانه) مربوط می‌شود. این کنترل شامل سامانه‌هایی می‌شود که در سطح فرایندهای مأموریت و کسب‌وکار (نظیر فعال‌سازی فرایندهای مأموریت و کسب‌وکار جایگزین) و در سطح سیستم اطلاعاتی پیاده‌سازی می‌شوند. کنترل مربوطه: CP-10.

(۱۰) مهار حوادث / هماهنگ زنجیره تدارکات

سازمان آن دسته فعالیت‌های مهار حوادث را که به رویدادهای زنجیره تدارکات مرتبط می‌شوند، با سایر سازمان‌های درگیر در زنجیره تدارکات هماهنگ می‌کند.

راهنمایی تکمیلی: تولیدکنندگان سیستم‌ها و محصولات، یکپارچه‌کننده‌ها، سازندگان، بسته‌بندی‌کننده‌ها، گردآورنده‌ها، توزیع‌کننده‌ها، فروشندگان بزرگ و فروشندگان کوچک نمونه‌هایی از سازمان‌های درگیر در فعالیت‌های زنجیره تدارکات هستند. حملات یا رخنه‌هایی که مؤلفه‌های سیستم‌های اطلاعاتی، محصولات فناوری اطلاعات، فرایندها یا کارکنان تهیه و توسعه و فرایندهای توزیع یا تأسیسات انبارداری را درگیر می‌کنند، نمونه‌هایی از حوادث زنجیره تدارکات هستند.

مراجع: دستور اجرایی ۱۳۵۸۷ و نشریه ویژه NIST 800-61

اولویت و تخصیص به مجموعه‌های پایه:

P1	IR-4 اولویت پایین	IR-4 (1) اولویت متوسط	IR-4 (1)(4) اولویت بالا

IR-5: پایش حوادث

کنترل: سازمان حوادث امنیتی در سیستم‌های اطلاعاتی را ردگیری و مستند می‌نماید.

راهنمایی تکمیلی: حفظ و نگهداری سوابق مربوط به هر حادثه، وضعیت آن حادثه و سایر اطلاعات مرتبط و ضروری برای ممیزی قانونی، ارزشیابی جزئیات حادثه، تحولات و مهار آن حادثه از جمله موارد مستندسازی حوادث امنیتی در سیستم‌های اطلاعاتی هستند. اطلاعات مربوط به حادثه را می‌توان از منابع مختلفی به دست آورد؛ نظیر گزارش‌های مربوط به حادثه، تیم‌های واکنش به حوادث، پایش ممیزی‌ها، پایش شبکه، پایش دسترسی فیزیکی، گزارش‌های کاربران و راهبران. کنترل‌های مربوطه: AU-6، IR-8، PE-6، SC-5، SC-7، SI-3، SI-4 و SI-7.

کنترل‌های پیشرفته:

(۱) پایش حوادث / ردگیری، جمع‌آوری اطلاعات و تجزیه و تحلیل به صورت خودکار

سازمان از سازوکارهای خودکار برای کمک به ردگیری حوادث امنیتی و جمع‌آوری و تجزیه و تحلیل اطلاعات مربوط به حوادث استفاده می‌کند.

راهنمایی تکمیلی: دستگاه پایش شبکه اینشتین و پایش مراکز آنلاین واکنش به حوادث رایانه‌ای (CIRC)[۲۰۷] یا سایر پایگاه‌های داده الکترونیکی مربوط به حوادث از جمله سازوکارهای خودکار برای ردگیری حوادث امنیتی و جمع‌آوری و تجزیه و تحلیل اطلاعات مربوط به حوادث هستند. کنترل‌های مربوطه: AU-7 و IR-4.

مراجع: نشریه ویژه NIST 800-61

اولویت و تخصیص به مجموعه‌های پایه:

P1	IR-5 اولویت پایین	IR-5 اولویت متوسط	IR-5 (1) اولویت بالا

IR-6: گزارش کردن حوادث

کنترل: سازمان:

الف. کارکنان را ملزم می‌سازد تا حوادث امنیتی مشکوک را [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] به سامانه سازمانی واکنش به حوادث گزارش دهند.

ب. اطلاعات مربوط به حوادث امنیتی را [اختصاص: مقامات تعیین‌شده توسط سازمان] گزارش می‌دهد.

راهنمایی تکمیلی: هدف از این کنترل، لحاظ کردن الزامات مشخص برای گزارش کردن حوادث در هر سازمان و نیز الزامات رسمی برای گزارش کردن حوادث در آژانس‌های فدرال و سازمان‌های زیرمجموعه آن‌ها است. دریافت ایمیل‌های مشکوک که احتمالاً حاوی کدهای مخرب هستند، نمونه‌ای از حوادث امنیتی مشکوک است. انواع حوادثی امنیتی که باید گزارش شوند، محتوا و تقویم زمانی گزارش‌ها و مقامات منصوب‌شده برای گزارش‌ها، بازگوکننده قوانین، دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها و راهنمایی‌های فدرال مربوطه هستند. خط‌مشی فعلی فدرال، همه آژانس‌های فدرال (مگر آن‌هایی که به طور مشخص این الزامات معاف شده

[207] Computer Incident Response Centers

باشند) را ملزم می‌نماید که حوادث امنیتی را در مدت زمانی مشخص به تیم آمادگی برای وضعیت‌های رایانه‌ای اضطراری آمریکا (US-CERT)[۲۰۸] گزارش دهند؛ این مدت زمانی مشخص در راهنمای عملیاتی US-CERT برای مهار حوادث افتا در آژانس‌های فدرال[۲۰۹] تعیین می‌شود. کنترل‌های مربوطه: IR-4، IR-5 و IR-8.

کنترل‌های پیشرفته:

(۱) گزارش کردن حوادث / گزارش خودکار

سازمان از سازوکارهای خودکار برای کمک به گزارش کردن حوادث امنیتی استفاده می‌کند.

راهنمایی تکمیلی: کنترل مربوطه: IR-7.

(۲) گزارش کردن حوادث / آسیب‌پذیری‌های مرتبط با حوادث

سازمان آن دسته از آسیب‌پذیری‌های سیستم‌های اطلاعاتی را که با حوادث امنیتی گزارش‌شده مرتبط هستند، به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] گزارش می‌کند.

(۳) گزارش کردن حوادث / هماهنگی با زنجیره تدارکات

سازمان اطلاعات مربوط به حوادث امنیتی را در اختیار سایر سازمان‌های درگیر در زنجیره تدارکات آن دسته از سیستم‌های اطلاعاتی یا مؤلفه‌های سیستم‌های اطلاعاتی را که با آن حوادث مرتبط هستند، قرار می‌دهد. تولیدکنندگان سیستم‌ها و محصولات، یکپارچه‌کننده‌ها، سازندگان، بسته‌بندی‌کننده‌ها، گردآورنده‌ها، توزیع‌کننده‌ها، فروشندگان بزرگ و فروشندگان کوچک نمونه‌هایی از سازمان‌های درگیر در فعالیت‌های زنجیره تدارکات هستند. حملات یا رخنه‌هایی که مؤلفه‌های سیستم‌های اطلاعاتی، محصولات فناوری اطلاعات، فرایندها یا کارکنان تهیه و توسعه و فرایندهای توزیع یا تأسیسات انبارداری را درگیر می‌کنند، نمونه‌هایی از حوادث زنجیره تدارکات هستند. سازمان‌ها تعیین می‌کنند که چه اطلاعاتی برای اشتراک‌گذاری مناسب هستند. این امر با توجه به ارزشی که این سازمان‌ها از پشتیبانی سازمان‌های خارجی به دست می‌آورند و نیز با در نظر گرفتن آسیب‌های احتمالی ناشی از انتشار اطلاعات حساس به سازمان‌های غیرخودی که اعتمادپذیری آن‌ها چندان ثابت‌شده نیست، تعیین می‌شود.

مراجع: نشریه ویژه NIST 800-61 و آدرس وب: http://www.us-cert.gov

[208] United States Computer Emergency Readiness Team
[209] US-CERT Concept of Operations for Federal Cyber Security Incident Handling

اولویت و تخصیص به مجموعه‌های پایه:

P1	IR-6 اولویت پایین	(1) IR-6 اولویت متوسط	(1) IR-6 اولویت بالا

IR-7: کمک‌رسانی در واکنش به حوادث

کنترل: سازمان یک منبع پشتیبانی برای واکنش به حوادث مشخص می‌کند. این منبع بخشی از سامانه سازمانی واکنش به حوادث است که به کاربران سیستم‌های اطلاعاتی در خصوص مهار و گزارش حوادث امنیتی توصیه و کمک می‌نماید.

راهنمایی تکمیلی: بخش پشتیبانی، گروه‌های کمک‌رسانی و دسترسی به خدمات ممیزی قانونی در هنگام نیاز، نمونه‌هایی از منابع پشتیبانی برای واکنش به حوادث هستند که توسط سازمان مشخص می‌شوند. کنترل‌های مربوطه: AT-2، IR-4، IR-6، IR-8 و SA-9.

کنترل‌های پیشرفته:

(۱) کمک‌رسانی در واکنش به حوادث / پشتیبانی خودکار برای آماده‌ی کار بودن اطلاعات و منابع پشتیبانی

سازمان از سازوکارهای خودکار برای افزایش آماده‌ی کار بودن اطلاعات و پشتیبانی مرتبط با واکنش به حوادث استفاده می‌کند.

راهنمایی تکمیلی: سازوکارهای خودکار می‌توانند یک سامانه درخواست و دریافت[۲۱۰] برای کاربران فراهم کنند که آن‌ها بتوانند از کمک‌های واکنش به حوادث برخوردار شوند. برای مثال، افراد ممکن است به وب‌سایتی دسترسی داشته باشند که به آن‌ها اجازه می‌دهد در سامانه کمک‌رسانی کوئری انجام دهند؛ یا برعکس، ممکن است سامانه کمک‌رسانی از این قابلیت برخوردار باشد که به صورت پیش‌کنشگرانه اطلاعات را در قالب عملی برای افزایش درک کاربران از پشتیبانی و سامانه‌های واکنشی فعلی، به کاربران ارسال نماید (توزیع عمومی یا هدفمند).

(۲) کمک‌رسانی در واکنش به حوادث / هماهنگی با سازمان‌های خارجی

سازمان:

[210] Push and Pull

(الف). یک رابطه مستقیم و همکارانه میان سامانه واکنش به حوادث خودش و تأمین‌کنندگان خارجی سامانه حفاظت از سیستم‌های اطلاعاتی برقرار می‌نماید.

(ب). اعضای تیم سازمانی واکنش به حوادث را به تأمین‌کنندگان خارجی معرفی می‌کند.

راهنمایی تکمیلی: برنامه دفاع از شبکه‌های رایانه‌ای[۲۱۱] در وزارت دفاع آمریکا نمونه‌ای از تأمین‌کنندگان خارجی سامانه حفاظت از سیستم‌های اطلاعاتی است. تأمین‌کنندگان خارجی به حفاظت، پایش، تجزیه و تحلیل، شناسایی و واکنش به فعالیت‌های غیرمجاز در سیستم‌های اطلاعاتی و شبکه‌های سازمانی کمک می‌نمایند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	IR-7 اولویت پایین	IR-7 (1) اولویت متوسط	IR-7 (1) اولویت بالا

IR-8: طرح و نقشه واکنش به حوادث

کنترل: سازمان:

الف. یک نقشه برای واکنش به حوادث تهیه می‌کند که از ویژگی‌های زیر برخوردار است:

۱. یک برنامه اجرایی برای پیاده‌سازی سامانه واکنش به حوادث برای سازمان تعیین می‌کند.

۲. ساختار و سازماندهی سامانه واکنش به حوادث را توصیف می‌کند.

۳. یک رویکرد حرفه‌ای در خصوص جایگاه سامانه واکنش به حوادث در ساختار کلی سازمان و نحوه تعامل آن ارائه می‌کند.

۴. الزامات منحصربه‌فرد سازمان را که به مأموریت، اندازه، ساختار و عملکردها مربوط می‌شوند، رعایت می‌کند.

۵. حوادثی را که باید گزارش شوند، تعیین می‌کنند.

۶. معیارهایی برای سنجش سامانه واکنش به حوادث در سازمان تعیین می‌کند.

[211] Computer Network Defense

۷. منابع و پیشتیبانی مدیریتی لازم برای تعمیر و نگهداری مؤثر و تکمیل و بهبود سامانه واکنش به حوادث را تعیین می‌کند.

۸. توسط [اختصاص: نقش‌ها و کارکنان تعیین‌شده توسط سازمان] بازبینی و تأیید می‌شود.

ب. کپی‌هایی از نقشه واکنش به حوادث را در اختیار [اختصاص: کارکنان تعیین‌شده توسط سازمان برای واکنش به حوادث (که به واسطه نام یا نقش فرد مشخص می‌شوند) و عناصر سازمانی] قرار می‌دهد.

پ. طرح و نقشه واکنش به حوادث را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند.

ت. به منظور مطابقت با تغییرات یا مشکلاتی در حین پیاده‌سازی، اجرا یا تست طرح و نقشه واکنش به حوادث بروز می‌کند، آن را به‌روزرسانی می‌نماید.

ث. تغییرات طرح و نقشه واکنش به حوادث را به [اختصاص: کارکنان تعیین‌شده توسط سازمان برای واکنش به حوادث (که به واسطه نام یا نقش فرد مشخص می‌شوند) و عناصر سازمانی] اطلاع می‌دهد.

ج. از طرح و نقشه واکنش به حوادث در مقابل افشاشدن و تغییرات غیرمجاز حفاظت می‌کند.

راهنمایی تکمیلی: بسیار مهم است که سازمان‌ها رویکردی هماهنگ و مدیریت‌شده را برای واکنش به حوادث تهیه و پیاده‌سازی نمایند. مأموریت‌ها، عملکردهای کسب‌وکار، راهبردها، مقاصد و اهداف سازمانی برای واکنش به حوادث به تعیین ساختار سامانه‌های واکنش به حوادث کمک می‌نمایند. در قالب بخشی از یک سامانه جامع واکنش به حوادث، سازمان‌ها اطلاعات را با سازمان‌های خارجی هماهنگ می‌کنند و به اشتراک می‌گذارند؛ نظیر سرویس‌دهندگان خارجی و سازمان‌های درگیر در زنجیره تدارکات برای سیستم‌های اطلاعاتی سازمانی. کنترل‌های مربوطه: MP-2، MP-4 و MP-5.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: نشریه ویژه NIST 800-61

اولویت و تخصیص به مجموعه‌های پایه:

P1	IR-8 اولویت پایین	IR-8 اولویت متوسط	IR-8 اولویت بالا

IR-9: واکنش به انتشار اطلاعات

کنترل: سازمان به شکل‌های زیر نسبت به انتشار اطلاعات واکنش می‌دهد:

الف. شناسایی دقیق اطلاعاتی که در جریان آلودگی سیستم اطلاعاتی به این اطلاعات، انتشار یافته‌اند.

ب. هشدار دادن به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] در خصوص انتشار اطلاعات از طریق شیوه‌ای که به این انتشار ارتباطی نداشته باشد.

پ. جداسازی سیستم‌های اطلاعاتی یا مؤلفه‌های سیستمی آلوده‌شده به اطلاعات.

ت. حذف و پاک کردن اطلاعات از سیستم‌های اطلاعاتی یا مؤلفه‌های آلوده‌شده به اطلاعات.

ث. شناسایی سایر سیستم‌های اطلاعاتی یا مؤلفه‌های سیستمی که امکان آلودگی بعدی آن‌ها به اطلاعات وجود دارد.

ج. انجام سایر [اختصاص: اقدامات تعیین‌شده توسط سازمان].

راهنمایی تکمیلی: انتشار اطلاعات به مواردی اطلاق می‌شود که اطلاعات محرمانه یا حساس به صورت غیرعمدی یا اتفاقی به برخی از سیستم‌های اطلاعاتی منتقل می‌شوند که مجوز پردازش چنین اطلاعاتی را ندارند. چنین مواردی از انتشار اطلاعات اغلب زمانی رخ می‌دهد که مجموعه‌ای از اطلاعات به یک سیستم اطلاعاتی منتقل می‌شود؛ اطلاعاتی که در ابتدا تصور می‌شود که حساسیت پایینی دارند، اما بعداً مشخص می‌شود که حساسیت بیشتری دارند. در این موقعیت، انجام اقدامات اصلاحی الزامی است. مآهیت واکنش سازمانی به طور عمومی به درجه حساسیت اطلاعات انتشاریافته (نظیر طبقه‌بندی امنیتی یا سطح محرمانگی)، قابلیت‌های امنیتی سیستم اطلاعاتی، ماهیت خاص رسانه ذخیره‌سازی آلوده‌شده به اطلاعات و مجوزهای دسترسی (نظیر تأییدیه‌های امنیتی) افرادی که مجوز دسترسی به سیستم آلوده‌شده به اطلاعات را دارند، بستگی دارد. روش‌های به‌کاررفته برای مخابره اطلاعات درباره انتشار رخ‌داده شامل روش‌هایی که به صورت مستقیم به این اتفاق مربوط می‌شوند، نمی‌گردد تا به این ترتیب از مخاطرات انتشار بیشتر آلودگی اطلاعاتی پیش از جداسازی و پاک‌سازی آن به حداقل برسد.

کنترل‌های پیشرفته:

(۱) واکنش به انتشار اطلاعات / کارکنان مسئول

سازمان [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] را به مسئولیت‌های مرتبط با واکنش به انتشار اطلاعات منصوب می‌کند.

(۲) واکنش به انتشار اطلاعات / آموزش

سازمان آموزش‌های مرتبط با واکنش به انتشار اطلاعات را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] ارائه می‌دهد.

(۳) واکنش به انتشار اطلاعات / عملیات‌های پس از انتشار اطلاعات

سازمان [اختصاص: رویه‌هایی را که توسط سازمان تعیین می‌شوند]، به این منظور پیاده‌سازی می‌کند که اطمینان حاصل شود کارکنانی که فعالیت آن‌ها تحت تأثیر انتشاراطلاعات قرار گرفته است، می‌توانند در طول زمان اصلاح شدن سیستم‌های آلوده‌شده به اطلاعات به وظایف اختصاص‌یافته خود ادامه دهند.

راهنمایی تکمیلی: انجام اقدامات اصلاحی روی سیستم‌های اطلاعاتی آلوده‌شده در اثر انتشار اطلاعات ممکن است بسیار وقت‌گیر باشند. در طول این زمان‌ها، ممکن است کارکنان به سیستم‌های آلوده‌شده به اطلاعات دسترسی نداشته باشند و این امر ممکن است به صورت جدی روی توانایی آن‌ها برای انجام کسب‌وکار سازمانی خود تأثیر بگذارد.

(۴) واکنش به انتشار اطلاعات / افشا شدن اطلاعات برای کارکنان غیرمجاز

سازمان [اختصاص: ضامن‌های امنیتی تعیین‌شده توسط سازمان] را برای کارکنانی به کار می‌گیرد که اطلاعاتی خارج از مجوزهای دسترسی اختصاص‌یافته به آن‌ها برایشان افشا شده است.

راهنمایی تکمیلی: یکی از نمونه‌های ضامن‌های امنیتی، مطلع ساختن کارکنانی که اطلاعات انتشاریافته برای آن‌ها افشا شده‌اند، نسبت به قوانین، بخش‌نامه‌ها، خط‌مشی‌ها و یا مقررات فدرال مربوط به آن اطلاعات و محدودیت‌های ناشی از افشا شدن آن اطلاعات برای آن‌ها است.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

IR-10: تیم یکپارچه تجزیه و تحلیل امنیت اطلاعات

کنترل: سازمان تیمی یکپارچه از تحلیلگران ممیزی قانونی و کدهای مخرب، توسعه‌دهندگان ابزارها و کارکنان عملیات‌های بلادرنگ تشکیل می‌دهد.

راهنمایی تکمیلی: داشتن تیمی یکپارچه برای واکنش به حوادث، اشتراک‌گذاری اطلاعات را تسهیل می‌کند. چنین تیمی به کارکنان سازمانی، از جمله توسعه‌دهندگان، افراد مسئول پیاده‌سازی و متصدی‌ها، اجازه می‌دهد تا از دانش این تیم درباره تهدیدات به منظور پیاده‌سازی تمهیدات دفاعی بهره بگیرند. این تمهیدات به سازمان‌ها کمک می‌کنند تا به صورت مؤثر از نفوذها جلوگیری نمایند. به علاوه، این تیم در شناسایی سریع نفوذها، طراحی روندهای مناسب برای کاهش آسیب‌ها و استقرار تمهیدات دفاعی مؤثر نقش مثبت دارد. برای مثال، هنگامی که یک نفوذ شناسایی شود، تیم یکپارچه تحلیل امنیتی به سرعت یک واکنش مناسب تدوین می‌کند تا متصدیان پیاده‌سازی نمایند، حادثه جدید را با اطلاعات مربوط به نفوذهای گذشته ارتباط می‌دهند و رشد و توسعه پیوسته هوشمندی و داده‌های پردازش‌شده را تقویت می‌کنند. این امر به تیم تحلیلی اجازه می‌دهد تا TTPهای مهاجمی را که با سرعت عملیات یا مأموریت‌هایی خاص و عملکردهای کسب‌وکار خاصی پیوند خورده‌اند، شناسایی نمایند و نیز اقدامات واکنشی را به نحوی تعیین کنند که در مأموریت‌ها و عملیات‌های کسب‌وکار اختلالی ایجاد نشود. در بهترین حالت، تیم‌های تحلیل امنیت اطلاعات درون سازمان‌ها پخش و توزیع می‌شوند تا انعطاف‌پذیری و مقاومت آن‌ها بهبود یابد.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

خانواده: حفاظت از رسانه‌ها

CP-1: خط‌مشی و رویه‌های حفاظت از رسانه‌ها

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۱۵. خط‌مشی حفاظت از رسانه‌ها شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و

۱۶. رویه‌های تسهیل پیاده‌سازی خط‌مشی حفاظت از رسانه‌ها و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۱۵. خط‌مشی حفاظت از رسانه‌ها؛ و

۱۶. رویه‌های حفاظت از رسانه‌ها.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده MP را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: شماره‌های ویژه NIST 800-12, 800-100.

اولویت و تخصیص به مجموعه‌های پایه:

P1	MP-1 اولویت پایین	MP-1 اولویت متوسط	MP-1 اولویت بالا

MP-2: **دسترسی به رسانه‌ها**

کنترل: سازمان دسترسی به [اختصاص: انواع دیجیتالی و یا غیردیجیتالی از رسانه‌ها که توسط سازمان تعریف می‌شود] را برای [اختصاص: کارکنان و نقش‌های تعیین‌شده توسط سازمان] محدود می‌سازد.

راهنمایی تکمیلی: رسانه‌های متعلق به سیستم‌های اطلاعاتی شامل رسانه‌های دیجیتالی و رسانه‌های غیردیجیتالی می‌شوند. از جمله رسانه‌های دیجیتالی می‌توان به دیسکت‌ها، نوارهای مغناطیسی، هارد دیسک‌های خارجی و جداشدنی، فلش درایو، دیسک‌های فشرده، دیسک‌های ویدیوی دیجیتالی اشاره کرد. از جمله رسانه‌های غیردیجیتالی می‌توان به کاغذ و میکروفیلم اشاره کرد. به عنوان مثال، عدم‌امکان دسترسی به سوابق پزشکی بیماران در یک بیمارستان اجتماعی، مگر این که فردی که درخواست دسترسی دارد یکی از کارکنان بهداشتی و درمانی و دارای مجوز باشد، نمونه‌ای از محدود کردن دسترسی به رسانه‌های غیردیجیتالی است. به عنوان مثال، محدود کردن دسترسی به جزئیات طراحی‌ها که در دیسک‌های فشرده در کتابخانه رسانه‌ها ذخیره شده‌اند، فقط برای مدیر پروژه و افراد تیم توسعه، نمونه‌ای از محدود کردن دسترسی به رسانه‌های دیجیتالی است. کنترل‌های مربوطه: AC-3، IA-2، MP-4، PE-2، PE-3 و PL-2

کنترل‌های پیشرفته:

(۱) دسترسی به رسانه‌ها / دسترسی محدودشده خودکار

[حذف شد: به بخش (2) MP-4 منتقل شد.]

(۲) دسترسی به رسانه‌ها / حفاظت از طریق رمزنگاری

[حذف شد: به بخش SC-28 منتقل شد.]

مراجع: نشریه FIPS 199، نشریه ویژه NIST 800-111

اولویت و تخصیص به مجموعه‌های پایه:

P2	MP-2 اولویت پایین	MP-2 اولویت متوسط	MP-2 اولویت بالا

MP-3: علامت‌گذاری رسانه‌ها

کنترل: سازمان:

الف. رسانه‌های متعلق به سیستم‌های اطلاعاتی را برای نشان دادن محدودیت‌های توزیع، برخورد با هشدارها و (در صورت وجود،) نشانه‌های امنیتی مربوط به اطلاعات علامت‌گذاری می‌کند: و

ب. [اختصاص: انواعی از رسانه‌های متعلق به سیستم‌های اطلاعاتی را که توسط سازمان تعریف می‌شوند]، از علامت‌گذاری معاف می‌کند، تا زمانی که این رسانه‌ها داخل [اختصاص: مناطق کنترل‌شده که توسط سازمان تعریف می‌شوند]، باقی بمانند.

راهنمایی تکمیلی:عبارت «علامت‌گذاری امنیتی» به استفاده ازمشخصه‌های امنیتی قابل خواندن توسط انسان اشاره دارد. عبارت «برچسب‌گذاری امنیتی» به استفاده از مشخصه‌های امنیتی با در نظر گرفت ساختارهای داده داخلی در سیستم‌های اطلاعاتی اشاره دارد (به بخش AC-16 رجوع شود). رسانه‌های متعلق به سیستم‌های اطلاعاتی شامل رسانه‌های دیجیتالی و رسانه‌های غیردیجیتالی می‌شوند. از جمله رسانه‌های دیجیتالی می‌توان به دیسکت‌ها، نوارهای مغناطیسی، هارد دیسک‌های خارجی و جداشدنی، فلش درایو، دیسک‌های فشرده، دیسک‌های ویدیوی دیجیتالی اشاره کرد. از جمله رسانه‌های غیردیجیتالی می‌توان به کاغذ و میکروفیلم اشاره کرد. عموماً علامت‌گذاری امنیتی برای آن دسته از رسانه‌های حاوی اطلاعات که سازمان برای استفاده در بخش‌های عمومی یا انتشار به صورت عمومی مشخص کرده است، الزامی نیست. اما با این حال، ممکن است برخی از سازمان‌ها علامت‌گذاری اطلاعات عمومی برای نشان دادن امکان انتشار عمومی آن اطلاعات را الزامی نمایند. علامت‌گذاری رسانه‌های متعلق به سیستم‌های اطلاعاتی بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، راهنمایی‌ها و قوانین فدرال هستند. کنترل‌های مربوطه: AC-16، PL-2 و RA-3.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: نشریه FIPS 199.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب‌نشده، اولویت پایین	MP-3 اولویت متوسط	MP-3 اولویت بالا

MP-4: ذخیره‌سازی رسانه‌ها

کنترل: سازمان:

الف. به صورت فیزیکی [اختصاص: انواع دیجیتالی و یا غیردیجیتالی از رسانه‌ها که توسط سازمان تعریف می‌شود] را کنترل می‌کند و آن‌ها را در [اختصاص: مناطق کنترل‌شده که توسط سازمان تعریف می‌شوند] به صورت امن و مطمئن ذخیره می‌کند.

ب. از رسانه‌های متعلق به سیستم‌های اطلاعاتی حفاظت می‌کند تا زمانی که این رسانه‌ها با استفاده از تجهیزات، شگردها و رویه‌های مورد تأیید پاکسازی شوند.

راهنمایی تکمیلی: رسانه‌های متعلق به سیستم‌های اطلاعاتی شامل رسانه‌های دیجیتالی و رسانه‌های غیردیجیتالی می‌شوند. از جمله رسانه‌های دیجیتالی می‌توان به دیسکت‌ها، نوارهای مغناطیسی، هارد دیسک‌های خارجی و جداشدنی، فلش درایو، دیسک‌های فشرده، دیسک‌های ویدیوی دیجیتالی اشاره کرد. از جمله رسانه‌های غیردیجیتالی می‌توان به کاغذ و میکروفیلم اشاره کرد. مدیریت انبار، حصول اطمینان از برقراری رویه‌هایی برای فراهم کردن امکان خارج کردن و بازگرداندن رسانه‌ها به کتابخانه رسانه‌ها توسط افراد و حفظ پاسخگویی برای همه رسانه‌های ذخیره‌شده نمونه‌هایی از کنترل فیزیکی رسانه‌های متعلق به سیستم‌های اطلاعاتی هستند. کشو، میز و کمدهای قفل‌شده و کتابخانه رسانه کنترل‌شده نمونه‌هایی از ذخیره‌سازی امن هستند. نوع ذخیره‌سازی رسانه‌ها با طبقه‌بندی امنیتی و یا دسته‌بندی اطلاعات موجود در آن رسانه‌ها مطابق است. مناطق کنترل‌شده، مناطقی هستند که سازمان‌ها به منظور مطابق با الزامات تعیین‌شده برای حفاظت از اطلاعات و سیستم‌های اطلاعاتی، از ضامن‌های فیزیکی و مبتنی بر رویه‌ها در حد کافی برای آن‌ها استفاده می‌کند. برای آن دسته از رسانه‌های حاوی اطلاعات که سازمان مشخص کرده است برای بخش عمومی قابل استفاده هستند یا امکان انتشار عمومی دارند یا در صورت دست یافتن افرادی غیر از کارکنان مجاز به آن‌ها، باید تأثیرات نامطلوب آن‌ها روی سازمان یا افراد در حد صفر یا کم باشد، ممکن است ضامن‌های کمتری نیاز باشد. در این شرایط، کنترل‌های دسترسی فیزیکی تمهیدات حفاظتی را در حد کفایت تأمین می‌نمایند. کنترل‌های مربوطه: CP-6، CP-9، MP-2، MP-7 وPE-3.

کنترل‌های پیشرفته:

(۱) دسترسی به رسانه‌ها / حفاظت از طریق رمزنگاری

[حذف شد: به بخش SC-28 (1) منتقل شد.]

(۲) دسترسی به رسانه‌ها / دسترسی محدودشده خودکار

سازمان از سازوکارهای خودکار به منظور محدود کردن دسترسی به مناطق ذخیره‌سازی رسانه‌ها و نیز به منظور کنترل ممیزی موارد تلاش برای دسترسی و دسترسی‌های داده‌شده استفاده می‌کند.

راهنمایی تکمیلی:

به عنوان نمونه‌ای از سازوکارهای خودکار می‌توان به قرار دادن صفحه‌کلید در ورودی‌های مناطق ذخیره‌سازی رسانه‌ها اشاره کرد. کنترل‌های مربوطه: AU-2، AU-9، AU-6 و AU-12.

مراجع: نشریه FIPS 199، نشریه‌های ویژه NIST 800-56, NIST 800-57, NIST 800-111

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	MP-4 اولویت متوسط	MP-4 اولویت بالا

MP-5: **جابجایی رسانه‌ها**

کنترل: سازمان:

الف. از [اختصاص: انواعی از رسانه‌های متعلق به سیستم‌های اطلاعاتی را که توسط سازمان تعریف می‌شوند] در طول جابجایی در خارج از مناطق کنترل‌شده، با استفاده از [اختصاص: ضامن‌های امنیتی که توسط سازمان تعریف می‌شوند] حفاظت می‌کند.

ب. پاسخگویی رسانه‌های متعلق به سیستم‌های اطلاعاتی را در طول جابجایی در خارج از مناطق کنترل‌شده حفظ می‌کند.

پ. فعالیت‌های مرتبط با جابجایی رسانه‌های متعلق به سیستم‌های اطلاعاتی را مستند می‌نماید.

ت. فعالیت‌های مرتبط با جابجایی رسانه‌های متعلق به سیستم‌های اطلاعاتی را به کارکنان مجاز محدود می‌سازد.

راهنمایی تکمیلی: رسانه‌های متعلق به سیستم‌های اطلاعاتی شامل رسانه‌های دیجیتالی و رسانه‌های غیردیجیتالی می‌شوند. از جمله رسانه‌های دیجیتالی می‌توان به دیسکت‌ها، نوارهای مغناطیسی، هارد دیسک‌های خارجی و جداشدنی، فلش درایو، دیسک‌های فشرده، دیسک‌های ویدیوی دیجیتالی اشاره کرد. از جمله رسانه‌های غیردیجیتالی می‌توان به کاغذ و میکروفیلم اشاره کرد. این کنترل به دستگاه‌های همراه با قابلیت ذخیره‌سازی اطلاعات (نظیر گوشی‌های هوشمند، تبلت‌ها و کتابخوان‌های الکترونیکی) که به خارج از

مناطق کنترل‌شده برده می‌شوند، نیز اطلاق می‌شود. مناطق کنترل‌شده، مناطقی هستند که سازمان‌ها به منظور مطابق با الزامات تعیین‌شده برای حفاظت از اطلاعات و یا سیستم‌های اطلاعاتی، از ضامن‌های فیزیکی و یا ضامن‌های مبتنی بر رویه‌ها در حد کافی برای آن‌ها استفاده می‌کند.

ضامن‌های فیزیکی و فنی رسانه‌ها با طبقه‌بندی امنیتی یا دسته‌بندی اطلاعات موجود در آن رسانه‌ها مطابق است. محفظه‌های قفل‌شده و رمزنگاری نمونه‌هایی از ضامن‌های به‌کاررفته برای رسانه‌ها در طول جابجایی هستند. بسته به سازوکارهای به‌کاررفته، سازوکارهای رمزنگاری می‌توانند تمهیداتی برای حفاظت از محرمانگی و یکپارچگی فراهم نمایند. فعالیت‌های مرتبط با جابجایی عبارتند از خود عمل جابجایی و نیز فعالیت‌هایی نظیر تحویل رسانه‌ها برای جابجایی و اطمینان از ورود رسانه‌ها به فرایندهای جابجایی صحیح. در مورد خود عمل جابجایی، کارکنان مجاز برای جابجایی و حمل ممکن است افرادی خارج از سازمان (نظیر کارکنان اداره پست یا یک شرکت بازرگانی یا شرکت تحویل) باشند. محدود ساختن فعالیت‌های جابجایی به کارکنان مجاز و ردگیری و یا کسب سوابق صریح فعالیت‌های جابجایی در هنگام انتقال رسانه‌ها در سیستم جابجایی به منظور پیشگیری از مفقود شدن، تخریب یا دستکاری و شناسایی این موارد، نمونه‌هایی از حفظ پاسخگویی رسانه‌ها در طول جابجایی هستند. به منظور برخورداری از انعطاف‌پذیری در تعریف روش‌های گوناگون ثبت سوابق برای شکل‌های مختلف جابجایی رسانه‌ها، به عنوان بخشی از یک سیستم کلی برای سوابق مربوط به جابجایی‌ها، سازمان‌ها الزاماتی برای مستندسازی فعالیت‌های مرتبط با جابجایی رسانه‌های متعلق به سیستم‌های اطلاعاتی تعیین می‌کنند که با ارزیابی‌های سازمانی از مخاطرات تطابق دارند. کنترل‌های مربوطه: AC-19، CP-9، MP-3، MP-4، RA-3، SC-8، SC-13 و SC-28.

کنترل‌های پیشرفته:

(۱) جابجایی رسانه‌ها / حفاظت در خارج از مناطق کنترل‌شده

[حذف شد: به بخش MP-5 منتقل شد.]

(۲) جابجایی رسانه‌ها / مستندسازی فعالیت‌ها

[حذف شد: به بخش MP-5 منتقل شد.]

(۳) جابجایی رسانه‌ها / سرپرست‌ها

سازمان از یک سرپرست مشخص در طول جابجایی رسانه‌های متعلق به سیستم‌های اطلاعاتی در خارج از مناطق کنترل‌شده استفاده می‌کند.

راهنمایی تکمیلی: سرپرست‌های مشخص، سازمان را از موارد مشخص تماس در طول فرایند جابجایی رسانه‌ها آگاه می‌نمایند و پاسخگویی فردی را تسهیل می‌کنند. تا زمانی که هویت سرپرست در همه زمان‌ها مشخص و بدون ابهام است، امکان انتقال مسئولیت‌های سرپرستی از یک فرد به فرد دیگر وجود دارد.

(۴) جابجایی رسانه‌ها / حفاظت از طریق رمزنگاری

سیستم اطلاعاتی به منظور حفاظت از محرمانگی و یکپارچگی اطلاعات ذخیره‌شده در رسانه‌های دیجیتالی در طول جابجایی در خارج از مناطق کنترل‌شده، از پیاده‌سازی سازوکارهای رمزنگاری بهره می‌گیرد.

راهنمایی تکمیلی: این کنترل پیشرفته هم به دستگاه‌های ذخیره‌سازی قابل حمل (نظیر حافظه‌های USB، دیسک‌های فشرده، دیسک‌های ویدیوی دیجیتالی، هارد دیسک‌های خارجی و جداشدنی) و هم به دستگاه‌های همراه با قابلیت ذخیره‌سازی (نظیر گوشی‌های هوشمند، تبلت‌ها و کتابخوان‌های الکترونیکی) اطلاق می‌شود. کنترل‌های مربوطه: MP-2

مراجع: نشریه FIPS 199، نشریه ویژه NIST 800-60

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	MP-5 (4) اولویت متوسط	MP-5 (4) اولویت بالا

MP-6: پاکسازی رسانه‌ها

کنترل: سازمان:

الف. [اختصاص: رسانه‌های متعلق به سیستم‌های اطلاعاتی که توسط سازمان تعیین می‌شوند] را پیش از دفع، خارج کردن از کنترل سازمان یا تخصیص برای استفاده مجدد، با استفاده از [اختصاص: رویه‌ها و شگردهای پاکسازی که توسط سازمان تعریف می‌شوند] مطابق با استانداردها و خط‌مشی‌های سازمانی و فدرال مربوطه پاکسازی می‌کند.

ب. از سازوکارهای پاکسازی با قدرت و یکپارچگی مطابق با طبقه‌بندی امنیتی یا دسته‌بندی اطلاعات استفاده می‌کند.

راهنمایی تکمیلی: این کنترل به همه رسانه‌های متعلق به سیستم‌های اطلاعاتی، هم دیجیتال و هم غیردیجیتال، که برای دفع یا استفاده مجدد در نظر گرفته شده‌اند، فارغ از این که این رسانه‌ها جداشدنی هستند یا خیر، اطلاق می‌شود. رسانه‌هایی که در اسکنرها، دستگاه‌های کپی، پرینتر، لپتاپ‌ها، ایستگاه‌های رایانه‌ای، مؤلفه‌های شبکه و دستگاه‌های همراه نمونه‌هایی از این مطلب هستند. فرایند پاکسازی اطلاعات را به نحوی از رسانه‌ها حذف می‌کند که این اطلاعات قابل دریافت یا بازسازی نباشند. شگردهای پاکسازی، از جمله حذف، خالص‌سازی، حذف از طریق رمزنگاری و تخریب، از افشا شدن اطلاعات به افراد غیرمجاز در صورت استفاده مجدد یا دفع رسانه‌ها پیشگیری می‌کند. سازمان‌ها روش‌های ناسب پاکسازی را تعیین می‌کنند؛ اما در برخی موارد، که روش‌های دیگر برای پاکسازی رسانه‌ها مناسب نیستند، تخریب رسانه‌ها ضروری است. سازمان‌ها می‌توانند هر یک از شگردها و رویه‌های تأییدشده برای پاکسازی را به اختیار خود به منظور پاکسازی آن دسته از رسانه‌های حاوی اطلاعات انتخاب نمایند که برای استفاده در بخش عمومی در نظر گرفته شده‌اند، قابلیت انتشار عمومی دارند یا در صورت استفاده مجدد یا دفع آن‌ها، هیچ گونه تأثیر نامطلوبی برای سازمان یا افراد ندارند. حذف ضمیمه‌های محرمانه از اسنادی که به خودی خود غیرمحرمانه هستند یا نگارش مجدد قسمت‌ها یا واژه‌های انتخابی از یک سند به صورتی که غیرقابل درک باشند و نتیجه آن همانند حذف آن قسمت‌ها یا واژه‌ها از سند باشد، نمونه‌هایی از پاکسازی رسانه‌های غیردیجیتال هستند. استانداردها و خط‌مشی‌های NSA، فرایند پاکسازی رسانه‌های حاوی اطلاعات محرمانه را کنترل می‌کنند. کنترل‌های مربوطه: MA-2، MA-4، RA-3 و SC-4.

کنترل‌های پیشرفته:

(۱) پاکسازی رسانه‌ها / بازبینی، موافقت، ردگیری، مستندسازی، تأیید نهایی

سازمان فعالیت‌های پاکسازی و دفع رسانه‌ها را بازبینی، انتخاب، ردگیری، مستند و تأیید می‌نماید.

راهنمایی تکمیلی: سازمان‌ها رسانه‌هایی را که قرار است پاکسازی شوند، بازبینی و تأیید می‌کند تا از مطابقت با خط‌مشی‌های نگهداری سوابق اطمینان حاصل نمایند. ثبت کارکنانی که فعالیت‌های پاکسازی و دفع را بازبینی و تأیید کرده‌اند، ثبت انواع رسانه‌هایی که پاکسازی شده‌اند، ثبت فایل‌هایی که در آن رسانه‌ها ذخیره شده‌اند، ثبت روش‌های پاکسازی به‌کاررفته، ثبت تاریخ و زمان فعالیت‌های پاکسازی انجام‌گرفته، ثبت کارکنانی فعالیت پاکسازی را انجام داده‌اند، ثبت فعالیت‌های مربوط به وظیفه تأیید، ثبت کارکنانی که وظیفه تأیید را انجام داده‌اند و ثبت فعالیت‌های دفعی انجام‌شده از جمله فعالیت‌های ردگیری و مستندسازی هستند. سازمان‌ها باید پیش از دفع رسانه‌ها، تأیید نمایند که پاکسازی انجام‌شده مؤثر بوده است. کنترل‌های مربوطه: SI-12.

(۲) پاکسازی رسانه‌ها / تست کردن تجهیزات

سازمان رویه‌ها و تجهیزات پاکسازی را در [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] تست می‌کنند تا بتوانند تأیید نمایند که فرایند پاکسازی همانند انتظار پیش می‌رود.

راهنمایی تکمیلی: تست کردن رویه‌ها و تجهیزات پاکسازی ممکن است توسط موجودیت‌های خارجی دارای صلاحیت و مجاز (نظیر سایر مؤسسات فدرال یا سرویس‌دهندگان خارجی) انجام شود.

(۳) پاکسازی رسانه‌ها / شگردهای غیرتخریبی

سازمان در شرایط زیر، از شگردهای پاکسازی غیرتخریبی برای دستگاه‌های ذخیره‌سازی قابل حمل پیش از اتصال این دستگاه‌ها به سیستم‌های اطلاعاتی استفاده می‌کنند:

[اختصاص: شرایطی که توسط سازمان تعیین می‌شوند و پاکسازی دستگاه‌های ذخیره‌سازی قابل حمل را الزامی می‌نمایند.]

راهنمایی تکمیلی: این کنترل پیشرفته به رسانه‌های دیجیتال حاوی اطلاعات محرمانه و اطلاعات غیرمحرمانه ولی کنترل‌شده (CUI)[۲۱۲] نیز اطلاق می‌شود. دستگاه‌های ذخیره‌سازی قابل حمل می‌توانند منبعی برای وارد کردن کدهای مخرب به سیستم‌های اطلاعاتی سازمانی باشند. بسیاری از این دستگاه‌ها از منابع ناشناخته و احتمالاً غیرقابل اعتماد به دست می‌آیند و ممکن است حاوی کدهای مخربی باشند که می‌توانند به آسانی از طریق پورت‌های USB یا سایر پورت‌های ورودی به سیستم‌های اطلاعاتی منتقل شوند. با این که اسکن این چنین دستگاه‌های ذخیره‌سازی همواره توصیه می‌شود، پاکسازی سبب اطمینان بیشتر می‌شود که این دستگاه‌ها عاری از کدهای مخرب حاوی دستوراتی هستند که قابلیت آغاز حملات روزصفر را دارند. سازمان‌ها در مواردی که دستگاه‌های ذخیره‌سازی قابل حمل به صورت دست اول از سازندگان یا ارائه‌دهندگان خریداری شده باشند، پیش از استفاده اولیه یا هنگامی که زنجیره مثبت مالکیت این دستگاه‌ها را از دست می‌دهند، شگردهای پاکسازی غیرتخریبی را به کار می‌برند. کنترل‌های مربوطه: SI-3.

(۴) پاکسازی رسانه‌ها / اطلاعات غیرمحرمانه ولی کنترل‌شده

[حذف شد: به بخش MP-6 منتقل شد.]

(۵) پاکسازی رسانه‌ها / اطلاعات محرمانه

[212] Controlled Unclassified Information

[حذف شد: به بخش MP-6 منتقل شد.]

(۶) پاکسازی رسانه‌ها / تخریب رسانه‌ها

[حذف شد: به بخش MP-6 منتقل شد.]

(۷) پاکسازی رسانه‌ها / صدور مجوز دوجانبه

سازمان از فرایند صدور مجوز دوجانبه برای پاکسازی [اختصاص: رسانه‌های متعلق به سیستم‌های اطلاعاتی که توسط سازمان تعیین می‌شوند] استفاده می‌کند.

راهنمایی تکمیلی: سازمان‌ها فرایند صدور مجوز دوجانبه را به این علت به کار می‌برند که مطمئن شوند پاکسازی رسانه‌های متعلق به سیستم‌های اطلاعاتی فقط در صورتی انجام می‌شود که این عمل توسط دو نفر که از نفر فنی دارای صلاحیت هستند، انجام می‌شود. افرادی که مسئولیت پاکسازی رسانه‌های متعلق به سیستم‌های اطلاعاتی را دارند، از مهارت و تخصص کافی برخوردار هستند که بتوانند تشخیص دهند آیا فرایند پاکسازی مورد نظر بازگوکننده استانداردها، خط‌مشی‌ها و رویه‌های سازمانی یا فدرال مربوطه است یا خیر. به علاوه، صدور مجوز دوجانبه کمک می‌کند که مطمئن شد فرایند پاکسازی همانند انتظار پیش می‌رود؛ یعنی هم در برابر بروز خطا و هم از گزارش دروغی مبنی بر انجام پاکسازی حفاظت به عمل می‌آورد. صدور مجوز دوجانبه ممکن است با نام کنترل دونفره نیز شناخته شود. کنترل‌های مربوطه: AC-3 و MP-3.

(۸) پاکسازی رسانه‌ها / خالص‌سازی از راه دور

سازمان این امکان را فراهم می‌کند که اطلاعات [اختصاص: سیستم‌های اطلاعاتی، مؤلفه‌های سیستم‌ها و دستگاه‌های تعیین‌شده توسط سازمان] را به صورت از راه دور یا در شرایط زیر پاک یا خالص‌سازی نمود: [اختصاص: شرایطی که توسط سازمان تعریف می‌شوند]

راهنمایی تکمیلی: این کنترل پیشرفته از اطلاعات و داده‌های موجود در سیستم‌های اطلاعاتی، مؤلفه‌های سیستم‌ها و دستگاه‌های سازمانی (نظیر دستگاه‌های همراه)، در صورتی که این سیستم‌ها، مؤلفه‌ها و دستگاه‌ها توسط افراد غیرمجاز تهیه شده باشند، حفاظت می‌کند. به منظور کاهش خطر حذف و خالص‌سازی سیستم، مؤلفه‌ها و دستگاه‌ها توسط افراد غیرمجاز، تعبیه یک فرایند احراز هویت قدرتمند برای اعمال حذف و خالص‌سازی الزامی است. اعمال حذف و خالص‌سازی را می‌توان به شیوه‌های مختلفی انجام داد؛ برای مثال، بازنویسی چندین باره اطلاعات و داده‌ها یا تخریب کلید لازم برای رمزگشایی داده‌های رمزگذاری‌شده.

مراجع: نشریه FIPS 199، نشریه‌های ویژه NIST 800-88، NIST 800-60، آدرس وب: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

اولویت و تخصیص به مجموعه‌های پایه:

P1	MP-6 اولویت پایین	MP-6 اولویت متوسط	MP-6 (1)(2)(3) اولویت بالا

MP-7: کاربرد رسانه‌ها

کنترل: سازمان با استفاده از [اختصاص: ضامن‌های امنیتی تعیین‌شده توسط سازمان]، به‌کارگیری [اختصاص: سیستم‌های اطلاعاتی یا مؤلفه‌های سیستمی تعیین‌شده توسط سازمان] را [انتخاب: محدود می‌کند، ممنوع می‌کند].

راهنمایی تکمیلی: رسانه‌های متعلق به سیستم‌های اطلاعاتی شامل رسانه‌های دیجیتالی و رسانه‌های غیردیجیتالی می‌شوند. از جمله رسانه‌های دیجیتالی می‌توان به دیسکت‌ها، نوارهای مغناطیسی، هارد دیسک‌های خارجی و جداشدنی، فلش درایو، دیسک‌های فشرده، دیسک‌های ویدیوی دیجیتالی اشاره کرد. از جمله رسانه‌های غیردیجیتالی می‌توان به کاغذ و میکروفیلم اشاره کرد. این کنترل به دستگاه‌های همراه با قابلیت ذخیره‌سازی (نظیر گوشی‌های هوشمند، تبلت‌ها و کتابخوان‌های الکترونیکی) اطلاق می‌شود. در مقایسه با MP-2 که دسترسی کاربران به رسانه‌ها را محدود می‌کند، این کنترل کاربرد انواع خاصی از رسانه‌ها برای سیستم‌های اطلاعاتی را محدود می‌سازد؛ برای مثال، محدود کردن یا ممنوع استفاده از فلش درایو یا هارد دیسک‌های خارجی. سازمان‌ها می‌توانند از ضامن‌های فنی و غیرفنی (نظیر خط‌مشی‌ها، رویه‌ها و قوانین رفتاری) برای محدود کردن کاربرد رسانه‌های متعلق به سیستم‌های اطلاعاتی استفاده نمایند. ممکن است سازمان‌ها کاربرد دستگاه‌های ذخیره‌سازی قابل حمل را محدود سازند؛ به عنوان نمونه، با به‌کارگیری قفسه‌های فیزیکی روی ایستگاه‌های رایانه‌ای برای ممانعت از دسترسی به برخی از پورت‌های خارجی مشخص یا غیرفعال کردن یا حذف کردن امکان وارد کردن، خواندن یا نوشتن روی چنین دستگاه‌هایی. همچنین ممکن است سازمان‌ها کاربرد دستگاه‌های ذخیره‌سازی قابل حمل را فقط به دستگاه‌های تأییدشده محدود نمایند؛ برای نمونه، دستگاه‌های که توسط سازمان ارائه می‌شوند یا دستگاه‌هایی که توسط سایر سازمان‌های تأییدشده ارائه می‌شوند و دستگاه‌هایی که متعلق به اشخاص حقوقی نیست. در نهایت، ممکن است سازمان‌ها کاربرد دستگاه‌های ذخیره‌سازی قابل حمل را بر اساس نوع آن‌ها محدود نمایند؛ برای مثال، ممانعت از کاربرد دستگاه‌های ذخیره‌سازی قابل حمل با قابلیت نوشتن و پیاده‌سازی این محدودیت از طریق غیرفعال کردن یا حذف قابلیت نوشتن روی این دستگاه‌ها. کنترل‌های مربوطه: AC-19 و PL-4.

کنترل‌های پیشرفته:

(۱) کاربرد رسانه‌ها / ممانعت از کاربرد رسانه‌های بدون مالک

در صورت مالک دستگاه‌های ذخیره‌سازی قابل حمل قابل شناسایی نیست، سازمان کاربرد این دستگاه‌ها در سیستم‌های اطلاعاتی سازمانی را ممنوع می‌نماید.

راهنمایی تکمیلی: الزامی بودن امکان شناسایی مالک برای دستگاه‌های ذخیره‌سازی قابل حمل (نظیر افراد، سازمان‌ها یا پروژه‌ها)، مخاطرات به‌کارگیری این فناوری‌ها کاهش می‌دهد؛ به این شکل که به سازمان‌ها اجازه می‌دهد برای رسیدگی به آسیب‌پذیری‌های شناخته‌شده در این دستگاه‌ها (نظیر ورود کدهای مخرب)، مسئولیت و پاسخگویی مشخص نمایند. کنترل‌های مربوطه: PL-4.

(۲) کاربرد رسانه‌ها / ممانعت از کاربرد رسانه‌های مقاوم در برابر پاکسازی

سازمان از کاربرد رسانه‌های مقاوم در برابر پاکسازی در سیستم‌های اطلاعاتی سازمانی ممانعت می‌نماید.

راهنمایی تکمیلی: مقاومت در برابر پاکسازی به امکان خالص‌سازی رسانه‌ها از اطالعات بر می‌گردد. انواع خاصی از رسانه‌ها از فرمان‌های پاکسازی پشتیبانی نمی‌کنند یا در صورت پشتیبانی، واسط‌های مربوطه به شکل استاندارد برای این دستگاه‌ها پشتیبانی نمی‌شوند. فلش‌های فشرده، فلش‌های تعبیه‌شده در مدارها یا دستگاه‌ها، درایوهای جامد و رسانه‌های USB جداشدنی نمونه‌هایی از رسانه‌های مقاوم در برابر پاکسازی هستند. کنترل‌های مربوطه: MP-6.

مراجع: نشریه FIPS 199، نشریه ویژه NIST 800-111

اولویت و تخصیص به مجموعه‌های پایه:

P1	MP-7 اولویت پایین	MP-7 (1) اولویت متوسط	MP-7 (1) اولویت بالا

MP-8: تقلیل رسانه‌ها

کنترل: سازمان:

الف. [اختصاص: فرایندهایی برای تقلیل رسانه‌ها که توسط سازمان تعریف می‌شوند] ایجاد می‌نماید که شامل به‌کارگیری سازوکارهای تقلیل با [اختصاص: میزان قدرت و یکپارچگی تعیین‌شده توسط سازمان] می‌شود.

ب. اطمینان حاصل می‌کند که فرایند تقلیل رسانه‌های متعلق به سیستم‌های اطلاعاتی با طبقه‌بندی امنیتی یا سطح دسته‌بندی اطلاعاتی که قرار است حذف شوند و نیز با مجوزهای دسترسی دریافت‌کننده‌های احتمالی اطلاعات تقلیل‌یافته مطابقت داشته باشد.

پ. [اختصاص: رسانه‌های متعلق به سیستم‌های اطلاعاتی و نیازمند تقلیل که توسط سازمان تعیین می‌شوند] را شناسایی می‌کند.

ت. رسانه‌های متعلق به سیستم‌های اطلاعاتی شناسایی‌شده را از طریق فرایندهای ایجادشده تقلیل می‌دهد.

راهنمایی تکمیلی: این کنترل به همه رسانه‌های متعلق به سیستم‌های اطلاعاتی، هم دیجیتال و هم غیردیجیتال، که برای انتشار در خارج از سازمان در نظر گرفته شده‌اند، فارغ از این که این رسانه‌ها جداشدنی هستند یا خیر، اطلاق می‌شود. هنگامی که فرایند تقلیل روی رسانه‌های سیستم اجرا می‌شود، اطلاعات را به صورت عمومی بر اساس طبقه‌بندی امنیتی یا سطح دسته‌بندی آن‌ها از آن رسانه‌ها حذف می‌کند، به نحوی که قابل دریافت یا بازسازی نباشند. تقلیل رسانه‌ها شامل نگارش مجدد اطلاعات می‌شود تا امکان انتشار و توزیع گسترده‌تر فراهم شود. به علاوه، تقلیل رسانه‌ها سبب اطمینان از عدم وجود اطلاعات روی فضاهای خالی موجود در رسانه‌ها (نظیر فضاهای بدون استفاده درون فایل‌ها) می‌شود.

کنترل‌های پیشرفته:

(۱) تقلیل رسانه‌ها / مستندسازی فرایند

سازمان فعالیت‌های تقلیل رسانه‌های متعلق به سیستم‌های اطلاعاتی را مستند می‌نماید.

راهنمایی تکمیلی: سازمان‌ها می‌توانند فرایند تقلیل رسانه‌ها را از طریق ارائه اطلاعاتی نظیر شگرد به‌کاررفته برای تقلیل، شماره شناسایی رسانه تقلیل‌یافته و هویت فردی که عمل تقلیل را انجام داده است یا اجازه انجام آن را داده است، مستند نمایند.

(۲) تقلیل رسانه‌ها / تست کردن تجهیزات

سازمان [اختصاص: تست‌هایی که توسط سازمان تعریف می‌شوند] را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] روی تجهیزات و رویه‌های تقلیل اجرا می‌کند تا عملکرد صحیح آن‌ها را تأیید نماید.

(۳) تقلیل رسانه‌ها / اطلاعات غیرمحرمانه ولی کنترل‌شده

سازمان رسانه‌های متعلق به سیستم‌های اطلاعاتی و حاوی [اختصاص: اطلاعات غیرمحرمانه ولی کنترل‌شده (CUI) که توسط سازمان تعریف می‌شوند] را پیش از انتشار عمومی، مطابق با استانداردها و خط‌مشی‌های سازمانی و فدرال مربوطه تقلیل می‌دهد.

(۴) تقلیل رسانه‌ها / اطلاعات محرمانه

سازمان رسانه‌های متعلق به سیستم‌های اطلاعاتی و حاوی اطلاعات محرمانه را پیش از تحویل به افرادی که فاقد مجوزهای دسترسی الزامی هستند، مطابق با استانداردها و خط‌مشی‌های NSA تقلیل می‌دهد.

راهنمایی تکمیلی: در فرایند تقلیل اطلاعات محرمانه برای انتقال اطلاعاتی که دستور غیرمحرمانه بودن آن‌ها صادر شده است، از سیستم‌های اطلاعاتی محرمانه به رسانه‌های غیرمحرمانه، از ابزارها، شگردها و رویه‌های پاکسازی تأییدشده استفاده می‌شود.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

خانواده: حفاظت فیزیکی و محیطی

PE-1: خط‌مشی و رویه‌های حفاظت فیزیکی و محیطی

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۱۷. خط‌مشی حفاظت فیزیکی و محیطی شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و

۱۸. رویه‌های تسهیل پیاده‌سازی خط‌مشی حفاظت فیزیکی و محیطی و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۱۷. خط‌مشی حفاظت فیزیکی و محیطی؛ و

۱۸. رویه‌های حفاظت فیزیکی و محیطی.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده PE را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: نشریه ویژه NIST 800-12, NIST 800-100

اولویت و تخصیص به مجموعه‌های پایه:

P1	PE-1 اولویت پایین	PE-1 اولویت متوسط	PE-1 اولویت بالا

PE-2: مجوزهای دسترسی فیزیکی

کنترل: سازمان:

الف. لیستی از افرادی که از مجوز دسترسی به تأسیسات حاوی سیستم‌های اطلاعاتی برخوردار هستند، تهیه، تأیید و نگهداری می‌کند.

ب. اطلاعات محرمانه مجوز دسترسی به تأسیسات را صادر می‌نماید.

پ. لیست افراد مجاز برای دسترسی به تأسیسات را [اختصاص: در بازه‌های تعیین‌شده توسط سازمان] بازبینی می‌کند.

ت. هنگامی که ضرورت دسترسی افراد به تأسیسات از بین می‌رود، آن‌ها را از لیست دسترسی به تأسیسات حذف می‌کند.

راهنمایی تکمیلی: این کنترل به کارکنان و ملاقات‌کننده‌های سازمانی اطلاق می‌شود. افرادی که از اطلاعات محرمانه دائمی برای مجوز دسترسی فیزیکی برخوردار هستند (نظیر کارکنان و پیمانکاران)، ملاقات‌کننده به حساب نمی‌آیند. نشان، کارت شناسایی و کارت‌های هوشمند نمونه‌هایی از اطلاعات محرمانه مجوز هستند. سازمان‌ها قدرت مورد نیاز برای اطلاعات محرمانه مجوز (از جمله سطح نشان‌های غیرقابل جعل، کارت‌های هوشمند یا کارت‌های شناسایی) را که با استانداردها، خط‌مشی‌ها و رویه‌های فدرال مطابقت دارند تعیین می‌کنند. این کنترل فقط مناطقی در تأسیسات اطلاق می‌شود که قابل دسترسی برای عموم نیستند. کنترل‌های مربوطه: PE-3، PE4 و PS3.

کنترل‌های پیشرفته:

(۱) مجوزهای دسترسی فیزیکی / دسترسی بر اساس مقام یا نقش

سازمان مجوزهای دسترسی فیزیکی به تأسیسات حاوی سیستم‌های اطلاعاتی را بر اساس مقام یا نقش افراد صادر می‌کند.

راهنمایی تکمیلی: کنترل‌های مربوطه: AC-2، AC-3 و AC-6.

(۲) مجوزهای دسترسی فیزیکی / دو روش شناسایی

سازمان دو روش شناسایی را از میان [اختصاص: لیست روش‌های قابل قبول برای شناسایی که توسط سازمان تعیین می‌شوند] برای ملاقات‌کننده‌هایی که می‌خواهند به تأسیسات حاوی سیستم‌های اطلاعاتی دسترسی داشته باشند، الزامی می‌نماید.

راهنمایی تکمیلی: گذرنامه، کارت‌های تأیید هویت افراد (PIV) و گواهینامه‌های رانندگی نمونه‌هایی از روش‌های قابل‌قبول شناسایی تصویری دولتی هستند. در مواردی که برای دسترسی یافتن به تأسیسات سازوکارهای خودکار به کار می‌روند، سازمان‌ها ممکن است از کارت‌های PIV، کارت‌های کلیدی، پین و مؤلفه‌های بیومتریک استفاده نمایند.

(۳) مجوزهای دسترسی فیزیکی / محدودیت دسترسی بدون همراه

سازمان دسترسی بدون همراه به تأسیسات حاوی سیستم‌های اطلاعاتی را به کارکنانی که از [انتخاب (یکی یا بیشتر): تأییدیه امنیتی برای همه اطلاعات موجود در سیستم‌ها، مجوزهای رسمی دسترسی به همه اطلاعات موجود در سیستم‌ها، نیاز به دسترسی به همه اطلاعات موجود در سیستم‌های اطلاعاتی، [اختصاص: اطلاعات محرمانه تعیین‌شده توسط سازمان]] برخوردار هستند، محدود می‌کند.

راهنمایی تکمیلی: به علت ماهیت بسیار حساس اطلاعات محرمانه که در برخی تأسیسات خاص ذخیره می‌شوند، بسیار مهم است که افرادی که از سطح کافی از تأییدیه‌های امنیتی کافی، تأییدیه‌های دسترسی یا نیاز به دانستن برخودار نیستند، توسط افرادی که دارای اطلاعات محرمانه مناسب هستند، همراهی شوند تا اطمینان حاصل شود که چنین اطلاعاتی افشا نمی‌شود یا در معرض خطر قرار نمی‌گیرد. کنترل‌های مربوطه: PS-2 و PS-6

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	PE-2 اولویت پایین	PE-2 اولویت متوسط	PE-2 اولویت بالا

PE-3: **کنترل دسترسی فیزیکی**

کنترل: سازمان:

الف. صدور مجوز دسترسی فیزیکی را در [اختصاص: نقاط ورود و خروج به تأسیسات حاوی سیستم‌های اطلاعاتی که توسط سازمان تعیین می‌شوند] به واسطه روش‌های زیر اعمال می‌کند:

۱. تأیید صحت مجوزهای دسترسی هر فرد پیش از دادن اجازه دسترسی به تأسیسات

۲. کنترل ورود و خروج به تأسیسات به وسیله [انتخاب (یکی یا بیشتر): [اختصاص: سیستم‌ها یا دستگاه‌های کنترل دسترسی فیزیکی که توسط سازمان تعیین می‌شوند]، نگهبان]

ب. گزارش‌های ممیزی کنترل فیزیکی مربوط به [اختصاص: نقاط ورود و خروج تعیین‌شده توسط سازمان] را حفظ و نگهداری می‌کند.

پ. از [اختصاص: ضامن‌های امنیتی تعیین‌شده توسط سازمان] برای کنترل دسترسی به مناطقی از تأسیسات که رسماً به عنوان قابل دسترسی برای عموم تعریف شده است، استفاده می‌کند.

ت. ملاقات‌کننده‌ها را همراهی می‌کند و فعالیت‌های آن‌ها را در [اختصاص: شرایطی که همراهی و پایش ملاقات‌کننده‌ها الزامی است و توسط سازمان تعریف می‌شوند] پایش می‌نماید.

ث. امنیت کلیدها، ترکیب‌ها[۲۱۳] و سایر دستگاه‌های دسترسی فیزیکی را تأمین می‌کند.

ج. از [اختصاص: دستگاه‌های دسترسی فیزیکی که توسط سازمان تعیین می‌شوند] [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] لیست و گزارش تهیه می‌کند.

چ. ترکیب‌ها و کلیدها را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] و یا هنگامی کلیدها گم می‌شوند، ترکیب‌ها در معرض افشا قرار می‌گیرند یا افراد جابجا یا حذف می‌شوند، تغییر می‌دهد.

راهنمایی تکمیلی:

این کنترل به ملاقات‌کننده‌ها یا کارکنان سازمانی اطلاق می‌شود. افرادی که از اطلاعات محرمانه دائمی برای مجوز دسترسی فیزیکی برخوردار هستند (نظیر کارکنان و پیمانکاران)، ملاقات‌کننده به حساب نمی‌آیند. سازمان‌ها انواع نگهبان‌های مورد نیاز برای تأسیسات را تعیین می‌کنند؛ از جمله کارکنان مخصوص امنیت فیزیکی یا سایر کارکنان نظیر کارکنان مدیریتی یا کاربران سیستم‌های اطلاعاتی. کلیدها، قفل‌ها، ترکیب‌ها و کارت‌خوان‌ها نمونه‌هایی از دستگاه‌های دسترسی فیزیکی هستند. دوربین‌ها، عملیات پایش توسط نگهبان‌ها و نگهداری جداگانه سیستم‌های اطلاعاتی و یا مؤلفه‌های سیستم‌ها در مناطق امن نمونه‌هایی از ضامن‌هایی هستند که در مناطق قابل دسترسی برای عموم به کار می‌روند. سیستم‌های کنترل دسترسی فیزیکی از قوانین، دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، مقررات، استانداردها و راهنمایی‌های فدرال مربوطه پیروی می‌کنند. برنامه فدرال مدیریت هویت، اطلاعات محرمانه و دسترسی[۲۱۴]، راهنمایی‌هایی برای پیاده‌سازی

[213] combination
[214] Federal Identity, Credential, and Access Management Program

قابلیت‌های مدیریت هویت، اطلاعات محرمانه و دسترسی در سیستم‌های کنترل دسترسی فیزیکی ارائه می‌دهد. سازمان‌ها در انواع گزارش‌های ممیزی که به کار می‌برند، انعطاف‌پذیر هستند. گزارش‌های ممیزی می‌توانند رویه‌ای (نظیر یک گزارش کتبی از افرادی که به تأسیسات دسترسی دارند و زمانی که این دسترسی صورت گرفته است)، خودکار (نظیر ثبت ID ارائه‌شده توسط که یک کارت PIV) یا ترکیبی از هر دو باشند. نقاط دسترسی فیزیکی می‌تواند شامل نقاط دسترسی به تأسیسات، نقاط دسترسی داخلی به سیستم‌های اطلاعاتی و یا مؤلفه‌هایی که به کنترل‌های دسترسی تکمیلی نیاز دارند یا هر دو شود. مؤلفه‌های سیستم‌های اطلاعاتی (نظیر ایستگاه‌های رایانه‌ای و ترمینال‌ها) ممکن است در مناطقی قرار داشته باشند که به عنوان قابل دسترسی برای عموم تعریف شده‌اند و سازمان‌ها، ضامن‌هایی برای دسترسی به چنین دستگاه‌هایی تعبیه کرده باشند. کنترل‌های مربوطه: AU-2، AU-6، MP-2، MP-4، PE-2، PE-4، PE-5، PS-3 و RA-3.

کنترل‌های پیشرفته:

(۱) کنترل دسترسی فیزیکی / دسترسی به سیستم‌های اطلاعاتی

سازمان، علاوه بر کنترل‌های دسترسی فیزیکی، صدور مجوز دسترسی فیزیکی را برای سیستم‌های اطلاعاتی تأسیسات در [اختصاص: فضاهای فیزیکی حاوی یک یا تعداد بیشتر از مؤلفه‌های سیستم‌های اطلاعاتی که توسط سازمان تعریف می‌شوند] اعمال می‌کند.

راهنمایی تکمیلی: این کنترل، امنیت فیزیکی بیشتری برای مناطقی از تأسیسات که در آن‌ها تجمعی از مؤلفه‌های سیستم‌های اطلاعاتی (نظیر اتاق‌های سرور، مناطق ذخیره‌سازی رسانه‌ها و مراکز داده و ارتباطات) وجود دارد، فراهم می‌کند. کنترل مربوطه: PS-2.

(۲) کنترل دسترسی فیزیکی / مرزهای سیستم‌های اطلاعاتی

سازمان [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] در مرزهای فیزیکی تأسیسات یا سیستم‌های اطلاعاتی در ارتباط با استخراج غیرمجاز اطلاعات یا حذف مؤلفه‌های سیستم‌های اطلاعاتی، بررسی امنیتی انجام می‌دهد.

راهنمایی تکمیلی: سازمان‌ها شدت، دفعات و تصادفی بودن بررسی‌های امنیتی را تعیین می‌کنند تا مخاطرات ناشی از استخراج را به میزان کافی کاهش دهند. کنترل‌های مربوطه: AC-4 و SC-7.

(۳) کنترل دسترسی فیزیکی / نگهبانی، زنگ هشدار و پایش پیوسته

سازمان از نگهبان‌ها و یا زنگ‌های هشدار برای پایش دائمی همه نقاط دسترسی فیزیکی به تأسیسات حاوی سیستم‌های اطلاعاتی در تمام لحظات، استفاده می‌کند.

راهنمایی تکمیلی: کنترل‌های مربوطه: CP-6 و CP-7.

(۴) کنترل دسترسی فیزیکی / جعبه‌های دارای قفل

سازمان از جعبه‌های فیزیکی دارای قفل برای حفاظت از [اختصاص: مؤلفه‌های سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] در برابر دسترسی فیزیکی و غیرمجاز استفاده می‌کند.

(۵) کنترل دسترسی فیزیکی / حفاظت در مقابل دستکاری

سازمان از [اختصاص: ضامن‌های امنیتی تعیین‌شده توسط سازمان] برای [انتخاب (یکی یا بیشتر): شناسایی، پیشگیری از] ایجاد تغییر یا دستکاری فیزیکی درون سیستم‌های اطلاعاتی در [اختصاص: مؤلفه‌های سخت‌افزاری تعیین‌شده توسط سازمان]، استفاده می‌کند.

راهنمایی تکمیلی: سازمان‌ها ممکن است روش‌های شناسایی و پیشگیری از دستکاری را در برخی مؤلفه‌های سخت‌افزاری انتخاب‌شده پیاده‌سازی نمایند یا روش‌های شناسایی را برخی از مؤلفه‌های سخت‌افزاری و روش‌های پیشگیری را در سایر مؤلفه‌ها پیاده‌سازی نمایند. در فعالیت‌های شناسایی و پیشگیری از دستکاری، می‌توان چندین نوع از فناوری‌های ضددستکاری، از جمله قفل‌های شناسایی دستکاری و پوشش‌های ضددستکاری، را به کار گرفت. برنامه‌های ضددستکاری به شناسایی تغییرات سخت‌افزاری از طریق تهیه بدل و سایر مخاطرات مربوط به زنجیره تأمین کمک می‌کنند. کنترل مربوطه: SA-12.

(۶) کنترل دسترسی فیزیکی / تست نفوذ به تأسیسات

سازمان از یک فرایند تست نفوذ استفاده می‌کند که [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] انجام می‌شود و شامل تلاش‌های اعلام‌نشده برای دور زدن یا عبور از کنترل‌های امنیتی مربوط به نقاط دسترسی فیزیکی به تأسیسات می‌شود.

راهنمایی تکمیلی: کنترل‌های مربوطه: CA-2 و CA-7.

مراجع: نشریه FIPS 201، نشریه‌های ویژه NIST 800-73، NIST 800-76، NIST 800-78، NIST 800-116، ICD 704، ICD 705، دستور DoD 5200.39، تأیید هویت افراد (PIV) در سیستم‌های کنترل دسترسی فیزیکی سازمانی (E-PACS).

آدرس‌های وب: http://idmanagement.gov، http://fips201ep.cio.gov

اولویت و تخصیص به مجموعه‌های پایه:

P1	PE-3 اولویت پایین	PE-3 اولویت متوسط	PE-3 (1) اولویت بالا

PE-4: کنترل دسترسی برای واسطه‌های انتقال پیام

کنترل: سازمان دسترسی فیزیکی به [اختصاص: خطوط توزیع و انتقال پیام سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] را درون تأسیسات سازمانی با استفاده از [اختصاص: ضامن‌های امنیتی تعیین‌شده توسط سازمان] کنترل می‌کند.

راهنمایی تکمیلی: ضامن‌های امنیتی فیزیکی به‌کاررفته برای خطوط توزیع و انتقال پیام سیستم‌های اطلاعاتی به پیشگیری از آسیب‌های اتفاقی، اختلال و دستکاری فیزیکی کمک می‌کنند. به علاوه، ضامن‌های امنیتی ممکن است برای پیشگیری از شنود یا ایجاد تغییرات در حین انتقال پیام‌های رمزگذاری‌نشده مؤثر باشند. نمونه‌هایی از ضامن‌های امنیتی به‌کاررفته برای کنترل دسترسی فیزیکی به خطوط انتقال پیام و توزیع سیستم عبارتند از (۱) جعبه‌های سیم‌کشی قفل‌شده، (۲) جک‌های اضافی قفل‌شده یا قطع‌شده و (۳) حفاظت از سیم‌کشی با استفاده از محفظه‌های سیم یا رسانا. کنترل‌های مربوطه: MP-2، MP-4، PE-2،PE-3، PE-5، SC-7 و SC-8.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: NSTISSI شماره ۷۰۰۳

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	PE-4 اولویت متوسط	PE-4 اولویت بالا

PE-5: کنترل دسترسی برای دستگاه‌های خروجی

کنترل: سازمان دسترسی فیزیکی به دستگاه‌های خروجی سیستم‌های اطلاعاتی را به منظور پیشگیری از دستیابی افراد غیرمجاز به این خروجی‌ها کنترل می‌کند.

راهنمایی تکمیلی: قرار دادن دستگاه‌های خروجی در اتاق‌های قفل‌شده یا سایر مناطق امن‌شده و ارائه اجازه دسترسی فقط به افراد مجاز و قرار دادن دستگاه‌های خروجی در مکان‌هایی که امکان پایش آن‌ها توسط کارکنان سازمانی وجود دارد، نمونه‌هایی از کنترل دسترسی فیزیکی به دستگاه‌های خروجی هستند. صفحه‌های نمایش، پرینترها، دستگاه‌های کپی، اسکنرها، دستگاه‌های فکس و دستگاه‌های صوتی نمونه‌هایی از دستگاه‌های خروجی سیستم‌های اطلاعاتی هستند. کنترل‌های مربوطه: PE-2، PE-3، PE4 و PE18.

کنترل‌های پیشرفته:

(۱) کنترل دسترسی برای دستگاه‌های خروجی / دسترسی افراد مجاز به خروجی‌ها

سازمان:

الف. دسترسی فیزیکی به [اختصاص: دستگاه‌های خروجی تعیین‌شده توسط سازمان] را کنترل می‌کند.

ب. اطمینان حاصل می‌کند که فقط افراد مجاز دستگاه‌های خروجی را دریافت نمایند.

راهنمایی تکمیلی: قرار دادن پرینترها، دستگاه‌های کپی و دستگاه‌های فکس در مناطق کنترل‌شده و دارای کنترل دسترسی با استفاده از صفحه‌کلید یا محدود کردن دسترسی فقط به افراد خاصی که دارای نوع خاصی از نشان هستند، نمونه‌هایی از کنترل دسترسی فیزیکی به دستگاه‌های خروجی انتخاب‌شده است.

(۲) کنترل دسترسی برای دستگاه‌های خروجی / دسترسی فردی به خروجی‌ها

سیستم اطلاعاتی:

الف. دسترسی فیزیکی به خروجی‌ها از طریق [اختصاص: دستگاه‌های خروجی تعیین‌شده توسط سازمان] را کنترل می‌کند.

ب. هویت فرد را به عنوان دریافت‌کننده خروجی از دستگاه ثبت می‌کند.

راهنمایی تکمیلی: نصب قابلیت‌های امنیتی در پرینترها، دستگاه‌های کپی و دستگاه‌های فکس نمونه‌هایی از کنترل دسترسی فیزیکی به دستگاه‌های خروجی است که امکان پیاده‌سازی احراز هویت (به عنوان مثال، با استفاده از پین یا توکن سخت‌افزاری) در دستگاه‌های خروجی پیش از دادن خروجی به افراد را فراهم می‌کند.

(۳) کنترل دسترسی برای دستگاه‌های خروجی / نشانه‌گذاری دستگاه‌های خروجی

سازمان [اختصاص: دستگاه‌های خروجی سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] را نشانه‌گذاری می‌کند که مشخص‌کننده نشانه امنیتی مناسب برای اطلاعاتی است که اجازه دارند از آن دستگاه خارج و ارائه شوند.

راهنمایی تکمیلی: پرینتر، صفحه نمایش، دستگاه‌های فکس، اسکنرها، دستگاه‌های کپی و دستگاه‌های صوتی نمونه‌هایی از دستگاه‌های خروجی هستند. به طور کلی امکان اعمال این کنترل پیشرفته دستگاه‌های خروجی غیر از دستگاه‌های همراه وجود دارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب‌نشده، اولویت پایین	PE-5 اولویت متوسط	PE-5 اولویت بالا

PE-6: پایش دسترسی فیزیکی

کنترل: سازمان:

الف. دسترسی فیزیکی تأسیسات حاوی سیستم‌های اطلاعاتی را به منظور شناسایی حوادث امنیت فیزیکی و واکنش به آن‌ها پایش می‌کند.

ب. گزارش‌گیری‌های دسترسی فیزیکی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] و در هنگام بروز [اختصاص: رویدادها یا نشانه‌های احتمالی رویدادهای تعیین‌شده توسط سازمان] بازبینی می‌کند.

پ. نتایج بازبینی‌ها و تحقیقات را قابلیت‌های سازمانی واکنش به حوادث هماهنگ و مطابق می‌نماید.

راهنمایی تکمیلی: قابلیت‌های سازمانی واکنش به حوادث شامل تحقیقات مربوط حوادث امنیت فیزیکی شناسایی‌شده و واکنش به آن‌ها می‌شود. تخلفات امنیتی آشکار یا فعالیت‌های دسترسی فیزیکی مشکوک نمونه‌هایی از حوادث امنیتی هستند. مثال‌هایی از فعالیت‌های دسترسی فیزیکی مشکوک عبارتند از: (۱) دسترسی خارج از ساعت‌های کاری معمول، (۲) دسترسی‌های چندباره به مناطقی که دسترسی به آن‌ها معمولاً صورت نمی‌پذیرد، (۳) دسترسی به مدت زمان غیرمعمول و (۴) دسترسی‌های خارج از نوبت. کنترل‌های مربوطه: CA-7، IR-4 و IR-8.

کنترل‌های پیشرفته:

(۱) پایش دسترسی فیزیکی / هشدارهای نفوذ و تجهیزات نظارتی

سازمان تجهیزات نظارتی و هشدارهای نفوذ فیزیکی را پایش می‌کند.

(۲) پایش دسترسی فیزیکی / تشخیص و واکنش خودکار به نفوذ

سازمان از سازوکارهای خودکار برای تشخیص [اختصاص: انواع و دسته‌های نفوذ که توسط سازمان تعیین می‌شوند] و فعال‌سازی [اختصاص: تمهیدات واکنشی تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی تکمیلی: کنترل مربوطه: SI-4.

(۳) پایش دسترسی فیزیکی / نظارت تصویری

سازمان نظارت تصویری را برای [اختصاص: مناطق عملیاتی تعیین‌شده توسط سازمان] به کار می‌گیرد و تصاویر ویدیویی ضبط‌شده را برای [اختصاص: مدت زمان تعیین‌شده توسط سازمان] نگه می‌دارد.

راهنمایی تکمیلی: این کنترل پیشرفته روی ضبط کردن ویدیوهای نظارت تصویری به هدف بازبینی‌های بعدی، در صورتی شرایط پیش‌آمده ایجاب نماید (نظیر ورود غیرقانونی که به روش‌های دیگر شناسایی شده است)، تمرکز می‌کند. الزامی به پایش ویدیوهای نظارتی نیست، اگرچه سازمان‌ها ممکن است بخواهند این کار را انجام دهند. توجه شود که ممکن است برخی ملاحظات قانونی در ارتباط با اعمال و حفظ نظارت تصویری وجود داشته باشد، به خصوص اگر این نظارت در مکانی عمومی انجام شود.

(۴) پایش دسترسی فیزیکی / پایش دسترسی فیزیکی به سیستم‌های اطلاعاتی

سازمان علاوه بر پایش دسترسی فیزیکی در تأسیسات به عنوان [اختصاص: فضاهای فیزیکی حاوی یک یا تعداد بیشتری از مؤلفه‌های سیستم‌های اطلاعاتی که توسط سازمان تعیین می‌شوند]، دسترسی فیزیکی به سیستم‌های اطلاعاتی را پایش می‌کند.

راهنمایی تکمیلی: این کنترل پیشرفته امکان پایش بیشتر برای مناطقی در تأسیسات را که در آن تجمع مؤلفه‌های سیستم‌های اطلاعاتی وجود دارد (نظیر اتاق‌های سرور، مناطق ذخیره‌سازی رسانه‌ها و مراکز ارتباطات)، به وجود می‌آورد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	PE-6 اولویت پایین	PE-6 (1) اولویت متوسط	PE-6 (1)(4) اولویت بالا

PE-7: کنترل ملاقات‌کننده‌ها

[حذف شد: به بخش‌های PE-2 و PE-3 منتقل شد.]

PE-8: سوابق دسترسی ملاقات‌کننده‌ها

کنترل: سازمان:

الف. سوابق دسترسی ملاقات‌کننده‌ها به تأسیسات حاوی سیستم‌های اطلاعاتی را برای [اختصاص: مدت زمان تعیین‌شده توسط سازمان] حفظ و نگهداری می‌کند.

ب. سوابق دسترسی ملاقات‌کننده‌ها را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند.

راهنمایی تکمیلی: نام و سازمان ملاقات‌کننده، امضای ملاقات‌کننده، روش‌های شناسایی هویت، تاریخ‌های دسترسی، زمان‌های ورود و خروج، اهداف ملاقات و نام و سازمان افراد ملاقات‌شده نمونه‌هایی از سوابق دسترسی ملاقات‌کننده‌ها هستند. ثبت سوابق دسترسی ملاقت‌کننده‌ها برای مناطق قابل دسترسی برای عموم الزامی نیست.

کنترل‌های پیشرفته:

(۱) سوابق دسترسی ملاقت‌کننده‌ها / حفظ و نگهداری و بازبینی خودکار سوابق

سازمان از سازوکارهای خودکار به منظور تسهیل حفظ و نگهداری و بازبینی سوابق دسترسی ملاقات‌کننده‌ها استفاده می‌نماید.

(۲) سوابق دسترسی ملاقات‌کننده‌ها / سوابق دسترسی فیزیکی

[حذف شد: به بخش PE-2 منتقل شد.]

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	PE-8 اولویت پایین	PE-8 اولویت متوسط	PE-8 (1) اولویت بالا

PE-9: سیم‌کشی و تجهیزات تولید انرژی

کنترل: سازمان از تجهیزات تولید انرژی و سیم‌کشی انتقال انرژی برای سیستم‌های اطلاعاتی در برای آسیب‌ها و تخریب حفاظت می‌کند.

راهنمایی تکمیلی: سازمان‌ها تعیین می‌کنند که چه انواعی از حفاظت برای سیم‌کشی و تجهیزات تولید انرژی به‌کاررفته در مکان‌های مختلف در داخل و خارج تأسیسات سازمانی و محیط‌های عملیاتی ضروری است. ژنراتورها و سیم‌کشی‌های انتقال انرژی در خارج از ساختمان‌ها، سیم‌کشی داخلی و منابع انرژی بدون‌قطعی (UPS) در داخل اداره‌ها یا مراکز داده و منابع انرژی برای موجودیت‌های خودکفا نظیر خودرها و ماهواره‌ها نمونه‌هایی از سیم‌کشی و تجهیزات تولید انرژی است. کنترل مربوطه: PE-4.

کنترل پیشرفته:

۱. سیم‌کشی و تجهیزات تولید انرژی / سیم‌کشی اضافی

سیسازمان از مسیرهای سیم‌کشی اضافی برای انتقال انرژی استفاده می‌کند که از نظر فیزیکی به صورت جدا از هم [اختصاص: در فاصله تعیین‌شده توسط سازمان] قرار می‌گیرند.

راهنمایی تکمیلی: سیم‌کشی‌های اضافی و از نظر فیزیکی مجزا، سبب اطمینان بیشتر می‌شوند که در صورت قطع شدن یکی از سیم‌ها یا آسیب دیدن سیم‌ها به هر شکل دیگری، انرژی همچنان جریان می‌یابد.

۲. سیم‌کشی و تجهیزات تولید انرژی / کنترل‌های خودکار ولتاژ

سازمان از کنترل‌های خودکار ولتاژ برای [مؤلفه‌های حیاتی سیستم‌های اطلاعاتی که توسط سازمان تعیین می‌شوند] استفاده می‌کند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P4	انتخاب‌نشده، اولویت پایین	PE-9 اولویت متوسط	PE-9 اولویت بالا

PE-10: خاموشی اضطراری

کنترل: سازمان:

الف. امکان قطع کردن انرژی سیستم‌های اطلاعاتی یا هر یک از مؤلفه‌های سیستم‌ها به صورت تکی در شرایط اضطراری را برقرار می‌کند.

ب. دستگاه‌ها یا سوییچ‌های خاموشی اضطراری را در [اختصاص: مکان‌های تعیین‌شده توسط سازمان در نزدیکی سیستم‌های اطلاعاتی یا مؤلفه‌های سیستم‌ها] قرار می‌دهد تا دسترسی آسان و ایمن را برای کارکنان تسهیل نماید.

پ. از سیستم قطع اضطراری انرژی در برابر فعال‌سازی غیرمجاز حفاظت می‌کند.

راهنمایی تکمیلی: این کنترل به طور عمده برای تأسیساتی اطلاق می‌شود که حاوی تجمعات منابع سیستم اطلاعاتی، نظیر مراکز داده، اتاق‌های سرور و اتاق‌های رایانه مرکزی، هستند. کنترل مربوطه: PE-15.

کنترل پیشرفته:

۱. خاموشی اضطراری / فعال‌سازی اتفاقی یا غیرمجاز

[حذف شد: به بخش PE-10 منتقل شد.]

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	PE-10 اولویت متوسط	PE-10 اولویت بالا

PE-11: انرژی اضطراری

کنترل: سازمان یک منبع انرژی بدون‌قطعی (UPS) کوتاه‌مدت را به منظور تسهیل [انتخاب (یکی یا بیشتر): خاموش کردن منظم و مناسب سیستم‌های اطلاعاتی، گذار سیستم‌های اطلاعاتی به منبع انرژی جایگزین و بلندمدت] تأمین می‌کند.

راهنمایی تکمیلی: کنترل مربوطه: AT-3، CP-2 و CP-7.

کنترل‌های پیشرفته:

(۱) انرژی اضطراری / منبع انرژی جایگزین و بلندمدت، قابلیت عملیاتی حداقلی

سازمان یک منبع انرژی جایگزین و بلندمدت را سیستم‌های اطلاعاتی فراهم می‌کند که در صورت قطعی طولانی منبع انرژی اصلی، می‌تواند قابلیت‌های عملیاتی را در حداقل سطح الزامی حفظ نماید.

راهنمایی تکمیلی: این کنترل پیشرفته را می‌توان مثلاً با به‌کارگیری منبع انرژی تجاری دست‌دوم یا سایر منابع انرژی خارجی رعایت نمود. می‌توان منابع انرژی جایگزین و طولانی‌مدت برای سیستم‌های اطلاعاتی را به صورت دستی یا خودکار فعال نمود.

(۲) انرژی اضطراری / منبع انرژی جایگزین و بلندمدت، خودکفایی

سازمان سازمان یک منبع انرژی جایگزین و بلندمدت را سیستم‌های اطلاعاتی فراهم می‌کند که:

الف. خودکفا است.

ب. به منبع خارجی تولید انرژی متکی نیست.

پ. در صورت قطعی طولانی منبع انرژی اصلی، می‌تواند [انتخاب: قابلیت‌های عملیاتی را در حداقل سطح الزامی، قابلیت‌های عملیاتی را سطح کامل] حفظ نماید.

راهنمایی تکمیلی: این کنترل پیشرفته را می‌توان مثلاً با به‌کارگیری یک یا چند ژنراتور با ظرفیت کافی برای مطابقت با نیازهای سازمان رعایت نمود. می‌توان منابع انرژی جایگزین و طولانی‌مدت برای سیستم‌های اطلاعاتی را به صورت دستی یا خودکار فعال نمود.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	PE-11 اولویت متوسط	PE-11 (1) اولویت بالا

PE-12: نورپردازی اضطراری

کنترل: سازمان نورپردازی اضطراری و خودکار را برای سیستم‌های اطلاعاتی به کار می‌برد و حفظ می‌نماید که در صورت قطعی انرژی یا تداخل، فعال می‌شود و خروجی‌های اضطراری و مسیرهای تخلیه و خروج در تأسیسات را پوشش می‌دهد.

راهنمایی تکمیلی: این کنترل به طور عمده برای تأسیساتی اطلاق می‌شود که حاوی تجمعات منابع سیستم اطلاعاتی، نظیر مراکز داده، اتاق‌های سرور و اتاق‌های رایانه مرکزی، هستند. کنترل‌های مربوطه: CP-2 و CP-7.

کنترل پیشرفته:

۱. نورپردازی اضطراری / مأموریت‌های اساسی و ضروری و عملکردهای کسب‌وکار

سازمان نورپردازی اضطراری را برای همه مناطق درون تأسیسات که شامل مأموریت‌های اساسی و ضروری و عملکردهای کسب‌وکار می‌شوند، فراهم می‌کند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	PE-12 اولویت پایین	PE-12 اولویت متوسط	PE-12 اولویت بالا

PE-13: حفاظت در برابر آتش‌سوزی

کنترل: سازمان، دستگاه‌ها و سیستم‌های شناسایی و اطفای آتش‌سوزی را برای آن دسته از سیستم‌های اطلاعاتی که توسط یک منبع انرژی مستقل پشتیبانی می‌شوند، به کار می‌گیرد و نگهداری می‌کند.

راهنمایی تکمیلی: این کنترل به طور عمده برای تأسیساتی اطلاق می‌شود که حاوی تجمعات منابع سیستم اطلاعاتی، نظیر مراکز داده، اتاق‌های سرور و اتاق‌های رایانه مرکزی، هستند. سیستم‌های آب‌پاش، کپسول‌های دستی، استخرهای آب ثابت و حسگرهای دود نمونه‌هایی از دستگاه‌ها و سیستم‌های شناسایی و اطفای آتش‌سوزی هستند.

کنترل‌های پیشرفته:

(۱) حفاظت در برابر آتش‌سوزی / دستگاه‌ها و سیستم‌های شناسایی

سازمان از دستگاه‌ها و سیستم‌های شناسایی آتش‌سوزی برای سیستم‌های اطلاعاتی استفاده می‌کند که به صورت خودکار فعال می‌شوند و در صورت بروز آتش‌سوزی، [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] و [اختصاص: پاسخ‌دهنده‌های اضطراری تعیین‌شده توسط سازمان] را مطلع می‌سازند.

راهنمایی تکمیلی: در صورتی که افراد ذکرشده در لیست اطلاع‌رسانی باید مجوزهای دسترسی و یا تأییدیه‌های مخصوصی داشته باشند، مثلاً برای دسترسی یافتن به تأسیساتی که در آن‌ها عملیات‌های محرمانه انجام می‌شود یا سیستم‌های اطلاعاتی حاوی اطلاعات محرمانه قرار دارد، سازمان‌ها می‌توانند کارکنان، نقش‌ها و پاسخ‌دهنده‌های مشخصی را برای این کار در نظر بگیرند.

(۲) حفاظت در برابر آتش‌سوزی / دستگاه‌ها و سیستم‌های اطفای آتش‌سوزی

سازمان از دستگاه‌هاو سیستم‌های اطفای حریق برای سیستم‌های اطلاعاتی استفاده می‌کند که از قابلیت اطلاع‌رسانی خودکار به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] و [اختصاص: پاسخ‌دهنده‌های اضطراری تعیین‌شده توسط سازمان] پس از هر فعال‌سازی را دارند.

راهنمایی تکمیلی: در صورتی که افراد ذکرشده در لیست اطلاع‌رسانی باید مجوزهای دسترسی و یا تأییدیه‌های مخصوصی داشته باشند، مثلاً برای دسترسی یافتن به تأسیساتی که در آن‌ها عملیات‌های محرمانه انجام می‌شود یا سیستم‌های اطلاعاتی حاوی اطلاعات محرمانه قرار دارد، سازمان‌ها می‌توانند کارکنان، نقش‌ها و پاسخ‌دهنده‌های مشخصی را برای این کار در نظر بگیرند.

(۳) حفاظت در برابر آتش‌سوزی / اطفای خودکار آتش‌سوزی

هنگامی که کارکنان به صورت پیوسته در تأسیسات حضور ندارند، سازمان از سیستم خودکار اطفای آتش‌سوزی برای سیستم‌های اطلاعاتی استفاده می‌کند.

(۴) حفاظت در برابر آتش‌سوزی / بررسی‌ها

سازمان اطمینان حاصل می‌کند که تأسیسات [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] توسط بازرسان مجاز و دارای صلاحیت مورد بررسی قرار بگیرد و نقص‌های شناسایی‌شده را [اختصاص: در مدت زمان تعیین‌شده توسط سازمان] بر طرف نماید.

مراجع: وجود ندارد.

اولویت و تخصیص اولیت:

P1	PE-13 اولویت پایین	(3) PE-13 اولویت متوسط	(3)(2)(1) PE-13 اولویت بالا

PE-14: کنترل‌های دما و رطوبت

کنترل: سازمان:

الف. سطح دما و رطوبت در تأسیسات حاوی سیستم‌های اطلاعاتی را در [اختصاص: سطوح قابل قبول که توسط سازمان تعیین می‌شوند] حفظ می‌کند.

ب. سطح دما و رطوبت را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] پایش می‌کند.

راهنمایی تکمیلی: این کنترل به طور عمده برای تأسیساتی اطلاق می‌شود که حاوی تجمعات منابع سیستم اطلاعاتی، نظیر مراکز داده، اتاق‌های سرور و اتاق‌های رایانه مرکزی، هستند. کنترل مربوطه: AT-3.

کنترل‌های پیشرفته:

(۱) کنترل‌های دما و رطوبت / کنترل‌های خودکار

سازمان به منظور پیشگیری از نوسانات دمایی و رطوبتی که احتمالاً برای سیستم‌های اطلاعاتی آسیب‌زا هستند، از کنترل‌های خودکار دما و رطوبت در تأسیسات استفاده می‌کند.

(۲) کنترل‌های دما و رطوبت / پایش به همراه هشدار و اطلاع‌رسانی

سازمان از سیستم پایش دما و رطوبت استفاده می‌کند که از قابلیت هشدار و اطلاع‌رسانی در صورت بروز تغییراتی که احتمالاً برای کارکنان و تجهیزات آسیب‌زا هستند، برخوردار است.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	PE-14 اولویت پایین	PE-14 اولویت متوسط	PE-14 اولویت بالا

PE-15: حفاظت در برابر آسیب‌های آب

کنترل: سازمان از سیستم‌های اطلاعاتی در برای آسیب‌های ناشی از نشت آب به وسیله یک دریچه اصلی[۲۱۵] یا دریچه‌های جداسازی که قابل دسترسی هستند، به درستی کار می‌کنند و کارکنان اصلی با آن‌ها آشنا هستند، حفاظت می‌کند.

راهنمایی تکمیلی: این کنترل به طور عمده برای تأسیساتی اطلاق می‌شود که حاوی تجمعات منابع سیستم اطلاعاتی، نظیر مراکز داده، اتاق‌های سرور و اتاق‌های رایانه مرکزی، هستند. می‌توان دریچه‌های جداسازی را در کنار یا به جای دریچه اصلی به کار برد تا جریان آب را در مناطق خاص و حساس بدون تأثیرگذاری بر تمام سازمان قطع نمود. کنترل مربوطه: AT-3.

کنترل‌های پیشرفته:

(۱) حفاظت در برابر آسیب‌های آب / پشتیبانی خودکار

سازمان از سازوکارهای خودکار برای تشخیص وجود آب در محدود سیستم‌های اطلاعاتی و هشدار به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی تکمیلی: حسگرهای تشخیص آب، هشدار و سیستم‌های اطلاع‌رسانی نمونه‌هایی از سازوکارهای خودکار هستند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	PE-15 اولویت پایین	PE-15 اولویت متوسط	PE-15 (1) اولویت بالا

PE-16: تحویل و حذف

کنترل: سازمان برای ورود [مؤلفه‌های سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] به تأسیسات و خروج از آن مجوز صادر می‌کند و این فعالیت را پایش و کنترل می‌کند و سوابق این موارد را حفظ می‌کند.

راهنمایی تکمیلی: ممکن است اعمال مؤثر مجوزها برای ورود و خروج مؤلفه‌های سیستم‌های اطلاعاتی نیازمند محدودسازی دسترسی به بخش‌های تحویل و حتی جداسازی این بخش‌ها از سیستم‌های اطلاعاتی و کتابخانه رسانه‌ها باشد. کنترل‌های مربوطه: CM-3، MA-2، MA-3، MP-5 و SA-12.

[215] Master Shutoff

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	PE-16 اولویت پایین	PE-16 اولویت متوسط	PE-16 اولویت بالا

PE-17: **محل کار جایگزین**

کنترل: سازمان:

الف. [اختصاص: کنترل‌های امنیتی تعیین‌شده توسط سازمان] را در محل‌های کار جایگزین به کار می‌برد.

ب. میزان اثربخی کنترل‌های امنیتی در محل‌های کار جایگزین را از نظر امکان‌پذیر بودن ارزیابی می‌کند.

پ. راهی برای ارتباط کارمندان با کارکنان امنیت اطلاعات، در صورت بروز مشکلات یا حوادث امنیتی، در نظر می‌گیرند.

راهنمایی تکمیلی: تأسیسات دولتی یا مسکن خصوصی کارکنان نمونه‌هایی از محل‌های کار جایگزین هستند. با این که به صورت متداول محل‌های کار جایگزین با محل‌های پردازش جایگزین متفاوت هستند، محل‌های کار جایگزین ممکن است مکان‌های جایگزینی را به عنوان بخشی از عملیات‌های مربوط به رویدادهای آینده ارائه دهند که به آسانی در دسترس هستند. سازمان‌ها ممکن است مجموعه‌های مختلفی از کنترل‌های امنیتی مختلف را برای محل‌های کار جایگزین مشخص یا انواع خاصی از محل‌ها، بسته به نوع فعالیت‌های کاری که در آن محل‌ها انجام می‌شود، تعیین نمایند. این کنترل از فعالیت‌های مربوط به برنامه‌ریزی برای رویدادهای آینده در سازمان‌ها و لایحه فدرال کار از راه دور پشتیبانی می‌کند. کنترل‌های مربوطه: AC-17 و CP-7.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: نشریه ویژه NIST 800-46

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب‌نشده، اولویت پایین	PE-17 اولویت متوسط	PE-17 اولویت بالا

PE-18: **مکان مؤلفه‌های سیستم‌های اطلاعاتی**

کنترل: سازمان مؤلفه‌های سیستم‌های اطلاعاتی را درون تأسیسات قرار می‌دهد تا آسیب‌های احتمالی ناشی از [اختصاص: خطرات فیزیکی و محیطی تعیین‌شده توسط سازمان] و نیز فرصت دسترسی غیرمجاز را به حداقل برساند.

راهنمایی تکمیلی: سیل، آتش‌سوزی، طوفان، زلزله، آتشفشان، اقدامات تروریستی، خرابکاری، پالس الکترومغناطیس (EMP)، تداخل الکتریکی و سایر شکل‌های تابش‌های الکترومغناطیسی نمونه‌هایی از خطرات فیزیکی و محیطی هستند. به علاوه، سازمان‌ها نقاط ورودی‌ها را هم در نظر می‌گیرند؛ چرا که ممکن است افراد غیرمجاز، حتی بدون دریافت مجوز دسترسی، در فاصله نزدیکی از سیستم‌های اطلاعاتی باشند و بنابراین احتمال دسترسی غیرمجاز به ارتباطات سازمانی را افزایش دهد (برای مثال با استفاده از حسگرهای بی‌سیم یا میکروفون). کنترل‌های مربوطه: CP-2، PE-19 و RA-3.

کنترل‌های پیشرفته:

(۱) مکان مؤلفه‌های سیستم‌های اطلاعاتی / محل تأسیسات

سازمان، مکان یا محل تأسیسات حاوی سیستم‌های اطلاعاتی را با در نظر گرفتن خطرات فیزیکی و محیطی برنامه‌ریزی نقشه‌ریزی می‌کند و برای تأسیسات موجود نیز، خطرات فیزیکی و محیطی را به عنوان بخشی از راهبرد کاهش مخاطرات در نظر می‌گیرد.

راهنمایی تکمیلی: کنترل مربوطه: PM-8.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	PE-18 اولویت بالا

PE-19: **نشت اطلاعات**

کنترل: سازمان از سیستم‌های اطلاعاتی در برابر نشت اطلاعات به واسطه پخش شدن امواج الکترومغناطیسی حفاظت می‌کند.

راهنمایی تکمیلی: نشت اطلاعات عبارت است از انتشار عمدی یا غیرعمدی اطلاعات به یک محیط غیرقابل اعتماد به واسطه پخش شدن امواج الکترومغناطیس. طبقه‌بندی‌های امنیتی یا دسته‌بندی‌های سیستم‌های اطلاعاتی (با در نظر گرفتن محرمانگی) و خط‌مشی‌های امنیتی سازمانی، در عمل انتخاب کنترل‌های امنیتی به‌کاررفته برای حفاظت از سیستم‌ها در برابر نشت اطلاعات به واسطه پخش شدن امواج الکترومغناطیسی راهنمایی می‌کند.

کنترل‌های پیشرفته:

(۱) نشت اطلاعات / برنامه‌های ملی و خط‌مشی‌ها و رویه‌های TEMPEST

سازمان اطمینان حاصل می‌کند مؤلفه‌های سیستم‌های اطلاعاتی، ارتباطات داده‌ای وابسته و شبکه‌ها بر اساس طبقه‌بندی امنیتی یا دسته‌بندی اطلاعات و مطابق با برنامه‌های ملی و خط‌مشی‌ها و رویه‌های TEMPEST حفاظت می‌شوند.

مراجع: نشریه FIPS 199

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

PE-20: پایش و ردگیری دارایی‌ها

کنترل: سازمان:

الف. از [اختصاص: فناوری‌های تشخیص مکان دارایی‌ها که توسط سازمان تعیین می‌شوند] برای ردگیری و پایش مکان و حرکت [اختصاص: دارایی‌های تعیین‌شده توسط سازمان] در [اختصاص: مناطق کنترل‌شده که توسط سازمان تعیین می‌شوند] استفاده می‌کند.

ب. اطمینان حاصل می‌کند که فناوری‌های تشخیص مکان دارایی‌ها مطابق با قوانین، دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها و راهنمایی‌های فدرال مربوطه به کار گرفته می‌شوند.

راهنمایی تکمیلی: فناوری‌های تشخیص مکان دارایی‌ها می‌توانند به سازمان‌ها در اطمینان حاصل کردن از ماندن دارایی‌های اساسی و حیاتی، نظیر خودروها یا مؤلفه‌های اساسی سیستم‌های اطلاعاتی، در مکان‌ها مجاز

کمک نمایند. سازمان‌ها با اداره شورای عمومی[۲۱۶] و مسئول ارشد آژانس در مسائل حریم خصوصی (SAOP)[۲۱۷] یا مدیر بخش مسائل حریم خصوصی (CPO)[۲۱۸] در ارتباط با استقرار و به‌کارگیری فناوری‌های تشخیص مکان برای رسیدگی به مسائل جدی حریم خصوصی مشورت می‌کنند.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

[216] Office of the General Counsel
[217] Senior Agency Official for Privacy
[218] Chief Privacy Officer

خانواده: برنامه‌ریزی

PL-1: خط‌مشی و رویه‌های برنامه‌ریزی

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۱۹. خط‌مشی برنامه‌ریزی شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و
۲۰. رویه‌های تسهیل پیاده‌سازی خط‌مشی برنامه‌ریزی و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۱۹. خط‌مشی برنامه‌ریزی؛ و
۲۰. رویه‌های برنامه‌ریزی.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده PL را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: نشریه‌های ویژه NIST 800-12، NIST 800-18 و NIST 800-100.

اولویت و تخصیص به مجموعه‌های پایه:

P1	PL-1 اولویت پایین	PL-1 اولویت متوسط	PL-1 اولویت بالا

PL-2: برنامه‌ریزی برای امنیت سیستم

کنترل: سازمان:

الف. یک برنامه‌ریزی امنیتی برای سیستم‌های اطلاعاتی تدوین می‌کند که دارای ویژگی‌های زیر باشد:

۱. با معماری ITمحور سازمان هماهنگ و منسجم باشد.

۲. مرزهای صدور مجوز برای سیستم را به طور صریح تعیین کند.

۳. اوضاع و شرایط عملیاتی سیستم‌های اطلاعاتی را از نظر مأموریت‌ها و فرایندهای کسب‌وکار شرح دهد.

۴. طبقه‌بندی امنیتی سیستم‌های اطلاعاتی، از جمله عوامل اولیه آن، را مشخص کند.

۵. محیط عملیات سیستم‌های اطلاعاتی و رابطه یا اتصالات آن‌ها با دیگر سیستم‌های اطلاعاتی را شرح دهد.

۶. نمایی کلی از الزامات امنیتی سیستم ارائه دهد.

۷. هر گونه پوشش خارجی مرتبط را در صورت قابل استفاده بودن مشخص می‌کند.

۸. کنترل‌های امنیتی تعبیه‌شده یا برنامه‌ریزی‌شده برای مطابقت با الزامات تعیین‌شده، از جمله دلیل تصمیمات اصلاحی، را شرح دهد.

۹. پیش از پیاده‌سازی برنامه‌ریزی‌ها، توسط مقامات مجاز یا نماینده‌های تعیین‌شده بازبینی و تأیید شود.

ب. نسخه‌هایی از برنامه‌ریزی‌ها را میان [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] توزیع می‌کند و تغییرات بعدی را نیز به آن‌ها اطلاع می‌دهد.

پ. برنامه‌ریزی‌های امنیتی مربوط به سیستم‌های اطلاعاتی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند.

ت. برنامه‌ریزی انجام‌شده را به منظور تأثیر دادن تغییرات سیستم اطلاعاتی و محیط عملیات یا مشکلات شناسایی‌شده در طول پیاده‌سازی برنامه‌ریزی یا ارزیابی‌های کنترل امنیتی، به‌روزرسانی می‌نماید.

ث. از برنامه‌ریزی امنیتی در برابر افشا شدن و ایجاد تغییرات غیرمجاز حفاظت می‌کند.

راهنمایی تکمیلی: برنامه‌ریزی‌های امنیتی، الزامات امنیتی را به مجموعه‌ای از کنترل‌های امنیتی و کنترل‌های پیشرفته تبدیل می‌کند. همچنین برنامه‌ریزی‌های امنیتی در سطحی بالا توضیح می‌دهند که چگونه کنترل‌های امنیتی و کنترل‌های پیشرفته با الزامات امنیتی مطابقت می‌یابند؛ اما توضیحات فنی، جزئی و دقیقی برای طراحی خاص یا پیاده‌سازی کنترل‌های امنیتی و کنترل‌های پیشرفته ارائه نمی‌دهد. برنامه‌ریزی‌های امنیتی حاوی اطلاعات کافی (از جمله تعیین مقادیر پارامترها برای اختصاص‌ها و انتخاب‌ها، به صورت صریح یا با ذکر مرجع) هستند تا امکان طراحی و پیاده‌سازی را به شکلی فراهم کنند که در صورت پیاده‌سازی برنامه‌ریزی‌ها مطابق اهداف تعیین‌شده، آشکارا با اهداف برنامه‌ریزی‌ها و نیز موارد بعدی بررسی و تعیین مخاطرات موجود برای عملیات‌ها و دارایی‌های سازمانی، افراد، سایر سازمان‌ها و کل کشور مطابقت داشته باشند. سازمان‌ها همچنین می‌توانند راهنمایی‌های اصلاحی را برای کنترل‌های امنیتی پایه در ضمیمه ت و حکم شماره ۱۲۵۳ از CNSS به کار ببرند. این حکم دستور می‌دهد که پوشش‌هایی برای استفاده سراسری همگان یا برای لحاظ کردن الزامات، فناوری‌ها یا مأموریت‌ها و محیط‌های تخصصی عملیات (نظیر عملیات‌های تاکتیکی وزارت دفاع آمریکا، زیرساخت کلید عمومی فدرال یا هویت، اطلاعات محرمانه و مدیریت دسترسی در بخش فدرال و عملیات‌های فضایی) تدوین و طراحی شوند. ضمیمه خ راهنمایی‌هایی برای تدوین و طراحی پوشش‌ها ارائه می‌دهد.

نیازی نیست برنامه‌ریزی‌های امنیتی در یک سند واحد گردآوری شوند. می‌توان برنامه‌ریزی‌ها را در مجموعه‌ای از اسناد مختلف، از جمله اسنادی که از پیش وجود داشته‌اند، گردآوری نمود. برنامه‌ریزی‌های امنیتی مؤثر به صورت گسترده و فراوان خط‌مشی‌ها، رویه‌ها و اسناد دیگر (نظیر مشخصه های طراحی و پیاده‌سازی) را به عنوان مرجع معرفی می‌کنند که می‌توان از آن‌ها اطلاعات دقیق‌تری به دست آورد. این امر الزامات مستندسازی مربوط به برنامه‌های امنیتی را کاهش می‌دهد و اطلاعات مرتبط با امنیت در سایر حوزه‌های تثبیت‌شده مدیریتی و عملیاتی وابسته به معماری سازمان، چرخه عمر توسعه سیستم، مهندسی سیستم‌ها و تملیک را حفظ و نگهداری می‌کند. برای مثال، برنامه‌ریزی‌های امنیتی شامل جزئیات برنامه‌ریزی برای رویدادهای آینده یا اطلاعات طرح‌های واکنش به حوادث نمی‌شوند؛ در عوض، به صورت صرحی یا با ارائه مرجع، اطلاعات کافی برای تعیین اهدافی که باید به واسطه این برنامه‌ریزی‌ها حصول شوند، ارائه می‌دهد. کنترل‌های مربوطه:AC-2، AC-6، AC-14، AC-17، AC-20، CA-2، CA-3، CA-7، CM-9، CP-2، IR-8، MA-4، MA-5، MP-2، MP-4، MP-5، PL-7، PM-1، PM-7، PM-8، PM-9، PM-11، SA-5 و SA-17.

کنترل‌های پیشرفته:

(۱) برنامه‌ریزی برای امنیت سیستم / راهنمای عملیاتی

[حذف شد: به بخش PL-7 منتقل شد.]

(۲) برنامه‌ریزی برای امنیت سیستم / معماری عملکردی

[حذف شد: به بخش PL-8 منتقل شد.]

(۳) برنامه‌ریزی برای امنیت سیستم / برنامه‌ریزی و هماهنگ‌سازی با سایر موجودیت‌های سازمانی

به منظور کاهش تأثیر بر روی سایر موجودیت‌های سازمانی، سازمان آن دسته از فعالیت‌های مرتبط با امنیت را که روی سیستم‌های اطلاعاتی تأثیر می‌گذارند، پیش از اجرای آن‌ها، برنامه‌ریزی می‌کند و با [اختصاص: افراد یا گروه‌های تعیین‌شده توسط سازمان] هماهنگ می‌نماید.

راهنمایی تکمیلی: ارزیابی‌های امنیتی، ممیزی‌ها، تعمیر و نگهداری سخت‌افزار و نرم‌افزار، مدیریت به‌روزرسانی‌ها و تست‌های برنامه‌ریزی برای رویدادهای آینده، نمونه‌هایی از فعالیت‌های مرتبط با امنیت هستند. برنامه‌ریزی و هماهنگ‌سازی پیش از اجرا شامل وضعیت‌های اضطراری و غیراضطراری (به عبارت دیگر، وضعیت‌های برنامه‌ریزی‌شده یا وضعیت‌های برنامه‌ریزی‌نشده و غیرفوری) می‌شود. می‌توان فرایند تعیین‌شده توسط سازمان برای برنامه‌ریزی و هماهنگ‌سازی فعالیت‌های مرتبط با امنیت را در صورت مناسبت، در برنامه‌ریزی‌های امنیتی برای سیستم‌های اطلاعاتی یا سایر اسناد ذکر کرد. کنترل‌های مربوطه: CP-4 و IR-4.

مراجع: نشریه ویژه NIST 800-18

اولویت و تخصیص به مجموعه‌های پایه:

P1	PL-2 اولویت پایین	PL-2 (3) اولویت متوسط	PL-2 (3) اولویت بالا

PL-3: به‌روزرسانی برنامه‌ریزی برای امنیت سیستم

[حذف شد: به بخش PL-2 منتقل شد.]

PL-4: قوانین رفتاری

کنترل: سازمان:

الف. برای افرادی که نیازمند دسترسی به سیستم‌های اطلاعاتی هستند، قوانینی را که مسئولیت‌های آن‌ها و رفتار مورد انتظار از آن‌ها در رابطه با اطلاعات و سیستم‌های اطلاعاتی را شرح می‌دهد، برقرار می‌کند و امکان دسترسی به این قوانین را برای آن‌ها آسان می‌نماید.

ب. پیش از صدور مجوز دسترسی به اطلاعات و سیستم‌های اطلاعاتی، یک گواهینامه امضاشده از افرادی که در مورد قبل ذکر شد، دریافت می‌کند که نشان می‌دهد آن‌ها قوانین رفتاری را مطالعه کرده‌اند، آن را درک می‌کنند و می‌پذیرند که مطابق با آن عمل کنند.

پ. قوانین رفتاری را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روزرسانی می‌نماید.

ت. افرادی را که گواهی نسخه قبلی قوانین رفتاری را امضا کرده‌اند، ملزم می‌نماید که نسخه بازبینی‌شده و به‌روزشده قوانین رفتاری بخوانند و دوباره گواهی آن را امضا نمایند.

راهنمایی تکمیلی: این کنترل به کاربران سازمانی اطلاق می‌شود. سازمان‌ها قوانین رفتاری را بر مبنای نقش‌ها و مسئولیت‌های انفرادی افراد در نظر می‌گیرد و برای مثال میان قوانینی که به کاربران ممتاز و قوانینی که به کاربران عمومی اطلاق می‌شوند، تمایز ایجاد می‌کند. وضع قوانین رفتاری برای انواعی از کاربران غیرسازمانی، نظیر افرادی که صرفاً داده‌ها یا اطلاعات را از سیستم‌های اطلاعاتی فدرال دریافت می‌کنند، غیرممکن است. علت این امر، شمار فراوان این چنین کاربران و ماهیت محدود تعاملات آن‌ها با سیستم‌ها است. قوانین رفتاری مربوط به کاربران سازمانی و کاربران غیرسازمانی را می‌توان به عنوان بخشی از AC-8، اعلانیه کاربرد سیستم، برقرار نمود. می‌توان قسمت ب PL-4 (بخش مربوط به امضای گواهینامه از همین کنترل) را به واسطه برنامه‌های آموزشی مربوط به آگاهی امنیتی و برنامه‌های آموزشی مربوط به امنیت مبتنی بر نقش به انجام رساند؛ البته اگر این برنامه‌های آموزشی شامل قوانین رفتاری نیز باشند. سازمان‌ها می‌توانند از امضاهای الکترونیکی نیز برای گواهینامه‌های قوانین رفتاری استفاده نمایند. کنترل‌های مربوطه: AC-2، AC-6، AC-8، AC-9، AC-17، AC-18، AC-19، AC-20، AT-2، AT-3، CM-11، IA-2، IA-4، IA-5، MP-7، PS-6، PS-8 و SA-5.

کنترل‌های پیشرفته:

(۱) قوانین رفتاری / محدودیت‌های رسانه‌ها و شبکه‌ها اجتماعی

سازمان در قوانین رفتاری، محدودیت‌هایی صریح در خصوص استفاده از رسانه‌ها و شبکه‌های اجتماعی و پخش کردن اطلاعات سازمانی در وب‌سایب‌های عمومی تعیین می‌کند.

راهنمایی تکمیلی:این کنترل پیشرفته به قوانین رفتاری مربوط به استفاده از رسانه‌ها و شبکه‌های اجتماعی در موارد مقابل می‌کند: (۱) هنگامی که کارکنان سازمانی از چنین سایت‌هایی برای وظایف رسمی یا در روند انجام کسب‌وکار رسمی استفاده نمایند؛ (۲) هنگامی که اطلاعات سازمانی در تراکنش‌های رسانه‌ها و شبکه‌های اجتماعی دخیل باشد و (۳) هنگامی که کارکنان از سیستم‌های اطلاعاتی سازمانی به منظور دسترسی به رسانه‌ها و شبکه‌های اجتماعی استفاده نمایند. سازمان‌ها همچنین قوانین مشخصی را وضع می‌کنند که از دستیابی یا استنباط اطلاعات سازمانی غیرعمومی (نظیر اطلاعات حساب کاربری سیستم و اطلاعات شناسایی افراد) توسط موجودیت‌های غیرمجاز از طریق رسانه‌ها و شبکه‌های اجتماعی پیشگیری می‌کند.

مراجع: نشریه ویژه NIST 800-18

اولویت و تخصیص به مجموعه‌های پایه:

P2	PL-4 اولویت پایین	(1) PL-4 اولویت متوسط	(1) PL-4 اولویت بالا

PL-5: ارزیابی تأثیرات حریم خصوصی

[حذف شد: به ضمیمه د AR-2 منتقل شد.]

PL-6: برنامه‌ریزی برای فعالیت‌های مرتبط با امنیت

[حذف شد: به بخش PL-2 منتقل شد.]

PL-7: راهنمای عملیاتیِ امنیتی

کنترل: سازمان:

الف. یک راهنمایی عملیاتی (CONOPS) از جنبه امنیتی برای سیستم‌های اطلاعاتی با پایین‌ترین سطح محتویات تدوین می‌کند که توضیح می‌دهد از دید امنیت اطلاعات، سازمان میل دارد به چه شکل با سیستم‌ها کار کند.

ب. CONOPS را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روزرسانی می‌نماید.

راهنمای تکمیلی: ممکن است CONOPS امنیتی به تناسب، به عنوان بخشی از طرح و نقشه امنیتی برای سیستم‌های اطلاعاتی یا سایر اسناد مربوط به چرخه عمر توسعه سیستم‌ها تدوین شود. تغییراتی که در CONOPS ایجاد می‌شوند در به‌روزرسانی‌های در حال اعمال در طرح و نقشه امنیتی، معماری امنیت اطلاعات و سایر اسناد سازمانی مرتبط (نظیر تبصره‌های امنیتی برای تهیه و تدارکات یا تملیک‌ها، اسناد چرخه عمر توسعه سیستم‌ها و اسناد مهندسی سیستم و امنیت) نمود می‌یابند. کنترل مربوطه: PL-2.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

PL-8: معماری امنیت اطلاعات

کنترل: سازمان:

الف. معماری امنیت اطلاعات را برای سیستم‌های اطلاعاتی به گونه‌ای طراحی می‌کند که از ویژگی‌های زیر برخوردار باشد:

۱. فلسفه، الزامات و رویکرد کلی را برای حفاظت از محرمانگی، یکپارچگی و آماده‌ی کار بودن اطلاعات سازمانی شرح دهد.

۲. توضیح دهد که معماری امنیت اطلاعات چگونه در معماری سازمان تلفیق می‌شود و از آن پشتیبانی می‌کند.

۳. هر گونه نگرش امنیت اطلاعات به خدمات خارجی و نیز وابستگی به آن‌ها را شرح می‌دهد.

ب. معماری امنیت اطلاعات را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روزرسانی می‌نماید تا به‌روزرسانی‌های انجام‌شده در معماری سازمان را اعمال کرده باشد.

پ. اطمینان حاصل می‌کند که تغییرات برنامه‌ریزی‌شده برای معماری امنیت اطلاعات در طرح و نقشه امنیتی، راهنمای عملیاتیِ امنیتی (CONOPS) و فرایندهای تهیه و تدارکات و تملیک‌های سازمانی نمود می‌یابند.

راهنمایی تکمیلی: این کنترل به اقدامات سازمان‌ها در جهت طراحی و توسعه سیستم‌های اطلاعاتی مربوط می شود. اگر معماری امنیت اطلاعات را فقط در سطح امنیت اطلاعات در نظر بگیریم، با آن شکل از معماری امنیت اطلاعات که جهانی‌تر است و در سراسر سازمان به‌کار می‌رود، هماهنگ و منسجم است و آن را تکمیل می‌کند. شکل جهانی‌تر و سراسری معماری امنیت اطلاعات در بخش PM-7 توضیح داده شده است و بخشی اساسی از معماری سازمان است که در همین قالب نیز تدوین می‌گردد. معماری امنیت اطلاعات شامل توضیحات مرتبط با معماری، جایگذاری یا تخصیص کارکردهای امنیتی (از جمله کنترل‌های امنیتی)، اطلاعات مربوط به امنیت برای واسط‌های خارجی، اطلاعات در حال تبادل در سطح واسط‌ها و سازوکارهای حفاظتی مربوط به هر یک از واسط‌ها می‌شود. به علاوه، معماری امنیتی می‌تواند شامل سایر اطلاعات مهم مربوط به امنیت نیز بشود؛ نظیر نقش‌های کاربران و امتیازات دسترسی اختصاص‌یافته به هر نقش، الزامات امنیتی منحصربه‌فرد، انواع اطلاعات پردازش‌شده، ذخیره‌شده و ارسال‌شده توسط سیستم‌های اطلاعاتی، اولویت‌های بازگردانی اطلاعات و خدمات سیستم‌های اطلاعاتی و هر گونه نیازهای خاص حفاظتی دیگر.

در معماری نوین امروزی، کمتر دیده می‌شود که سازمان‌ها همه منابع اطلاعات را کنترل نمایند. در آینده، وابستگی‌هایی کلیدی به ارائه‌دهندگان خارجی خدمات اطلاعاتی و سرویس‌دهندگان خارجی دیده خواهد شد. تشریح چنین وابستگی‌هایی در معماری امنیت اطلاعات، اقدامی مهم جهت تدوین یک راهبرد جامع حفاظت از مأموریت و کسب‌وکار است. برقراری، توسعه و مستندسازی یک پیکربندی پایه برای سیستم‌های اطلاعاتی سازمانی و نگه داشتن آن تحت کنترل پیکربندی، به منظور پیاده‌سازی و تعمیر و نگهداری یک معماری امنیت اطلاعات مؤثر بسیار مهم و اساسی است. تدوین و توسعه معماری امنیت اطلاعات با مسئول ارشد آژانس در مسائل حریم خصوصی (SAOP)[۲۱۹] یا مدیر بخش مسائل حریم خصوصی (CPO)[۲۲۰] هماهنگ می‌شود تا اطمینان حاصل شود که کنترل‌های امنیتی مورد نیاز جهت پشتیبانی از الزامات حریم خصوصی مشخص و به نحو مؤثر پیاده‌سازی خواهند شد. بخش PL-8 به طور عمده در ارتباط با سازمان‌ها است (به عبارت دیگر، تمرکز آن داخلی است) تا مطمئن بود که سازمان یک معماری امنیت اطلاعات برای سیستم‌های اطلاعاتی تدوین خواهند کرد و آن که این معماری امنیتی به واسطه معماری امنیت اطلاعات سراسری سازمان‌ها با معماری سازمانی تلفیق شود یا عمیقاً با آن پیوند بخورد. در مقابل، SA-17 به طور عمده متوجه توسعه‌دهندگان و یکپارچه‌کننده‌های خارجی محصولات و سیستم‌های IT است (اگرچه می‌توان SA-17 را به صورت داخلی و برای توسعه داخلی سیستم‌ها نیز به کار گرفت). SA-17 که تکمیل‌کننده PL-8 است، هنگامی انتخاب می‌شود که سازمان‌ها توسعه سیستم‌های اطلاعاتی یا مؤلفه‌های سیستم‌های اطلاعاتی را به موجودیت‌های خارجی

[219] Senior Agency Official for Privacy
[220] Chief Privacy Officer

برون‌سپاری می‌کند و نیاز است که میان آن‌ها و معماری سازمانی و معماری سیستم‌های اطلاعاتی سازمان هماهنگی و انسجام به وجود آید. کنترل‌های مربوطه: CM-2، CM-6، PL-2، PM-7، SA-5، SA-17 و ضمیمه د.

کنترل‌های پیشرفته:

(۱) معماری امنیت اطلاعات / دفاع در عمق

سازمان معماری امنیتی خودش با رویکرد دفاع در عمق طراحی می‌کند به گونه‌ای که:

الف. [اختصاص: ضامن‌های امنیتی تعیین‌شده توسط سازمان] را به [اختصاص: مکان‌ها و لایه‌های معماری تعیین‌شده توسط سازمان] تخصیص دهد.

ب. اطمینان حاصل نماید که ضامن‌های امنیت تخصیص‌یافته به شکل هماهنگ و تقویت‌کننده یکدیگر عمل می‌کنند.

راهنمایی تکمیلی: سازمان‌ها ضامن‌های امنیتی (رویه‌ای، فنی یا هر دو) را به صورت راهبردی در معماری امنیتی تخصیص می‌دهند تا به این ترتیب متخلفان مجبور باشند چندین ضامن مختلف را پشت سر بگذارند تا به اهداف خود دست یابند. ملزم ساختن متخلفان به گذر از چندین سازوکار مختلف، موفقیت در حمله به منابع اطلاعاتی اساسی و حیاتی را بسیار دشوارتر می‌سازد (به عبارت دیگر، میزان کار و زحمت متخلفان را افزایش می‌دهد) و احتمال شناسایی را نیز بیشتر می‌نماید. هماهنگی ضامن‌های تخصیص‌یافته اطمینان حاصل می‌کند حمله‌ای که فقط یک ضامن را درگیر می‌کند، پیامدهای نامطلوب و ناخواسته‌ای (نظیر قفل شدن و هشدارهای زنجیره‌ای) را به واسطه دخالت در ضامن‌های دیگر ایجاد نخواهد کرد. قرار دادن و تبعیه کردن ضامن‌های امنیتی، یک اقدام کلیدی محسوب می‌شود. حساسیت و اهمیت بیشتر دارایی‌ها یا ارزش اطلاعات موجب به نیاز به لایه‌های اضافی می‌شود. بنابراین، سازمان می‌تواند انتخاب کند که نرم‌افزار آنتی‌ویروس را در لایه‌های مرزی سازمان، سرورهای ایمیل و وب، رایانه‌های نوت‌بوک و ایستگاه‌های رایانه‌ای قرار دهد تا تعداد ضامن‌هایی را که متخلفان باید از آن‌ها عبور کنند تا بتوانند به اطلاعات و سیستم‌های اطلاعاتی دسترسی بیابند، به حداکثر برساند. کنترل‌های مربوطه: SC-29 و SC-36.

(۲) معماری امنیت اطلاعات / تنوع تأمین‌کنندگان

سازمان الزامی می‌داند که [اختصاص: ضامن‌های امنیتی تعیین‌شده توسط سازمان] و تخصیص‌یافته به [اختصاص: مکان‌ها و لایه‌های معماری تعیین‌شده توسط سازمان] از تأمین‌کنندگان مختلفی تهیه شود.

راهنمایی تکمیلی: محصولات IT گوناگون، نقاط قوت و ضعف متفاوتی دارند. تهیه طیف گسترده‌ای از محصولات سبب تکمیل ویژگی‌های انفرادی هر یک از آن‌ها است. برای مثال، سازندگانی که محصولاتی برای حفاظت در برابر کدهای مخرب ارائه می‌دهند، محصولات خود را در زمان‌های متفاوتی به‌روزرسانی می‌کنند و اغلب راهکارهای مقابله با ویروس‌ها، تروجان‌ها و کرم‌های شناخته‌شده را بر اساس اولویت‌ها و برنامه‌های خود توسعه می‌دهند. با قرار دادن محصولات مختلف در مکان‌های مختلف (نظیر سرورها، مرزها و دسکتاپ)، احتمال این که دست‌کم یکی از این‌ها کد مخرب را شناسایی کند، افزایش می‌یابد. کنترل مربوطه: SA-12.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	PL-8 اولویت متوسط	PL-8 اولویت بالا

PL-9: مدیریت مرکزی

کنترل مرکزی: سازمان به صورت مرکزی [اختصاص: کنترل‌های امنیتی تعیین‌شده توسط سازمان و فرایندهای مربوطه] را مدیریت می‌کند.

راهنمایی تکمیلی: مدیریت مرکزی به مدیریت سراسری سازمان و پیاده‌سازی کنترل‌های امنیتی انتخاب‌شده و فرایندهای مربوطه گفته می‌شود. مدیریت مرکزی شامل برنامه‌ریزی، پیاده‌سازی، ارزیابی، صدور مجوز و پایش کنترل‌ها و فرایندهایی که توسط سازمان تعیین می‌شوند و به صورت مرکزی مدیریت می‌شوند، می‌گردد. از آنجایی که مدیریت مرکزی کنترل‌های امنیتی معمولاً با کنترل‌های متداول ارتباط دارد، چنین مدیریتی وظیفه ترویج و تسهیل استانداردسازی پیاده‌سازی و مدیریت کنترل‌های امنیتی و استفاده مناسب و به‌جا از منابع سازمانی را بر عهده دارد. همچنین ممکن است کنترل‌ها و فرایندهای امنیتی با مدیریت مرکزی با الزامات استقلال در ارزیابی‌ها نیز مطابقت داشته باشند؛ ارزیابی‌هایی که از مجوزهای اولیه و جاری برای فعالیت به عنوان بخشی از پایش مستمر سازمانی پشتیبانی می‌کنند. سازمان‌ها به عنوان بخشی از فرایند انتخاب کنترل‌های امنیتی، بر اساس منابع و قابلیت‌های سازمانی مشخص می‌کنند که چه کنترل‌هایی ممکن است برای مدیریت مرکزی مناسب باشند. سازمان‌ها این نکته را در نظر می‌گیرند که ممکن است همیشه امکان آن وجود نداشته باشد که همه جنبه‌های یک کنترل امنیتی را به صورت مرکزی مدیریت کرد. در چنین مواردی، آن کنترل امنیتی به صورت یک کنترل ترکیبی تلقی می‌شود و به صورت مرکزی یا در سطح سیستم اطلاعاتی مدیریت و

پیاده‌سازی می‌شود. نمونه‌هایی از آن دسته از کنترل‌ها و کنترل‌های پیشرفته که گزینه‌های مناسبی برای مدیریت مرکزی به صورت کامل یا جزئی به حساب می‌آیند، عبارتند از: AC-2(1) (2) (3) (4)، AC-17 (1) (2) (9)، AC-18 (1) (3) (4) (5)، AC-19 (4)، AC-22، AC-23، AT-2 (1) (2)، AT-3 (1) (2) (3)، AT-4، CA-2 (1) (2) (3)، CA-3 (1) (2) (3)، CA-7 (1)، CA-9، CM-2 (1) (2)، CM-3 (1) (4)، CM-4، CM-6 (1)، CM-7 (4) (5)، CM-8 (همه کنترل‌ها)، CM-9 (1)، CM-10، CM-11، CP-7 (همه کنترل‌ها)، CP-8 (همه کنترل‌ها)، SC-43، SI-2، SI-3، SI-7 و SI-8.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: نشریه ویژه NIST 800-37

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

خانواده: امنیت کارکنان

PS-1: خط‌مشی و رویه‌های امنیت کارکنان

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۲۱. خط‌مشی امنیت کارکنان شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و

۲۲. رویه‌های تسهیل پیاده‌سازی خط‌مشی امنیت کارکنان و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۲۱. خط‌مشی امنیت کارکنان؛ و

۲۲. رویه‌های امنیت کارکنان.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده PS را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: رهنمود شماره ۱ فدرال در مورد امنیت کارکنان؛ شماره‌های ویژه NIST 800-12, 800-34, 800-100.

اولویت و تخصیص به مجموعه‌های پایه:

P1	PS-1 اولویت پایین	PS-1 اولویت متوسط	PS-1 اولویت بالا

PS-2: تبیین درجه مخاطره مقام‌ها

کنترل: سازمان:

الف. به همه جایگاه‌های سازمانی یک درجه مخاطره نسبت می‌دهد.

ب. معیارهای غربال افرادی را که قرار است که آن جایگاه‌ها را داشته باشند، تعیین می‌کنند.

پ. درجه مخاطره مقام‌ها را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌نماید.

راهنمایی تکمیلی: تبیین درجه مخاطره مقام‌ها، نمود خط‌مشی و راهنمایی اداره مدیریت کارکنان[۲۲۱] است. درجه‌های مخاطره می‌توانند در خصوص انواع مجوزهایی که افراد در هنگام دسترسی به اطلاعات و سیستم‌های اطلاعاتی سازمانی دریافت می‌کنند، راهنمایی و آگاه‌سازی نمایند. معیارهای غربالگری جایگاه شامل الزامات صریح انتصاب نقش‌های امنیت اطلاعات (نظیر آموزش و تأییدیه امنیتی) می‌شود. کنترل‌های مربوطه: AT-3، PL-2 و PS-3.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: 5 C.F.R. 731.106

اولویت و تخصیص پایه:

P1	PS-2 اولویت پایین	PS-2 اولویت متوسط	PS-2 اولویت بالا

PS-3: غربالگری کارکنان

کنترل: سازمان:

الف. پیش از صدور مجوز دسترسی به سیستم‌های اطلاعاتی برای افراد، آن‌ها را غربال می‌کند.

ب. افراد را مطابق با [اختصاص: شرایط تعیین‌شده توسط سازمان که بازغربالگری را الزامی می‌نمایند و در مواردی که باید بازغربالگری انجام شود، بازه‌های زمانی آن را تعیین می‌کنند] بازغربالگری می‌کنند.

[221] Office of Personnel Management

راهنمایی تکمیلی: فعالیت‌های غربالگری و بازغربالگری کارکنان، نمود قوانین، دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، راهنمایی‌ها و معیارهای مشخص و تعیین‌شده برای درجه‌های مخاطره جایگاه‌های انتصابی هستند. ممکن است سازمان‌ها شرایط و بازه‌های زمانی مختلفی را بر اساس انواع اطلاعات پردازش‌شده، ذخیره‌شده یا ارسال‌شده به وسیله سیستم‌ها، برای غربالگری کارکنانی که به سیستم‌های اطلاعاتی دسترسی دارند، تعیین نمایند. کنترل‌های مربوطه: AC-2، IA-4، PE-2 و PS-2.

کنترل‌های پیشرفته:

(۱) غربالگری کارکنان / اطلاعات محرمانه

سازمان اطمینان حاصل می‌کند افرادی که به یک سیستم اطلاعاتی در حال پردازش، ذخیره‌سازی یا ارسال اطلاعات محرمانه دسترسی دارند، تأییدیه داشته باشند و برای دسترسی به بالاترین سطح دسته‌بندی اطلاعات قابل دسترسی برای آن‌ها در آن سیستم آموزش دیده باشند.

راهنمایی تکمیلی: کنترل‌های مربوطه: AC-3 و AC-4

(۲) غربالگری کارکنان / آموزش رسمی

سازمان اطمینان حاصل می‌کند افرادی که به یک سیستم اطلاعاتی در حال پردازش، ذخیره‌سازی یا ارسال انواع خاصی از اطلاعات محرمانه و ملزوم به دریافت آموزش‌های رسمی، دسترسی دارند، برای دسترسی به همه انواع اطلاعات مربوطه که در آن سیستم به آن‌ها دسترسی دارند، آموزش دیده باشند.

(۳) غربالگری کارکنان / اطلاعات مشمول تمهیدات حفاظتی خاص

سازمان اطمینان حاصل می‌کند افرادی که به یک سیستم اطلاعاتی در حال پردازش، ذخیره‌سازی یا ارسال اطلاعات مشمول حفاظت خاص دسترسی دارند، :

الف. دارای مجوزهای دسترسی معتبر باشند که در قالب وظایف رسمی و تفویض‌شده دولت بروز می‌یابد.

ب. با [اختصاص: معیارهای جانبی تعیین‌شده توسط سازمان برای غربالگری کارکنان] مطابقت داشته باشند.

راهنمایی تکمیلی: اطلاعات غیرمحرمانه ولی کنترل‌شده (CUI) و اطلاعات منابع و روش‌ها (SAMI)[۲۲۲] نمونه‌هایی از اطلاعات سازمانی ملزوم به تمهیدات حفاظتی خاص هستند. الزامات غربالگری مربوطه به سابقه حساسیت جایگاه افراد نمونه‌هایی از معیارهای امنیت کارکنان هستند.

مراجع: 5 C.F.R. 731.106، نشریه FIPS 199، نشریه‌های ویژه NIST 800-60، NIST 800-73، NIST800-76، NIST 800-78 و ICD 704

اولویت و تخصیص به مجموعه‌های پایه:

P1	PS-3 اولویت پایین	PS-3 اولویت متوسط	PS-3 اولویت بالا

PS-4: خاتمه دوره کارکنان

کنترل: در هنگام خاتمه دوره کار افراد، سازمان:

الف. امکان دسترسی به سیستم‌های اطلاعاتی را در [اختصاص: مدت زمان تعیین‌شده توسط سازمان] غیرفعال می‌نماید.

ب. هر گونه اطلاعات محرمانه یا وسیله احراز هویت مربوط به فرد را ابطال می‌نماید و از بین می‌برد.

پ. مصاحبه‌های هنگام خروج فرد انجام می‌دهد. این مصاحبه‌ها شامل بحث درباره [اختصاص: موضوعات تعیین‌شده توسط سازمان در ارتباط با امنیت اطلاعات] می‌شود.

ت. همه متعلقات سیستم‌های اطلاعاتی سازمانی مربوط به امنیت را بازپس می‌گیرد.

ث. دسترسی به آن دسته از اطلاعات و سیستم‌های اطلاعاتی سازمانی را که پیش از این در کنترل آن فرد بوده‌اند، حفظ می‌کند.

ج. [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] را در [اختصاص: مدت زمان تعیین‌شده توسط سازمان] مطلع می‌نماید.

راهنمایی تکمیلی: توکن‌های سخت‌افزاری احراز هویت، دفترچه‌های راهنمای فنی مدیریت سیستم، کلیدها، کارت‌های شناسایی و حکم‌های عبور و مرور نمونه‌هایی از متعلقات سیستم‌های اطلاعاتی هستند. انجام مصاحبه‌های هنگام خروج فرد تضمین می‌کند که افرادی که دوره کار آن‌ها پایان یافته است، قید و بندهای

[222] Sources and Methods Information

امنیتی ناشی از سابقه اشتغال را درک می‌کنند و نیز از دستیابی به سطح مطلوبی از پاسخگویی برای متعلقات سیستم‌های اطلاعاتی اطمینان حاصل می‌کند. یادآوری توافق‌نامه‌های عدم‌افشا و محدودیت‌های احتمالی برای شغل‌های آتی به افرادی که دوره کار آن‌ها پایان یافته است، از جمله موضوعات امنیتی مورد توجه در مصاحبه‌های هنگام خروج فرد است. ممکن است انجام مصاحبه‌های هنگام خروج برای برخی از افرادی که دوره کار آن‌ها پایان یافته است؛ برای مثال به علت ترک شغل، بیماری یا عدم حضور مسئولان ارشد مربوطه. انجام مصاحبه‌های هنگام خروج برای افراد دارای تأییدیه‌های امنیتی بسیار مهم است. اجرای به‌موقع اقدامات مربوط به خاتمه دوره کار برای برخی از افرادی که دوره کار آن‌ها به دلایل خاصی پایان یافته است، اساسی و مهم است. سازمان‌ها در شرایط خاصی، پیش از آگاه کردن افراد از خاتمه دوره کار آن‌ها، حساب‌های کاربری آن‌ها در سیستم‌های اطلاعاتی را می‌بندند. کنترل‌های مربوطه: AC-2، IA-4، PE-2، PS-5 و PS-6.

کنترل‌های پیشرفته:

(۱) خاتمه دوره کار کارکنان

سازمان:

الف. افرادی را که دوره کار آن‌ها خاتمه یافته است، نسبت به الزامات قانونی مربوطه و جاری در دوره پس از اشتغال برای حفاظت از اطلاعات سازمانی مطلع می‌نمایند.

ب. افرادی را که دوره کار آن‌ها خاتمه یافته است، ملزم می‌نماید که یک تعهدنامه شامل الزامات دوره پس از اشتغال را به عنوان بخشی از فرایند خاتمه دوره کار سازمانی امضا نمایند.

راهنمایی تکمیلی: سازمان‌ها با اداره شورای عمومی درباره مسائل مربوط به الزامات دوره پس از اشتغال افرادی که دوره کار آن‌ها خاتمه یافته است، مشورت می‌کنند.

(۲) خاتمه دوره کار کارکنان / اطلاع‌رسانی خودکار

سازمان از سازوکارهایی خودکار برای اطلاع دادن به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] در هنگام خاتمه دوره کار یک فرد استفاده می‌کند.

راهنمایی تکمیلی: در سازمان‌های بزرگ با شمار کارکنان بسیار زیاد، همه کارکنانی که باید درباره اقدامات مربوط به خاتمه دوره کار آگاه باشند، به شیوه مناسب اطلاع‌رسانی نمی‌شوند و در مواردی که اطلاع‌رسانی صورت می‌پذیرد، ممکن است به‌موقع و در زمان درست انجام نشود. می‌توان در هنگام خاتمه دوره کار افراد، از سازوکارهای خودکار برای ارسال اطلاعیه‌ها یا هشدارهای خودکار به نقش‌ها یا

کارکنان سازمانی مشخص (نظیر کارکنان مدیریت، مسئولان ارشد، مأموران امنیت کارکنان، مأموران امنیت اطلاعات، مدیران سیستم‌ها یا مدیران IT) استفاده نمود. اطلاعیه‌ها یا هشدارهای خودکار را می‌توان به شکل‌های مختلفی ارسال نمود؛ برای مثال با استفاده از تماس تلفنی، ایمیل، پیام متنی یا وب‌سایت.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	PS-4 اولویت پایین	PS-4 اولویت متوسط	PS-4 (2) اولویت بالا

PS-5: انتقال کارکنان

کنترل: سازمان:

الف. در هنگام انتصاب مجدد یا انتقال افراد به جایگاه‌های دیگر در سازمان، نیازهای عملیاتی جاری در خصوص مجوزهای دسترسی فیزیکی و منطقی به سیستم‌های اطلاعاتی و تأسیسات را بازبینی و تأیید می‌کند.

ب. [اختصاص: اقدامات تعیین‌شده توسط سازمان مربوط به انتصاب مجدد یا انتقال افراد] را در [اختصاص: مدت زمان تعیین‌شده توسط سازمان پس از انتقال رسمی] را در دستور کار قرار می‌دهد.

پ. مجوزهای دسترسی را بر حسب نیاز تغییر می‌دهد تا با هر گونه تغییرات در نیازهای عملیاتی به علت انتصاب مجدد یا انتقال افراد مطابقت داشته باشند.

ت. [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] را در [اختصاص: مدت زمان تعیین‌شده توسط سازمان] مطلع می‌نماید.

راهنمایی تکمیلی: این کنترل هنگامی اطلاق می‌شود که انتصاب مجدد یا انتقال افراد دائمی یا به اندازه‌ای طولانی باشد که انجام این اقدامات را ضروری نماید. سازمان‌ها اقدامات مناسب برای انواع انتصاب‌های مجدد یا انتقال‌ها، چه دائمی چه طولانی‌مدت، را تعیین می‌نمایند. از جمله اقداماتی که ممکن است برای انتصاب مجدد یا انتقال کارکنان به سایر جایگاه‌ها در سازمان الزامی باشند عبارتند از: (۱) بازگرداندن کلیدهای قدیمی و صادر کردن کلیدها، کارت‌های شناسایی و مجوزهای عبور و مرور جدید (۲) بستن حساب‌های کاربری در سیستم‌های اطلاعاتی و ساخت‌های حساب‌های جدید (۳) تغییر مجوزهای دسترسی به سیستم‌های اطلاعاتی (نظیر امتیازات) و (۴) فراهم کردن امکان دسترسی به آن دسته از سوابق رسمی که افراد در مکان کاری قبلی و در

حساب‌های کاربری قبلی در سیستم‌های اطلاعاتی به آن‌ها دسترسی داشتند. کنترل‌های مربوطه: AC-2، IA-4، PE-2 و PS-4.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص‌های اولیه:

P2	PS-5 اولویت پایین	PS-5 اولویت متوسط	PS-5 اولویت بالا

PS-6: توافق‌نامه‌های دسترسی

کنترل: سازمان:

الف. توافق‌نامه‌های دسترسی برای سیستم‌های اطلاعاتی سازمانی را تهیه و مستندسازی می‌نماید.

ب. توافق‌نامه‌های دسترسی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روزرسانی می‌نماید.

پ. اطمینان حاصل می‌کند که افرادی که نیازمند دسترسی به اطلاعات و سیستم‌های اطلاعاتی سازمانی هستند:

۱. پیش از دریافت اجازه دسترسی، توافق‌های دسترسی مربوطه را امضا نمایند.

۲. هنگامی که توافق‌نامه‌های دسترسی [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] به‌روزرسانی می‌شوند، توافق‌نامه‌های دسترسی را به منظور حفظ دسترسی به سیستم‌های اطلاعاتی سازمانی دوباره امضا نمایند.

راهنمایی تکمیلی: توافق‌نامه‌های عدم‌افشا، توافق‌نامه‌های کاربرد قابل قبول، قوانین رفتاری و توافق‌نامه‌های تعارض منافع[۲۲۳] نمونه‌هایی از توافق‌نامه‌های دسترسی هستند. توافق‌نامه‌های دسترسی امضاشده شامل یک تعهدنامه هستند که افراد آن را می‌خوانند، آن را می‌فهمند و می پذیرند که از قید و بندهای مربوط به سیستم‌های اطلاعاتی سازمانی که دسترسی به آن‌ها مجاز است، تبعیت کنند. سازمان‌ها می‌توانند از امضاهای

[223] Conflict Of Interest

الکترونیکی برای تثبیت توافق‌نامه‌های دسترسی استفاده نمایند؛ مگر آن که این کار به طور مشخص به وسیله خط‌مشی سازمانی ممنوع شده باشد. کنترل‌های مربوطه: PL-4، PS-2، PS-3، PS-4 و PS8.

کنترل‌های پیشرفته:

(۱) توافق‌نامه‌های دسترسی / اطلاعات نیازمند تمهیدات حفاظتی خاص

[حذف شد: به بخش PS-3 منتقل شد.]

(۲) توافق‌نامه‌های دسترسی / اطلاعات محرمانه و نیازمند تمهیدات حفاظتی خاص

سازمان اطمینان حاصل می‌کند که اجازه دسترسی به اطلاعات محرمانه و مشمول تمهیدات حفاظتی خاص فقط به افرادی داده شود که:

الف. دارای یک مجوز دسترسی معتبر باشند که در قالب وظایف رسمی و تفویض‌شده دولت بروز می‌یابد.

ب. با معیارهای مربوطه امنیت کارکنان مطابقت داشته باشند.

پ. توافق‌نامه عدم‌افشا را خوانده باشند، فهمیده باشند و امضا کرده باشند.

راهنمایی تکمیلی: اطلاعات جانبی، برنامه دسترسی خاص (SAP)[۲۲۴] و اطلاعات بخش‌شده و حساس (SCI)[۲۲۵] نمونه‌هایی از اطلاعات محرمانه نیازمند تهمیدات حفاظتی خاص هستند. معیارهای امنیت کارکنان بازگوکننده قوانین، دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها و راهنمایی‌های فدرال مربوطه هستند.

(۳) توافق‌نامه‌های دسترسی / الزامات دوره پس از اشتغال

سازمان:

الف. افرادی را که دوره کار آن‌ها خاتمه یافته است، نسبت به الزامات قانونی مربوطه و جاری در دوره پس از اشتغال برای حفاظت از اطلاعات سازمانی مطلع می‌نمایند.

ب. در صورت مشمولیت، افرادی را که دوره کار آن‌ها خاتمه یافته است، ملزم می‌نماید که یک تعهدنامه شامل این الزامات را به عنوان بخشی از ارائه دسترسی اولیه به اطلاعات پوشش‌یافته امضا نمایند.

[224] Special Access Program
[225] Sensitive Compartmented Information

راهنمایی تکمیلی: سازمان‌ها سازمان‌ها با اداره شورای عمومی درباره مسائل مربوط به الزامات دوره پس از اشتغال افرادی که دوره کار آن‌ها خاتمه یافته است، مشورت می‌کنند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	PS-6 اولویت پایین	PS-6 اولویت متوسط	PS-6 اولویت بالا

PS-7: امنیت کارکنان شخص ثالث

کنترل: سازمان:

الف. الزامات مربوط به امنیت کارکنان شامل نقش‌ها و مسئولیت‌های امنیتی تأمین‌کنندگان شخص ثالث را وضع می‌کند.

ب. تأمین‌کنندگان شخص ثالث را ملزم می‌نماید که از خط‌مشی‌ها و رویه‌های شخص ثالث وضع‌شده پیروی کنند.

پ. الزامات امنیت کارکنان را مستند می‌نماید.

ت. تأمین‌کنندگان شخص ثالث را ملزم می‌نماید که [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] را در [اختصاص: مدت زمانی تعیین‌شده توسط سازمان] از هر گونه انتقال یا خاتمه دوره کار کارکنان شخص ثالثی که اطلاعات محرمانه سازمانی یا نشان دارند یا از امتیازات سیستم‌های اطلاعاتی برخوردار هستند، مطلع نمایند.

ث. تأمین‌کنندگان را از نظر پیروی از قوانین پایش می‌نماید.

راهنمایی تکمیلی: دفاتر خدمات، پیمانکارها و سایر سازمان‌های فراهم‌کننده سیستم‌های اطلاعاتی توسعه‌یافته، خدمات فناوری اطلاعات، برنامه‌های کاربردی برون‌سپاری‌شده و مدیریت شبکه و امنیت نمونه‌هایی از تأمین‌کنندگان شخص ثالث هستند. سازمان‌ها به صورت صریح الزامات امنیت کارکنان را در اسناد مربوط به تملیک‌ها ذکر می‌کنند. ممکن است کارکنانی از جانب تأمین‌کنندگان شخص ثالث با دارا بودن اطلاعات محرمانه، نشان‌ها یا امتیازات سیستم‌های اطلاعاتی که توسط سازمان صادر شده‌اند، در تأسیسات سازمانی کار کنند. اطلاع‌رسانی در خصوص تغییر در کارکنان شخص ثالث تضمین می‌کند که امتیازات و اطلاعات محرمانه در اختیار فرد به صورت صحیح و مناسب منقضی شوند. سازمان‌ها، موارد انتقال و خاتمه دوره کار را که بر اساس ویژگی‌های مرتبط با امنیت باید گزارش شوند، تعیین می‌نمایند. این ویژگی‌ها عبارتند از: عملکردها، نقش‌ها و

ماهیت اطلاعات محرمانه و امتیازات مرتبط لا افرادی که منتقل شده‌اند یا دوره کار آن‌ها خاتمه یافته است. کنترل‌های مربوطه: PS-2، PS-3، PS-4، PS-5، PS-6، SA-9 و SA-21.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: نشریه ویژه NIST 800-35

اولویت و تخصیص به مجموعه‌های پایه:

P1	PS-7 اولویت پایین	PS-7 اولویت متوسط	PS-7 اولویت بالا

PS-8: محرومیت‌های کارکنان

کنترل: سازمان:

الف. برای افرادی که از خط‌مشی‌ها و رویه‌های امنیت اطلاعات وضع‌شده پیروی نکنند، یک فرایند رسمی محرومیت به کار می‌برد.

ب. هنگامی که فرایند رسمی محرومیت کارکنان در دستور کار قرار گیرد، [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] را در [اختصاص: مدت زمانی تعیین‌شده توسط سازمان] مطلع می‌نماید تا فرد محروم‌شده و علت محرومیت وی شناسایی شود.

راهنمایی تکمیلی: فرایندهای محرومیت سازمانی بازگوکننده قوانین، دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها و راهنمایی‌های فدرال مربوطه هستند. فرایندهای محرومیت در توافق‌نامه‌های دسترسی آورده و توضیح داده می‌شوند و می‌توانند به عنوان بخشی از خط‌مشی‌ها و رویه‌های عمومی کارکنان در سازمان‌ها مطرح شوند. سازمان‌ها با اداره شورای عمومی در خصوص مسائل مربوط به محرومیت‌های کارکنان مشورت می‌کنند. کنترل‌های مربوطه: PL-4 و PS-6.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P3	PS-8 اولویت پایین	PS-8 اولویت متوسط	PS-8 اولویت بالا

خانواده: ارزیابی مخاطرات

RA-1: خط‌مشی و رویه‌های ارزیابی مخاطرات

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۲۳. خط‌مشی ارزیابی مخاطرات شامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و

۲۴. رویه‌های تسهیل پیاده‌سازی خط‌مشی ارزیابی مخاطرات و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۲۳. خط‌مشی ارزیابی مخاطرات؛ و

۲۴. رویه‌های ارزیابی مخاطرات.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده RA را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: نشریه ویژه NIST 800-12، NIST 800-30 و NIST 800-100

اولویت و تخصیص به مجموعه‌های پایه:

P1	RA-1 اولویت پایین	RA-1 اولویت متوسط	RA-1 اولویت بالا

RA-2: **طبقه‌بندی امنیتی**

کنترل: سازمان:

الف. اطلاعات و سیستم‌های اطلاعاتی را مطابق با قوانین، دستورات اجرایی، رهنمودها، خط‌مشی‌ها، مقررات، استانداردها و راهنمایی‌های فدرال مربوطه طبقه‌بندی می‌کند.

ب. نتایج طبقه‌بندی امنیتی (و از جمله دلایل منطقی آن) را در طرح و نقشه امنیتی برای سیستم‌های اطلاعاتی مستند می‌نماید.

پ. اطمینان حاصل می‌کند که مسئول صدور مجوز یا مسئول صدور مجوزی که به عنوان نماینده منصوب می‌شود، تصمیمات مربوط به طبقه‌بندی امنیتی را بازبینی و تأیید می‌کند.

راهنمایی تکمیلی: تعیین دقیق و واضح مرزهای صدور مجوز، پیش‌نیازی برای مؤثر واقع شدن تصمیمات طبقه‌بندی امنیتی به حساب می‌آید. طبقه‌بندی‌های امنیتی توضیح می‌دهند که در صورتی که اطلاعات و سیستم‌های اطلاعاتی سازمانی به واسطه از بین رفتن محرمانگی، یکپارچگی و آماده‌ی کار بودن، در معرض خطر قرار بگیرند، احتمالاً چه پیامدهای نامطلوبی به عملیات‌ها و دارایی‌های سازمانی و افراد وارد می‌شود. سازمان‌ها فرایند طبقه‌بندی امنیتی را به صورت یک فعالیت سازمانی سراسری و با همکاری مدیران ارشد اطلاعات، مقامات ارشد امنیت اطلاعات، صاحبان سیستم‌های اطلاعاتی، صاحبان مأموریت و کسب‌وکار و صاحبان یا مأموران اطلاعات انجام می‌دهند. سازمان‌ها همچنین پیامدهای نامطلوب و احتمالی تهدیدکننده سایر سازمان‌ها و نیز، بر اساس لایحه میهن‌پرستی آمریکا[۲۲۶] در سال ۲۰۰۱ و رهنمودهای ریاست‌جمهوری به وزارت امنیت داخلی آمریکا، پیامدهای نامطلوب احتمالی در سطح ملی را در نظر می‌گیرند. فرایندهای طبقه‌بندی امنیتی انجام‌شده توسط سازمان، تهیه و توسعه انبارهای دارایی‌های اطلاعاتی و همراه با CM-8، نقشه‌کشی‌های مؤلفه‌های خاصی از سیستم‌های اطلاعاتی را در جایی که اطلاعات پردازش، ذخیره یا ارسال می‌شوند، تسهیل می‌نماید. کنترل‌های مربوطه: CM-8، MP-4، RA-3 و SC-7.

کنترل‌های مربوطه: وجود ندارد.

مراجع: نشریه FIPS 199، نشریه ویژه NIST 80-30، NIST 800-39 و NIST 800-60.

[226] USA PATRIOT Act

اولویت و تخصیص به مجموعه‌های پایه:

P1	RA-2 اولویت پایین	RA-2 اولویت متوسط	RA-2 اولویت بالا

RA-3: ارزیابی مخاطرات

کنترل: سازمان:

الف. مخاطرات و نیز احتمال و شدت آسیب ناشی از دسترسی غیرمجاز، کاربرد، افشا، اختلال، تغییر یا تخریب سیستم‌های اطلاعاتی و اطلاعاتی را که این سیستم‌ها پردازش، ذخیره یا ارسال می‌نمایند، ارزیابی می‌کند.

ب. نتایج ارزیابی مخاطرات را در [اختصاص: اسناد مربوط به [انتخاب: طرح و نقشه امنیتی، گزارش ارزیابی مخاطرات] که سازمان تعیین می‌کند]، مستند می‌نماید.

پ. نتایج ارزیابی مخاطرات را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند.

ت. نتایج ارزیابی مخاطرات را در [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد.

ث. ارزیابی مخاطرات را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] یا در هر زمان که تغییرات قابل توجهی در سیستم‌های اطلاعاتی یا محیط عملیات‌ها (از جمله شناسایی تهدیدات و آسیب‌پذیری‌های جدید) ایجاد می‌شوند یا در هر شرایط دیگری که ممکن است روی وضعیت امنیتی سیستم تأثیر بگذارد، بازبینی می‌کند.

راهنمایی تکمیلی: تعیین دقیق و واضح مرزهای صدور مجوز، پیش‌نیازی برای مؤثر واقع شدن ارزیابی‌های مخاطرات به حساب می‌آید. تهدیدات، آسیب‌پذیری‌ها، احتمال و تأثیرات دامن‌گیر عملیات‌ها و دارایی‌های سازمانی، افراد، سایر سازمان‌ها و کشور، بر اساس عملیات و کاربرد سیستم‌های اطلاعاتی در ارزیابی‌های مخاطرات در نظر گرفته می‌شوند. مخاطرات ناشی از گروه‌های خارجی (نظیر ارائه‌دهندگان خدمات، پیمانکارانی که سیستم‌های اطلاعاتی را به نمایندگی از طرف سازمان اداره می‌کنند، افرادی که به سیستم‌های اطلاعاتی سازمانی دسترسی دارند و موجودیت‌های دخیل در برون‌سپاری‌ها) نیز در ارزیابی‌های مخاطرات در نظر گرفته می‌شوند. مطابق با خط‌مشی OMB و طرح احراز هویت الکترونیکی مربوطه، ممکن است نیاز باشد به منظور حفاظت از اطلاعات غیرعمومی و اطلاعات مربوط به حریم خصوصی، آن دسته از کاربران عمومی که به سیستم‌های اطلاعاتی فدرال دسترسی می‌یابند، نیز احراز هویت شوند. بر این اساس، ارزیابی‌های سازمانی از مخاطرات به دسترسی‌های عمومی به سیستم‌های اطلاعاتی فدرال را لحاظ می‌کنند.

ارزیابی‌های مخاطرات (چه رسمی و چه غیررسمی) را می‌توان در هر سه سطح از سلسله مدیریت مخاطرات (به عبارت دیگر، سطح سازمان، سطح فرایند مأموریت و کسب‌وکار یا سطح سیستم‌های اطلاعاتی) و در هر مرحله‌ای از چرخه عمر توسعه سیستم انجام داد. همچنین می‌توان ارزیابی‌های مخاطرات را در گام‌های متعدد در چارچوب مدیریت مخاطرات، از جمله طبقه‌بندی، انتخاب کنترل امنیتی، پیاده‌سازی کنترل امنیتی، ارزیابی کنترل امنیتی، صدور مجوز برای سیستم‌های اطلاعاتی و پایش کنترل امنیتی، انجام داد. قابل توجه است که باید RA-3 را قبل از پیاده‌سازی سایر کنترل‌ها تا درجه پیاده‌سازی نمود تا دو گام اول چارچوب مدیریت مخاطرات را تکمیل نمود. ارزیابی‌های مخاطرات می‌توانند نقشی مهم در فرایندهای انتخاب کنترل امنیتی، به خصوص در طول اعمال راهنمایی اصلاحی که شامل کنترل‌های امنیتی مکمل می‌شود، داشته باشند. کنترل‌های مربوطه: RA-2 و PM-9.

کنترل‌های مربوطه: وجود ندارد.

مراجع: تفهیم‌نامه OMB 04-04، نشریه ویژه NIST 80-30، NIST 800-39 و آدرس وب: http://idmanagement.gov.

اولویت و تخصیص به مجموعه‌های پایه:

P1	RA-3 اولویت پایین	RA-3 اولویت متوسط	RA-3 اولویت بالا

RA-4: به‌روزرسانی ارزیابی مخاطرات

[حذف شد: به بخش RA-3 منتقل شد.]

RA-5: پویش آسیب‌پذیری‌ها

کنترل: سازمان:

الف. آسیب‌پذیری‌های موجود در سیستم‌های اطلاعاتی و برنامه‌های کاربردی روی آن‌ها را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان و یا به صورت تصادفی مطابق با فرایندهای تعیین‌شده توسط سازمان] و نیز در هنگام شناسایی و گزارش آسیب‌پذیری‌های جدیدی که احتمالاً روی سیستم‌ها یا برنامه‌های کاربردی تأثیر می‌گذارند، پویش می‌کند.

ب. از ابزارها و شگردهای پویش آسیب‌پذیری که هم‌کنش‌پذیری[۲۲۷] میان ابزارها و قطعات خودکار در فرایند مدیریت آسیب‌پذیری، را به واسطه استانداردهای زیر تسهیل می‌کنند، استفاده می‌کند:

۱. مشخص کردن پلت‌فرم‌ها، نقایص نرم‌افزاری و پیکربندی‌های نادرست

۲. قالب‌بندی چک‌لیست‌ها و رویه‌های تست

۳. سنجش تأثیر آسیب‌پذیری‌ها

پ. گزارش‌ها و نتایج پویش آسیب‌پذیری حاصل از ارزیابی‌های کنترل امنیتی را تجزیه و تحلیل می‌کند.

ت. آسیب‌پذیری‌های شناخته‌شده را [اختصاص: در طول زمان تعیین‌شده توسط سازمان برای واکنش نشان دادن] و مطابق با ارزیابی سازمانی از مخاطرات اصلاح می‌کند.

ث. اطلاعات به‌دست‌آمده از فرایند پویش آسیب‌پذیری و ارزیابی‌های کنترل امنیتی را با [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] به اشتراک می‌گذارد تا به حذف آسیب‌پذیری‌های مشابه در سایر سیستم‌های اطلاعاتی (به عبارت دیگر ضعف‌ها یا ناکارامدی‌های سیستمی) کمک نماید.

راهنمایی تکمیلی: طبقه‌بندی امنیتی سیستم‌های اطلاعاتی راهنمایی‌هایی در خصوص دفعات و جامعیت پویش‌های آسیب‌پذیری ارائه می‌دهد. سازمان‌ها پویش آسیب‌پذیری را برای همه مؤلفه‌های سیستم‌های اطلاعاتی الزامی می‌کنند تا اطمینان حاصل شود که از منابع احتمالی آسیب‌پذیری نظیر پرینترها، اسکنرها و دستگاه‌های کپیِ متصل به شبکه غفلت نخواهد شد. ممکن است تجزیه و تحلیل‌های آسیب‌پذیری برای برنامه‌های کاربردی نرم‌افزاری و سفارشی به روش‌های مضاعفی، نظیر تجزیه و تحلیل ایستا، تجزیه و تحلیل پویا، تجزیه و تحلیل دوتایی یا ترکیبی از این سه روش، نیاز داشته باشند. سازمان‌ها می‌توانند این روش‌های تجزیه و تحلیل را در قالب انواع مختلفی از ابزارها (نظیر پویشگرهای تحت وب برای برنامه‌های کاربردی، ابزارهای تجزیه و تحلیل ایستا و سیستم‌های تجزیه و تحلیل دوتایی) و در بازبینی‌های سورس‌کدها به کار بگیرند. نمونه‌هایی از پویش آسیب‌پذیری عبارتند از: (۱) پویش سطوح به‌روزرسانی، (۲) پویش عملکردها، پورت‌ها، پروتکل‌ها و خدماتی که نباید برای کاربران یا دستگاه‌ها قابل دسترسی باشند و (۳) پویش سازوکارهای کنترل جریان اطلاعات با پیکربندی یا عملکرد نادرست. سازمان‌ها گزینه به‌کارگیری ابزارهایی را که آسیب‌پذیری‌ها را به شیوه نام‌گذاری رایج CVE یا آسیب‌پذیری‌ها و افشاهای متداول[۲۲۸] گزارش می‌کنند و از زبان باز ارزیابی آسیب‌پذیری (OVAL)[۲۲۹] برای برای تشخیص یا تست وجود آسیب‌پذیری استفاده می‌کنند، در نظر می‌گیرند. فهرست

[227] Interoperability
[228] Common Vulnerabilities and Exposures
[229] Open Vulnerability Assessment Language

ضعف‌های متداول (CWE)[۲۳۰] و پایگاه داده ملی آسیب‌پذیری (NVD)[۲۳۱] نمونه‌هایی از منابع پیشنهادی برای اطلاعات آسیب‌پذیری هستند. به علاوه، ارزیابی‌های کنترل امنیتی نظیر مانور تیم‌های قرمز نیز منابع دیگری برای پویش آسیب‌پذیری‌های احتمالی هستند. همچنین سازمان‌ها گزینه به‌کارگیری ابزارهایی را که تأثیرات آسیب‌پذیری‌ها را به واسطه سیستم متداول امتیازبندی آسیب‌پذیری‌ها (CVSS)[۲۳۲] گزارش می‌دهند، در نظر می‌گیرند. کنترل‌های مربوطه: CA-2، CA-7، CM-4، CM-6، RA-2، RA-3، SA-11 و SI-2.

کنترل‌های پیشرفته:

(۱) پویش آسیب‌پذیری / قابلیت به‌روزرسانی ابزار

سازمان از دسته‌ای از ابزارهای پویش آسیب‌پذیری استفاده می‌کند که می‌توان مجموعه مرجع آن برای آسیب‌پذیری‌های سیستم‌های اطلاعاتی را به راحتی به‌روزرسانی نمود.

راهنمایی تکمیلی: همچنان که آسیب‌پذیری‌های جدید کشف و اعلام می‌شوند و شیوه‌های پویش نیز توسعه می‌یابند، مجموعه آسیب‌پذیری‌هایی که باید پویش شوند، نیز باید به‌روزرسانی شود. این فرایند به‌روزرسانی کمک می‌نماید بتوان اطمینان حاصل نمود که آسیب‌پذیری‌های احتمالی در سیستم‌های اطلاعاتی شناسایی می‌شوند و در سریع‌ترین زمان ممکن بر طرف می‌شوند. کنترل‌های مربوطه: SI-3 و SI-7.

(۲) پویش آسیب‌پذیری / به‌روزرسانی در بازه‌های زمانی مشخص، پیش از پویش جدید، هنگام شناسایی

سازمان مجموعه آسیب‌پذیری‌هایی را که باید در سیستم‌های اطلاعاتی پویش شوند، [انتخاب (یکی یا بیشتر): [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان، پیش از پویش جدید، هنگامی که آسیب‌پذیری‌های جدید شناسایی و گزارش می‌شوند]، به‌روزرسانی می‌کند.

راهنمایی تکمیلی: کنترل‌های مربوطه: SI-3 و SI-5.

(۳) پویش آسیب‌پذیری / گستره و عمق پوشش

سازمان رویه‌هایی برای پویش آسیب‌پذیری به کار می‌برد که می‌توانند گستره و عمق پوشش را شناسایی کنند (به عبارت دیگر مؤلفه‌های سیستم‌های اطلاعاتی را پویش و آسیب‌پذیری‌ها را بررسی کنند).

[230] Common Weakness Enumeration
[231] National Vulnerability Database
[232] Common Vulnerability Scoring System

(۴) پویش آسیب‌پذیری / اطلاعات قابل کشف

سازمان تشخیص می‌دهد که چه اطلاعاتی درباره سیستم‌های اطلاعاتی برای مهاجمان قابل کشف است و به تبع آن [اختصاص: اقدامات اصلاحی تعیین‌شده توسط سازمان] را انجام می‌دهد.

راهنمایی تکمیلی: اطلاعات قابل کشف شامل اطلاعاتی است که مهاجمان می‌توانند بدون حمله یا نفوذ مستقیم به سیستم‌های اطلاعاتی به دست آورند؛ برای مثال، از طریق جمع‌آوری اطلاعاتی که سیستم در معرض دسترسی قرار می‌دهد یا انجام جستجوهای گسترده و وسیع در وب. اطلاع دادن به کارکنان سازمانی مربوطه، حذف اطلاعات مشخص‌شده یا تغییر سیستم اطلاعاتی به منظور کاهش جذابیت یا ارزش اطلاعات مشخص‌شده برای مهاجمان نمونه‌هایی از اقدامات اصلاحی هستند. کنترل مربوطه: AU-13.

(۵) پویش آسیب‌پذیری / دسترسی ممتاز

سیستم اطلاعاتی برای [اختصاص: فعالیت‌های مربوط به پویش آسیب‌پذیری و تعیین‌شده توسط سازمان]، مجوز دسترسی ممتاز به [اختصاص: مؤلفه‌های سیستم‌های اطلاعاتی تشخیص‌داده‌شده توسط سازمان] صادر می‌کند.

راهنمایی تکمیلی: در شرایط خاصی، ماهیت پویش آسیب‌پذیری ممکن است تهاجمی‌تر و نفوذگرانه‌تر باشد یا آن مؤلفه‌ای از سیستم اطلاعاتی که مورد پویش قرار دارد، ممکن است حاوی اطلاعاتی بسیار حساس باشد. صدور مجوز دسترسی ممتاز به مؤلفه‌های انتخابی از سیستم، امکان پویش کامل‌تر آسیب‌پذیری‌ها را تسهیل می‌کند و نیز از ماهیت حساس چنین پویشی حفاظت می‌نماید.

(۶) پویش آسیب‌پذیری / تجزیه و تحلیل خودکار تحولات

سازمان از سازوکارهای خودکار برای مقایسه نتایج پویش‌های آسیب‌پذیری در گذر زمان استفاده می‌کند تا تحولات ایجادشده در آسیب‌پذیری‌های سیستم‌های اطلاعاتی را تشخیص دهد.

راهنمایی تکمیلی: کنترل‌های مربوطه: IR-4، IR-5 و SI-4.

(۷) پویش آسیب‌پذیری / شناسایی خودکار و اطلاع‌رسانی در خصوص مؤلفه‌های غیرمجاز

[حذف شد: به بخش CM-8 منتقل شد.]

(۸) پویش آسیب‌پذیری / بازبینی سوابق گزارش‌های ممیزی

سازمان سوابق گزارش‌های ممیزی را بازبینی می‌کند تا دریابد که آسیب‌پذیری شناسایی‌شده در سیستم اطلاعاتی، پیش از این مورد سوءاستفاده واقع شده است یا خیر.

راهنمایی تکمیلی: کنترل مربوطه: AU-6.

(۹) پویش آسیب‌پذیری / تست و تجزیه و تحلیل آسیب‌پذیری

[حذف شد: به بخش CA-8 منتقل شد.]

(۱۰) پویش آسیب‌پذیری / ارتباط برقرار کردن میان اطلاعات پویش‌ها

سازمان میان خروجی ابزارهای پویش آسیب‌پذیری ارتباط برقرار می‌کند تا وجود بردارهای حمله با چند آسیب‌پذیری یا چند مسیره[۲۳۳] را تشخیص دهد.

مراجع: نشریه ویژه NIST 800-40، NIST 800-70، NIST 800-115 و آدرس‌های وب: http://cwe.mitre.org و http://nvd.nist.gov.

اولویت و تخصیص به مجموعه‌های پایه:

P1	RA-5 اولویت پایین	RA-5 (1)(2)(5) اولویت متوسط	RA-5 (1)(2)(4)(5) اولویت بالا

RA-6: بررسی اقدامات دفاعی در برابر جاسوسی‌های فنی[۲۳۴]

کنترل: سازمان [انتخاب (یکی یا بیشتر): [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان]، [اختصاص: هنگامی که رویدادهای تعیین‌شده توسط سازمان رخ می‌دهند یا نشانه‌های تعیین‌شده توسط سازمان بروز می‌کنند]]، اقدامات دفاعی در برابر جاسوسی‌های فنی را [اختصاص: در مکان‌های تعیین‌شده توسط سازمان] بررسی می‌کند.

راهنمایی تکمیلی: بررسی اقدامات دفاعی در برابر جاسوسی‌های فنی، توسط کارکنان دارای صلاحیت انجام می‌شود تا در صورت وجود دستگاه‌ها یا عوامل احتمالی جاسوسی فنی، آن‌ها را شناسایی نمود و نیز ضعف‌های فنی و امنیتی موجودی که می‌توانند در نفوذهای فنی در تأسیسات مورد بررسی به کار آیند، مشخص شوند. چنین بررسی‌هایی، موقعیت و وضعیت فنی و امنیتی سازمان و تأسیسات را ارزشیابی می‌کنند و معمولاً شامل بازرسی‌های بصری، الکترونیکی و فیزیکی درون و در اطراف تأسیسات می‌شوند. همچنین این بررسی‌ها، منابع

[233] multi-vulnerability/multi-hop attack vectors
[234] Technical Surveillance countermeasures

اطلاعاتی مناسبی برای ارزیابی‌های مخاطرات و نیز قرار گرفتن سازمان در معرض دسترسی مهاجمان احتمالی فراهم می‌کنند.

کنترل پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، اولویت پایین	انتخاب‌نشده، اولویت متوسط	انتخاب‌نشده، اولویت بالا

خانواده:حفاظت از ارتباطات و سیستم

SC-1: خط‌مشی و رویه‌های حفاظت از ارتباطات و سیستم

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۲۵. خط‌مشی برنامه‌ریزی برای رویدادهای آیندهشامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و

۲۶. رویه‌های تسهیل پیاده‌سازیخط‌مشیبرنامه‌ریزی برای رویدادهای آینده و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۲۵. خط‌مشی برنامه‌ریزی برای رویدادهای آینده؛ و

۲۶. رویه‌های برنامه‌ریزی برای رویدادهای آینده.

راهنمایی‌های تکمیلی: اینکنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانوادهSCرا ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع:نشریه‌های ویژه شماره ۸۰۰-۱۲ و ۸۰۰-۱۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-1سطح تأثیرکم	SC-1سطح تأثیر متوسط	SC-1 سطح تأثیر زیاد

SC-2: بخش‌بندی کاربردها

کنترل:سیستم اطلاعاتی کارکردهای کاربران و خدمات واسط کاربری آن‌ها را از کارکردهای مدیریت سیستم اطلاعاتی تفکیک می‌کند.

راهنمایی‌های تکمیلی:کارکردهای مدیریت سیستم اطلاعاتی مواردی از این دست را در بر می‌گیرند: کارکردهای مورد نیاز برای راهبری پایگاه‌های داده، مؤلفه‌های شبکه، ایستگاه‌های کاری یا سرورها. این کارکردها معمولاً نیازمند اختیارات ویژه توسط کاربر هستند. تفکیک کارکردهای کاربران از کارکردهای مدیریت سیستم اطلاعاتی به شکل فیزیکی یا منطقی اتفاق می‌افتد. سازمان‌ها بدین منظور از رایانه‌های مختلف، واحدهای پردازش مرکزی مختلف، سیستم‌عامل‌های مختلف، آدرس‌های شبکه مختلف، شیوه‌های مجازی‌سازی، یا ترکیبی از این روش‌ها یا روش‌های دیگر استفاده می‌کنند. این نوع تفکیک به عنوان مثال شامل واسط‌های راهبری وب است که روش‌های احراز هویت مجزا برای هر یک از دیگر منابع سیستم اطلاعاتی را به کار می‌گیرند. تفکیک کارکردهای سیستم از کارکردهای کارکنان می‌تواند شامل ایزوله کردن واسط‌های راهبری روی دامنه‌های مختلف و استفاده از کنترل‌های دسترسی اضافی باشد. کنترل‌های مربوطه: SA-4, SA-8, SC-3.

کنترل‌های پیشرفته:

(۱) بخش‌بندی کاربردها / واسط‌های کاربران بدون اختیار ویژه

سیستم اطلاعاتی اجازه نمی‌دهد که کارکردهای مدیریت سیستم اطلاعاتی در واسط کاربران غیر ویژه قرار گیرند.

راهنمایی‌های تکمیلی: با استفاده از این کنترل پیشرفته می‌توان اطمینان حاصل نمود که گزینه‌های راهبری (مانند اختیارات ویژه راهبری) در اختیار کاربران عادی قرار نمی‌گیرند. به عنوان مثال، گزینه‌های راهبری ارائه نمی‌شوند تا زمانی که کاربران اقدام به ایجاد نشست‌هایی با اختیارات ویژه راهبری نمایند. کنترل مربوطه: AC-3.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده،سطح تأثیرکم	SC-2سطح تأثیر متوسط	SC-2 سطح تأثیر زیاد

SC-3: **تفکیک کارکردهای امنیتی**

کنترل:سیستم اطلاعاتی کارکردهای امنیتی را از کارکردهای غیر امنیتی جدا می‌کند.

راهنمایی‌های تکمیلی: سیستم اطلاعاتی با استفاده از یک مرز تفکیکی که به روش بخش‌بندی یا با استفاده از دامنه‌ها محقق می‌شود، کارکردهای امنیتی را از کارکردهای غیر امنیتی جدا می‌کند.این کنترل‌های تفکیکی، به سخت‌افزارها، نرم‌افزارها و ثابت‌افزارهای اجراکننده این کارکردهای امنیتی دسترسی پیدا می‌کنند و از یکپارچگی آن‌ها محافظت می‌نمایند. سیستم‌های اطلاعاتی، تفکیک کدها (یعنی تفکیک کارکردهای امنیتی از کارکردهای غیر امنیتی) را به روش‌های مختلفی انجام می‌دهند که از آن جمله می‌توان به ارائه کرنل‌های امنیتی از طریق حلقه‌های پردازشگر یا مدهای پردازشگر اشاره کرد. در مورد کدهای غیر کرنل، تفکیک کارکردهای امنیتی معمولاً از طریق ابزارهایحفاظتی سیستم فایل انجام می‌شود که وظیفه حفاظت از کدها روی دیسک را بر عهده دارند. سیستم‌های اطلاعاتی دسترسی به کارکردهای امنیتی را با استفاده از سازوکارهای کنترل دسترسی و با پیاده‌سازی قابلیت حداقل بودن اختیارات، محدود می‌کنند. ایده‌آل این است که کدهای موجود در مرز تفکیکی کارکردهای امنیتی تنها شامل کدهای امنیتی باشند، اما گاهی نیز لازم است که کارکردهای غیر امنیتی به طور استثنا وارد مرز تفکیکی شوند. کنترل‌های مربوطه: AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39.

کنترل‌های پیشرفته:

(۱) تفکیک کارکردهای امنیتی / تفکیک سخت‌افزار

سیستم اطلاعاتی با استفاده از سازوکارهای تفکیک سخت‌افزار، کارکردهای امنیتی را تفکیک می‌نماید.

راهنمایی‌های تکمیلی: سازوکارهای تفکیک سخت‌افزار مواردی از این دست را شامل می‌شوند: معماری حلقوی سخت‌افزار که معمولاً در ریزپردازنده‌ها استفاده می‌شود و بخش‌بندی آدرس مبتنی بر سخت‌افزار که برای پشتیبانی از حافظه‌های مجزا از لحاظ منطقی با ویژگی‌های مجزا (یعنی قابل خواندن و قابل نوشتن بودن) به کار گرفته می‌شود.

(۲) تفکیک کارکردهای امنیتی / کارکردهای کنترل جریان و کنترل دسترسی

سیستم اطلاعاتی، کارکردهای امنیتی اجراکننده کنترل‌های جریان اطلاعات و کنترل دسترسی را از کارکردهای غیر امنیتی و همچنین از سایر کارکردهای امنیتی تفکیک می‌کند.

راهنمایی‌های تکمیلی: تفکیک کارکردهای امنیتی نتیجه پیاده‌سازی است؛ این کارکردها را کماکان می‌توان اسکن و پایش کرد. کارکردهای امنیتی که از کارکردهای اجرای کنترل جریان و کنترل دسترسی تفکیک می‌شوند، مواردی از این دست را در بر می‌گیرند: کارکرد ممیزی، کارکرد تشخیص ورود غیر مجاز و کارکرد آنتی‌ویروس.

(۳) تفکیک کارکردهای امنیتی / حداقل کردن کارکردهای غیر امنیتی

سازمان تعداد کارکردهای غیر امنیتی موجود در مرز تفکیکی را به حداقل می‌رساند.

راهنمایی‌های تکمیلی: در صورتی که نتوان کارکردهای امنیتی را به طور کامل از کارکردهای غیر امنیتی تفکیک کرد، باید اقداماتی را برای به حداقل رساندن تعداد کارکردهای غیر امنیتی در مرز تفکیکی به عمل آورد. کارکردهای غیر امنیتی موجود در مرز تفکیک، کارکرد مربوط به امنیت به شمار می‌آیند، زیرا خطاها و بدخواهی‌های نهفته در این نرم‌افزارها می‌تواند بر کارکرد امنیتی سیستم‌های اطلاعاتی سازمان اثر سوء داشته باشد. هدف این است که بخش‌های خاصی از سیستم‌های اطلاعاتی تأمین‌کننده امنیت اطلاعات، دارای حداقل اندازه و پیچیدگی باشند. حداقل کردن تعداد کارکردهای غیر امنیتی به طراحان و پیاده‌سازان امکان می‌دهد تا تنها بر کارکردهایی تمرکز داشته باشند که برای تأمین قابلیت‌های امنیتی مطلوب ضروری هستند. با حداقل کردن تعداد کارکردهای غیر امنیتی در مرز تفکیکی، میزان کدهایی که برای اجرای خط‌مشی‌های امنیتی باید به آن‌ها اعتماد کرد کاهش می‌یابد و در نتیجه سیستم قابل‌درک‌تر می‌شود.

(۴) تفکیک کارکردهای امنیتی / انسجام[۲۳۵] و جفت‌شدگی[۲۳۶] ماژول‌ها

سازمان کارکردهای امنیتی را به عنوان ماژول‌های مستقل پیاده‌سازی می‌کند، به طوری که انسجام درونی بین ماژول‌ها حداکثر و جفت‌شدگی بین آن‌ها حداقل شود.

راهنمایی‌های تکمیلی:کاهش تعامل بین ماژول‌ها باعث محدود شدن کارکردهای امنیتی و سهولت مدیریت پیچیدگی‌ها می‌شود. در حیطه ماژول‌بندی در طراحی نرم‌افزار، مفاهیم انسجام و جفت‌شدگی از اهمیت بالایی برخوردار هستند. منظور از جفت‌شدگی، وابستگی‌هایی است که دو ماژول به یکدیگر

[235] cohesiveness
[236] coupling

دارند. انسجام نیز به رابطه بین توابع مختلف در یک ماژول خاص اشاره دارد. روش‌های خوب مهندسی نرم‌افزار، مبتنی بر تجزیه، لایه‌بندی و حداقل کردن ماژول‌ها هستند تا بتوان پیچیدگی را کاهش داد و آن را بهتر مدیریت کرد. بدین ترتیب، ماژول‌های نرم‌افزاری در اختیار خواهیم داشت که انسجام بیشتر و جفت‌شدگی کمتری دارند.

(۵) تفکیک کارکردهای امنیتی / ساختارهای لایه‌ای

سازمان کارکردهای امنیتی را با ساختار لایه‌ای پیاده‌سازی می‌کند تا تعامل بین لایه‌های مختلف طراحی را حداقل کند و از هر گونه وابستگی لایه‌های پایین‌تر به توابع یا انسجام لایه‌های بالاتر پرهیز کند.

راهنمایی‌های تکمیلی: پیاده‌سازی ساختار لایه‌ای با حداقل تعامل بین کارکردهای امنیتی و لایه‌های غیر حلقوی (یعنی این که توابع لایه‌های پایین‌تر به توابع لایه‌های بالاتر وابستگی نداشته باشند)، امکان تفکیک بهتر کارکردهای امنیتی و مدیریت مؤثرتر پیچیدگی‌ها را فراهم می‌آورد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده،سطح تأثیرکم	انتخاب نشده،سطح تأثیر متوسط	SC-3 سطح تأثیر زیاد

SC-4: اطلاعات موجود در منابع اشتراکی

کنترل:سیستم اطلاعاتی از انتقال غیر مجاز و ناخواسته اطلاعات از طریق منابع اشتراکی سیستم جلوگیری به عمل می‌آورد.

راهنمایی‌های تکمیلی:کنترل حاضر مانع از این می‌شود که اطلاعات و ارائه‌های رمزگذاری‌شده اطلاعات تولیدشده در اثر اقدامات نقش‌ها و کارکنان سابق (یا فرایندهایی که به نمایندگی از آن‌ها عمل می‌کنند)، در اختیار آن دسته از نقش‌ها و کارکنان فعلی (یا فرایندهای فعلی) قرار گیرند که به منابع اشتراکی سیستم (مانند رجیسترها، حافظه اصلی و دیسک‌های سخت) دسترسی دارند (پس از این که منابع مذکور مجدداً در اختیار سیستم‌های اطلاعاتی قرار گرفتند). به فرایند کنترل اطلاعات موجود در منابع اشتراکی معمولاً استفاده مجدد از موجودیت‌های غیر فعال و حفاظت از اطلاعات بایگانی‌شده گفته می‌شود. کنترل حاضر به موارد روبرو نمی‌پردازد:

(۱) پسماند اطلاعات[۲۳۷]، یعنی نمایش اطلاعاتی که پاک یا حذف شده‌اند؛ (۲) کانال‌های مخفی (شامل کانال‌های ذخیره‌سازی و/یا زمان‌بندی) که منابع اشتراکی در آن‌ها دستکاری می‌شوند تا محدودیت‌های جریان اطلاعات را نقض نمایند؛ یا (۳) آن دسته از مؤلفه‌های سیستم‌های اطلاعاتی که تنها یک نقش یا کاربر برای آن‌ها وجود دارد. کنترل‌های مربوطه: AC-3, AC-4, MP-6.

(۱) اطلاعات موجود در منابع اشتراکی / سطوح امنیتی

[حذف شد: به بخش SC-4 منتقل شد].

(۲) اطلاعات موجود در منابع اشتراکی / پردازش سطح‌بندی‌شده[۲۳۸]

هنگامی که سیستم پردازش‌گر بین سطوح مختلف اطلاعات یا دسته‌بندی‌های امنیتی مختلف سوئیچ می‌کند، سیستم اطلاعاتی بر اساس [اختصاص: رویه‌های تعیین‌شده توسط سازمان] از انتقال غیر مجاز اطلاعات از طریق منابع اشتراکی جلوگیری به عمل می‌آورد.

راهنمایی‌های تکمیلی:این کنترل پیشرفته در مواردی اعمال می‌شود که در جریان عملیات سیستم اطلاعاتی، مثلاً در جریان پردازش چندسطحی و پردازش سطح‌بندی‌شده اطلاعات در سطوح یا دسته‌بندی‌های امنیتی مختلف، تغییرات آشکاری در سطح پردازش اطلاعات مشاهده شود. رویه‌های تعیین‌شده توسط سازمان مواردی از جمله فرایند پاکسازی اطلاعات ذخیره‌شده به صورت الکترونیکی را در بر می‌گیرند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده،سطح تأثیرکم	SC-4سطح تأثیر متوسط	SC-4 سطح تأثیر زیاد

SC-5: **حفاظت در برابر حملات** DoS

کنترل: سیستم اطلاعاتی با استفاده از [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان]، با حملات روبرو مقابله می‌کند یا اثرات آن‌ها را کاهش می‌دهد: [انواع حملات DoS تعیین‌شده توسط سازمان یا ارجاع به منابع این اطلاعات].

[237] information remanence

[238] periods processing

راهنمایی‌های تکمیلی: فناوری‌های مختلفی برای کاهش یا حتی حذف اثر حملات DoS ارائه شده‌اند. به عنوان مثال، دستگاه‌های حفاظت مرزی می‌توانند برخی از انواع بسته‌ها را فیلتر کنند و در نتیجه مانع از تأثیر مستقیم حملات DoS روی مؤلفه‌های سیستم اطلاعاتی موجود در شبکه درون‌سازمانی شوند. با افزایش ظرفیت و پهنای باند در کنار استفاده از خدمات جایگزین نیز می‌توان آسیب‌پذیری سیستم در برابر حملات DoS را کاهش داد.
کنترل‌های مربوطه: SC-6, SC-7.

کنترل‌های پیشرفته:

(۱) حفاظت در برابر حملات DoS / محدود کردن کاربران داخلی
سیستم اطلاعاتی امکان انجام [اختصاص: حملات DoS تعیین‌شده توسط سازمان] توسط افراد بر علیه سیستم‌های اطلاعاتی دیگر را محدود می‌کند.
راهنمایی‌های تکمیلی: برای محدود کردن امکان انجام حملات DoS توسط افراد، باید سازوکارهای مورد استفاده در این حملات را از دسترس خارج کرد. منظور از افراد مورد اشاره، متخاصمان داخلی یا خارجی است که با موفقیت به سیستم اطلاعاتی نفوذ کرده‌اند و از آن به عنوان پلت‌فرمی برای حمل به اشخاص ثالث استفاده می‌کنند. سازمان‌ها می‌توانند امکان اتصال افراد به رسانه‌های انتقال اطلاعات (مانند شبکه و ابزارهای بی‌سیم) و ارسال اطلاعات از طریق آن‌ها را محدود کنند. سازمان‌ها همچنین می‌توانند امکان استفاده از تعداد زیادی از منابع سیستم اطلاعاتی توسط افراد را محدود نمایند. مقابله با این حملات DoS ممکن است در برخی سیستم‌های اطلاعاتی خاص یا در دستگاه‌های شبکه انجام شود.

(۲) حفاظت در برابر حملات DoS / فراهم آوردن ظرفیت و پهنای باند اضافی
سیستم اطلاعاتی برای محدود کردن اثر آن دسته از حملات DoS که با روانه کردن سیلی از اطلاعات انجام می‌شوند[۲۳۹]، اقدام به فراهم آوردن ظرفیت و پهنای باند اضافی می‌نماید.
راهنمایی‌های تکمیلی: با فراهم آوردن ظرفیت اضافی می‌توان اطمینان حاصل نمود که ظرفیت کافی برای مقابله با این نوع از حملات DoS وجود دارد. برای نیل به این هدف، می‌توان اقداماتی از قبیل اولویت‌بندی کاربردها، سهمیه‌بندی و بخش‌بندی را انجام داد.

(۳) حفاظت در برابر حملات DoS / ردیابی/پایش
سازمان:

[239] information flooding denial of service attacks

(الف) برای ردیابی نشانه‌های حملات DoS بر علیه سیستم اطلاعاتی، از [اختصاص: ابزارهای پایش تعیین‌شده توسط سازمان] استفاده می‌کند؛ و
(ب) [اختصاص: منابع سیستم اطلاعاتی تعیین‌شده توسط سازمان] را پایش می‌کند تا تعیین کند که آیا منابع کافی برای مقابله با حملات مؤثر DoS وجود دارد یا خیر.
راهنمایی‌های تکمیلی: سازمان‌ها در هنگام مدیریت مخاطرات ناشی از حملات DoS، به قابلیت کاربرد و ظرفیت منابع سیستم اطلاعاتی توجه می‌نمایند. حملات DoS می‌توانند از داخل یا خارج از سازمان نشأت گیرند. برخی از منابع سیستم اطلاعاتی به حملات DoS حساس هستند که از آن جمله می‌توان به حافظه‌های فیزیکی و حلقه‌های CPU اشاره کرد. سازمان‌ها برای مقابله با حملات DoS اقدام به سهمیه‌بندی دیسک می‌کنند، سیستم اطلاعاتی را به گونه‌ای پیکربندی می‌کنند که در هنگام پر شدن یک حافظه به راهبران هشدار دهد، فناوری‌های فشرده‌سازی را برای استفاده بهینه از فضای حافظه به کار می‌گیرند، و بخش‌های مجزایی را به داده‌های کاربری و داده‌های سیستم اختصاص می‌دهند.
کنترل‌های مربوطه: CA-7, SI-4.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-5 سطح تأثیرکم	SC-5سطح تأثیر متوسط	SC-5 سطح تأثیر زیاد

SC-6: آماده کار بودن منابع

کنترل: سیستم اطلاعاتی با تخصیص دادن [اختصاص: منابع تعیین‌شده توسط سازمان] با [انتخاب (یک یا چند مورد): اولویت، سهمیه، [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان]]، آماده کار بودن منابع را تضمین می‌نمایند.

راهنمایی‌های تکمیلی:اولویت‌بندی باعث می‌شود که فرایندهای با اولویت پایین‌تر سبب ایجاد وقفه یا اخلال در فرایندهای با اولویت بالاتر نشوند. سهمیه‌بندی نیز باعث می‌شود که کاربران یا فرایندها تنها به حجمی از منابع دسترسی پیدا کنند که از پیش برای آن‌ها تعیین شده است. آن دسته از مؤلفه‌های سیستم اطلاعاتی که تنها یک نقش یا کاربر برای آن‌ها وجود دارد، شامل این الزام نمی‌شوند.

کنترل‌های پیشرفته:وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده،سطح تأثیرکم	انتخاب نشده،سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-7: **حفاظت مرزی**

کنترل: سیستم اطلاعاتی:

الف. ارتباطات را در مرز خارجی سیستم و در مرزهای داخلی اصلی در سیستم، پایش و کنترل می‌کند؛

ب. شبکه‌هایی فرعی را برای آن دسته از مؤلفه‌های سیستم که در دسترس عموم قرار دارند و به صورت [انتخاب: فیزیکی، منطقی] از شبکه‌های درونی سازمان مجزا شده‌اند، پیاده‌سازی می‌نماید؛ و

پ. تنها از طریق واسط‌های مدیریت‌شده‌ای با شبکه‌ها یا سیستم‌های اطلاعاتی خارجی ارتباط برقرار می‌کند که همسو با معماری امنیتی سازمان، مجهز به دستگاه‌های حفاظت مرزی باشند.

راهنمایی‌های تکمیلی:به عنوان مثال‌هایی از واسط‌های مدیریت‌شده، می‌توان به گیت‌وی‌ها، مسیریاب‌ها، فایروال‌ها، گاردها، سیستم‌های تحلیل و مجازی‌سازی کدهای مخرب مبتنی بر شبکه، یا تونل‌های رمزگذاری‌شده که در معماری امنیتی پیاده‌سازی می‌شوند (مانند مسیریاب‌هایی که از فایروال‌ها یا گیت‌وی‌های برنامه کاربردی مستقر روی شبکه‌های فرعی حفاظت می‌کنند) اشاره کرد. به شبکه‌های فرعی که به صورت منطقی یا فیزیکی از شبکه‌های داخلی مجزا شده‌اند، منطقه غیر نظامی[۲۴۰] یا DMZ گفته می‌شود. برای محدود کردن یا جلوگیری از فعالیت واسط‌ها در سیستم‌های اطلاعاتی سازمان می‌توان اقدامات مختلفی را انجام داد که از آن جمله می‌توان به این موارد اشاره نمود: محدود کردن ترافیک وب خارجی به سرورهای وب تعیین‌شده در واسط‌های مدیریت‌شده و جلوگیری از جریان یافتن ترافیک خارجی که به نظر می‌رسد آدرس‌های داخلی را جعل کرده است. سازمان‌ها در هنگام پیاده‌سازی کنترل‌های امنیتی مربوط به کاربرد این خدمات، به ماهیت اشتراکی خدمات مخابراتی تجاری توجه می‌کنند. خدمات مخابراتی تجاری معمولاً مبتنی بر مؤلفه‌های شبکه و

[240] demilitarized zone

سیستم‌های مدیریت یکپارچه‌ای هستند که بین تمام مشتریان تجاری به اشتراک گذاشته شده‌اند و ممکن است شامل خطوط دسترسی تأمین‌شده توسط شخص ثالث و سایر عناصر خدماتی نیز باشند. حتی با وجود مفاد امنیتی که در قراردادها گنجانده می‌شوند، استفاده از این خدمات ممکن است مخاطراتی را برای سازمان در پی داشته باشد. کنترل‌های مربوطه: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

کنترل‌های پیشرفته:

(۱) حفاظت مرزی / شبکه‌های فرعی با تفکیک فیزیکی

[حذف شد: به بخش SC-7 منتقل شد].

(۲) حفاظت مرزی / دسترسی عمومی

[حذف شد: به بخش SC-7 منتقل شد].

(۳) حفاظت مرزی / نقاط دسترسی

سازمان تعداد اتصالات شبکه خارجی به سیستم اطلاعاتی را محدود می‌نماید.

راهنمایی‌های تکمیلی: با محدود کردن تعداد اتصالات شبکه خارجی، می‌توان ترافیک ارتباطی ورودی و خروجی را به صورت جامع‌تری پایش کرد. به عنوان مثالی از این نوع محدودسازی، می‌توان به پروژه اتصال اینترنتی مورد اعتماد[۲۴۱] (TIC) اشاره کرد.

(۴) حفاظت مرزی / خدمات مخابراتی خارجی

سازمان:

(الف) یک واسط مدیریت‌شده را برای هر خدمت مخابراتی خارجی پیاده‌سازی می‌کند؛

(ب) یک خط‌مشی جریان ترافیک را برای هر خدمت مخابراتی خارجی برقرار می‌سازد؛

(پ) از محرمانگی و یکپارچگی اطلاعات انتقالی از هر واسط محافظت می‌نماید؛

(ت) هر یک از موارد استثنای خط‌مشی جریان ترافیک را به همراه نیاز کسب‌وکار/مأموریت و طول مدت آن نیاز مستندسازی می‌کند؛ و

(ث) موارد استثنای خط‌مشی جریان ترافیک را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی می‌کند و مواردی که دیگر توسط یک نیاز آشکار کسب‌وکار/مأموریت پشتیبانی نمی‌شوند را حذف می‌نماید.

راهنمایی‌های تکمیلی: کنترل مربوطه: SC-8.

[241] Trusted Internet Connection

(۵) حفاظت مرزی / انکار به صورت پیش‌فرض / اجازه دادن با استثنا

سیستم اطلاعاتی در واسط‌های مدیریت‌شده، ترافیک ارتباطی شبکه را به صورت پیش‌فرض انکار می‌کند و با استثنا به آن‌ها اجازه عبور می‌دهد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته هم در مورد ترافیک شبکه ورودی و هم در مورد ترافیک شبکه خروجی اعمال می‌شود. با استفاده از این خط‌مشی می‌توان اطمینان حاصل نمود که تنها اجازه ارتباطات مجاز و تأییدشده داده می‌شود.

(۶) حفاظت مرزی / واکنش به شکست‌های شناسایی‌شده

[حذف شد: به بخش SC-7(18) منتقل شد].

(۷) حفاظت مرزی / جلوگیری از تونل‌زنی مجزا برای دستگاه‌های راه دور

سیستم اطلاعاتیبه دستگاه راه دور اجازه نمی‌دهد که به طور همزمان یک اتصال غیر راه دور را با سیستم برقرار کند و از طریق یک اتصال دیگر نیز با منابع موجود در شبکه‌های خارجی ارتباط برقرار نماید.

راهنمایی‌های تکمیلی:در دستگاه‌های راه دور (مانند لپتاپ‌ها)، این کنترل پیشرفته از طریق تنظیمات پیکربندی پیاده‌سازی می‌شود تا از تونل‌زنی مجزا در این دستگاه‌ها جلوگیری نماید. بدین ترتیب، این تنظیمات توسط کاربران قابل پیکربندی نخواهند بود. در سیستم اطلاعاتی، این کنترل پیشرفته از طریق شناسایی تونل‌زنی مجزا (یا شناسایی آن دسته از تنظیمات پیکربندی که امکان تونل‌زنی مجزا را فراهم می‌آورند) در دستگاه‌های راه دور پیاده‌سازی می‌شود. بدین ترتیب، اگر دستگاه راه دور از تونل‌زنی مجزا استفاده کرده باشد، امکان برقراری اتصال نخواهد داشت. گاهی تونل‌زنی مجزا برای کاربران راه دور مطلوب است (مثلاً برای برقراری ارتباط با منابع محلی سیستم اطلاعاتی مانند چاپگرها و سرورهای فایل). با این حال،تونل‌زنی مجزا در واقع امکان برقراری اتصالات غیر مجاز خارجی را فراهم می‌آورد و سیستم را در معرض خطر حملات و سرقت اطلاعات قرار می‌دهد. در صورتی که VPNها مجهز به کنترل‌های امنیتی کافی باشند، سازمان می‌تواند از آن‌ها برای برقراری اتصالات راه دور استفاده کند و تا حد خوبی اطمینان داشته باشد که یکپارچگی و محرمانگی اطلاعات حفظ می‌شود. بنابراین، با استفاده از VPNها می‌توان مسیرهای ارتباطی غیر راه دور را از دستگاه‌های راه دور برقرار نمود. با این حال، استفاده از یک VPN حفاظت‌شده بدین معنی نیست که می‌توان منع تونل‌زنی مجزا را نادیده گرفت.

(۸) حفاظت مرزی / مسیردهی ترافیک به سمت سرورهای پراکسی احرازهویت‌شده

سیستم اطلاعاتی [اختصاص: ترافیک ارتباطات داخلی تعیین‌شده توسط سازمان] را از طریقسرورهای پراکسی احرازهویت‌شده در واسط‌های مدیریت‌شده، به [اختصاص: شبکه‌های خارجی تعیین‌شده توسط سازمان] مسیردهی می‌کند.

راهنمایی‌های تکمیلی:منظور از شبکه‌های خارجی، شبکه‌هایی است که تحت کنترل سازمان نیستند. منظور از سرور پراکسی، یک سرور (یعنی برنامه کاربردی یا سیستم اطلاعاتی) است که به عنوان میانجی کلاینتی عمل می‌کند که منابع سیستم اطلاعاتی (مانند فایل‌ها، اتصالات، صفحات وب یا خدمات) را از سایر سرورهای سازمان درخواست کرده است. درخواست‌های کلاینت که از طریق یک اتصال اولیه به سرور پراکسی برقرار شده‌اند، مورد ارزیابی قرار می‌گیرند تا بتوان پیچیدگی‌ها را مدیریت کرد و با محدود کردن امکان اتصال مستقیم، حفاظت بیشتری را فراهم آورد. دستگاه‌های فیلترینگ محتوای وب از جمله متداول‌ترین سرورهای پراکسی هستند که امکان دسترسی به اینترنت را فراهم می‌کنند. سرورهای پراکسی از گزارش‌گیری نشست‌های پروتکل کنترل انتقال (TCP) و مسدود کردن URLها، نام‌های دامنه و آدرس‌های IP خاص پشتیبانی می‌کنند. پراکسی‌های وب را می‌توان بر اساس لیست وب‌سایت‌های مجاز و غیر مجاز تعیین‌شده توسط سازمان، پیکربندی نمود. کنترل‌های مربوطه: AC-3, AU-2.

(۹) حفاظت مرزی / محدود کردن ترافیک ارتباطی خروجی خطرناک

سیستم اطلاعاتی:

(الف) ترافیک ارتباطی خروجی که می‌توانند تهدیدی بر علیه سیستم‌های اطلاعاتی خارجی باشند را شناسایی و انکار می‌کند؛ و

(ب) هویت کاربران داخلی مرتبط با ارتباطات انکارشده را ممیزی می‌کند.

راهنمایی‌های تکمیلی:شناسایی ترافیک ارتباطی خروجی از روی اقدامات داخلی که می‌توانند تهدیدی بر علیه سیستم‌های اطلاعاتی خارجی باشند، گاهی اوقات «شناسایی اکستروژن»[۲۴۲] نامیده می‌شود. شناسایی اکستروژن در مرزهای سیستم اطلاعاتی به عنوان بخشی از واسط‌های مدیریت‌شده، شامل تحلیل ترافیک ارتباطی ورودی و خروجی وجستجوی نشانه‌های تهدیدات داخلی بر علیه امنیت سیستم‌های خارجی است. این تهدیدات مواردی از جمله ترافیک نشان‌دهنده حملات DoS و ترافیک محتوی کدهای بدخواه را در بر می‌گیرند. کنترل‌های مربوطه: AU-2, AU-6, SC-38, SC-44, SI-3, SI-4.

[242] extrusion detection

(۱۰) حفاظت مرزی / جلوگیری از خروج غیر مجاز اطلاعات

سازمان از خروج غیر مجاز اطلاعات از واسط‌های مدیریت‌شده جلوگیری می‌کند.

راهنمایی‌های تکمیلی: ابزارهای امنیتی مورد استفاده سازمان برای جلوگیری از خروج غیر مجاز اطلاعات از سیستم‌های اطلاعاتی، مواردی از این دست را در بر می‌گیرند: (۱) پیروی کامل از فرمت پروتکل‌ها؛ (۲) پایش و جلوگیری از فریب خوردن سیستم‌های اطلاعاتی؛ (۳) پایش و جلوگیری از پنهان‌نگاری[۲۴۳]؛ (۴) قطع کردن واسط‌های شبکه خارجی به جز در مواردی که به آن‌ها نیاز مبرم باشد؛ (۵) جدا کردن و سر هم کردن مجدد سربرگ بسته‌ها؛ و (۶) تحلیل پروفایل ترافیک برای شناسایی موارد انحراف از حجم و نوع ترافیک مورد انتظار در سازمان یا تماس‌های برقرارشده با مراکز کنترل. برخی دستگاه‌ها از جمله فایروال‌های بازرسی ژرف بسته‌ها و گیت‌وی‌های XML، قوانین دقیقی در زمینه پیروی از فرمت پروتکل دارند. این دستگاه‌ها پیروی از فرمت پروتکل را در لایه برنامه کاربردی خود تأیید می‌کنند و آسیب‌پذیری‌هایی که توسط دستگاه‌های فعال در لایه شبکه یا لایه انتقال قابل ردیابی نیستند را شناسایی می‌نمایند. این کنترل پیشرفته ارتباط تنگاتنگی با روش‌های بین دامنه‌ای و محافظ‌های سیستمی دارد که الزامات جریان اطلاعات را پیاده‌سازی می‌نمایند. کنترل مربوطه: SI-3.

(۱۱) حفاظت مرزی / محدود کردن ترافیک ارتباطی ورودی

سیستم اطلاعاتی تنها اجازه ورود ارتباطات از [اختصاص: منابع مجاز تعیین‌شده توسط سازمان] به مقصد [اختصاص: مقاصد مجاز تعیین‌شده توسط سازمان] را می‌دهد.

راهنمایی‌های تکمیلی:این کنترل پیشرفته مبادی و مقصد ارتباطات مجاز را تعیین می‌نماید. تعیین این آدرس‌های مجاز بر اساس عوامل مختلفی صورت می‌گیرد که از آن جمله می‌توان به وجود جفت آدرس‌های مبدأ/مقصد در لیست ارتباطات مجاز، عدم وجود جفت آدرس‌های مبدأ/مقصد در لیست ارتباطات غیر مجاز، یا انطباق با قوانین کلی‌تر در زمینه جفت آدرس‌های مبدأ/مقصد مجاز اشاره کرد. کنترل مربوطه: AC-3.

(۱۲) حفاظت مرزی / حفاظت مبتنی بر میزبان

سازمان از [اختصاص: سازوکارهای حفاظت مرزی مبتنی بر میزبان تعیین‌شده توسط سازمان] در [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی:به عنوان مثالی از سازوکارهای حفاظت مرزی مبتنی بر میزبان می‌توان به فایروال‌های مبتنی بر میزان اشاره کرد. مؤلفه‌های سیستم اطلاعاتی که از حفاظت مرزی مبتنی بر

[243] steganography

میزبان استفاده می‌کنند نیز مواردی از جمله سرورها، ایستگاه‌های کاری و دستگاه‌های همراه را در بر می‌گیرند.

(۱۳) حفاظت مرزی / ایزوله کردن ابزارهای امنیتی، سازوکارها و مؤلفه‌های پشتیبان

سازمان [اختصاص: ابزارهای امنیتی، سازوکارها و مؤلفه‌های پشتیبان تعیین‌شده توسط سازمان] را با پیاده‌سازی زیرشبکه‌های مجزای فیزیکی با واسط‌های مدیریت‌شده، از سایر مؤلفه‌های سیستم اطلاعاتی ایزوله می‌کند.

راهنمایی‌های تکمیلی:با استفاده از زیرشبکه‌های مجزای فیزیکی با واسط‌های مدیریت‌شده، می‌توان سیستم‌های دفاعی شبکه‌های رایانه‌ای را از شبکه‌های پردازشگر حساس جدا کرد تا عوامل متخاصم نتوانند از روش‌های تحلیل و جرم‌شناسی سازمان آگاهی پیدا کنند. کنترل‌های مربوطه: SA-8, SC-2, SC-3.

(۱۴) حفاظت مرزی / جلوگیری از اتصالات فیزیکی غیر مجاز

سازمان از برقراری اتصالات غیر مجاز از طریق [اختصاص: واسط‌های مدیریت‌شده تعیین‌شده توسط سازمان] جلوگیری به عمل می‌آورد.

راهنمایی‌های تکمیلی: سیستم‌های اطلاعاتی که در دسته‌های امنیتی یا سطوح دسته‌بندی مختلف کار می‌کنند، ممکن است کنترل‌های محیطی یا فیزیکی مشترکی داشته باشند. دلیل این است که ممکن است سیستم‌های مذکور در فضای مشترکی در تأسیسات سازمان مستقر شده باشند. در واقع، ممکن است که این سیستم‌های مجزا از اتاق‌های تجهیزات، جعبه‌های سیم‌کشی و مسیرهای کابل‌کشی واحدی بهره گیرند. برای جلوگیری از اتصالات فیزیکی غیر مجاز می‌توان از جعبه‌های کابل، اتصالات و پانل‌هایی استفاده کرد که کاملاً مشخص و به صورت فیزیکی از هم تفکیک شده باشند. به منظور محدود کردن دسترسی مجاز به این مؤلفه‌ها نیز می‌توان از کنترل‌های دسترسی فیزیکی استفاده نمود. کنترل‌های مربوطه: PE-4, PE-19.

(۱۵) حفاظت مرزی / مسیریابی سطوح دسترسی ویژه به شبکه

سیستم اطلاعاتی تمام سطوح دسترسی ویژه به شبکه را از طریق یک واسط اختصاصی و مدیریت‌شده مسیریابی می‌کند تا بتواند دسترسی‌ها را کنترل و ممیزی نماید.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: AC-2, AC-3, AU-2, SI-4.

(۱۶) حفاظت مرزی / جلوگیری از شناسایی مؤلفه‌ها و دستگاه‌ها

سیستم اطلاعاتی از شناسایی مؤلفه‌های خاصی که یک واسط مدیریت‌شده را می‌سازند جلوگیری به عمل می‌آورد.

راهنمایی‌های تکمیلی:این کنترل پیشرفته از مانع از آن می‌شود که آن دسته از آدرس‌های شبکه مؤلفه‌های سیستم اطلاعاتی که بخشی از واسط‌های مدیریت‌شده هستند، با استفاده از شیوه‌ها و ابزارهای معمول شناسایی شوند. آدرس‌های شبکه قابل شناسایی نیستند (به عنوان مثال، آدرس‌های شبکه منتشر نمی‌شوند یا در سیستم‌های نام دامنه وارد نمی‌گردند) و برای دسترسی به آن‌ها نیاز به دانش قبلی است. یکی از شیوه‌هایی که می‌توان برای جلوگیری از شناسایی آدرس‌های شبکه به کار گرفت، تغییر این آدرس‌ها در بازه‌های زمانی مشخص است.

(۱۷) حفاظت مرزی / اجرای خودکار فرمت پروتکل

سیستم اطلاعاتی، خط‌مشی پایبندی به فرمت پروتکل را اجرا می‌نماید.

راهنمایی‌های تکمیلی: برخی مؤلفه‌های سیستم اطلاعاتی از جمله فایروال‌های بازرسی ژرف بسته‌ها و گیت‌وی‌های XML، قوانین دقیقی در زمینه پیروی از فرمت پروتکل دارند. این مؤلفه‌ها پیروی از فرمت پروتکل (مانند IEEE) را در لایه برنامه کاربردی خود تأیید می‌کنند و آسیب‌پذیری‌هایی که توسط دستگاه‌های فعال در لایه شبکه یا لایه انتقال قابل ردیابی نیستند را شناسایی می‌نمایند. کنترل مربوطه:SC-4.

(۱۸) حفاظت مرزی / از کار افتادن امن

در صورت از کار افتادن یک دستگاه حفاظت مرزی، سیستم اطلاعاتی به صورت امن از کار می‌افتد.

راهنمایی‌های تکمیلی:این ویژگی باعث می‌شود که در صورت از کار افتادن دستگاه‌های حفاظت مرزی در واسط‌های مدیریت‌شده (مانند مسیریاب‌ها، فایروال‌ها، محافظ‌ها و گیت‌وی‌های برنامه کاربردی که روی زیرشبکه‌های حفاظت‌شده موسوم به منطقه غیر نظامی مستقر هستند)، سیستم اطلاعاتی وارد حالت غیر امن نمی‌شود و ویژگی‌های امنیتی خود را از دست نمی‌دهد. از کار افتادن دستگاه‌های حفاظت مرزی باعث نمی‌شود که اطلاعات خارجی وارد دستگاه‌ها شوند یا اطلاعات به صورت غیر مجاز منتشر گردند. کنترل‌های مربوطه: CP-2, SC-24.

(۱۹) حفاظت مرزی / مسدود کردن ارتباطات نشأت‌گرفته از میزبان‌هایی که سازمان آن‌ها را پیکربندی نکرده است

سیستم اطلاعاتی، ترافیک ورودی و خروجی بین [اختصاص: کلاینت‌های ارتباطی تعیین‌شده توسط سازمان] که به صورت مستقل توسط کاربران نهایی و تأمین‌کنندگان خدمات خارجی پیکربندی شده‌اند را مسدود می‌کند.

راهنمایی‌های تکمیلی:کلاینت‌های ارتباطی که به صورت مستقل توسط کاربران نهایی و تأمین‌کنندگان خدمات خارجی پیکربندی شده‌اند، مواردی از جمله کلاینت‌های ارسال پیام‌های آنی را در بر می‌گیرند. مسدود کردن ترافیک شامل آن دسته از کلاینت‌هایی نمی‌شود که توسط سازمان پیکربندی شده‌اند تا کارکردهای مجاز را انجام دهند.

(۲۰) حفاظت مرزی / جداسازی و ایزوله کردن پویا

سیستم اطلاعاتی این قابلیت را فراهم می‌آورد که بتوان [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] را به صورت پویا از سایر مؤلفه‌های سیستم جدا/ایزوله کرد.

راهنمایی‌های تکمیلی: قابلیت جداسازی و ایزوله کردن پویای برخی مؤلفه‌های خاص سیستم اطلاعاتی سازمان زمانی سودمند است که بخواهیم مؤلفه‌هایی با منشأ مشکوک را از مؤلفه‌های قابل اعتماد تفکیک نماییم. جداسازی مؤلفه‌ها خطر حمله به سیستم‌های اطلاعاتی سازمان را کاهش می‌دهد. ایزوله کردن برخی مؤلفه‌های سیستم اطلاعاتی همچنین باعث می‌شود که در صورت رخ دادن حملات سایبری، دامنه خسارات محدود شود.

(۲۱) حفاظت مرزی / ایزوله کردن مؤلفه‌های سیستم اطلاعاتی

سازمان با استفاده از سازوکارهای حفاظت مرزی، [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] پشتیبان [اختصاص: مأموریت و/یا کارکردهای کسب‌وکار تعیین‌شده توسط سازمان] را از بقیه مؤلفه‌ها تفکیک می‌کند.

راهنمایی‌های تکمیلی: سازمان‌ها قادر به ایزوله کردنآن دسته از مؤلفه‌های سیستم اطلاعاتی هستند که مأموریت و/یا کارکردهای مختلف کسب‌وکار را انجام می‌دهند. این ایزوله‌سازی، جریان غیر مجاز اطلاعات بین مؤلفه‌های سیستم را محدود می‌کند و امکان حفاظت بیشتر از برخی مؤلفه‌های خاص را پدید می‌آورد. جدا کردن مؤلفه‌های سیستم اطلاعاتی با استفاده از سازوکارهای حفاظت مرزی امکان محافظت بیشتر از مؤلفه‌ها را فراهم می‌آورد و سازمان را قادر می‌سازد تا جریان اطلاعات بین مؤلفه‌های مختلف را به شکل بهتری کنترل کند. این نوع حفاظت پیشرفته، مخاطرات ناشی از خطاها و حملات سایبری را کاهش می‌دهد. میزان جداسازی مؤلفه‌ها می‌تواند متفاوت باشد که این امر به سازوکار مورد استفاده بستگی دارد. سازوکارهای حفاظت مرزی مواردی از این دست را در بر می‌گیرند: مسیریاب‌ها،

گیت‌وی‌ها و فایروال‌هایی که مؤلفه‌های سیستم را در قالب شبکه‌ها و زیرشبکه‌های فیزیکی مجزایی تفکیک می‌کنند، دستگاه‌های بین دامنه‌ای که زیرشبکه‌ها را از یکدیگر تفکیک می‌نمایند، روش‌های مجازی‌سازی، و جریان‌های اطلاعاتی که با استفاده از کلیدهای رمزگذاری بین مؤلفه‌های سیستم رمزگذاری شده‌اند. کنترل‌های مربوطه: CA-9, SC-3.

(۲۲) حفاظت مرزی / تفکیک زیرشبکه‌ها برای اتصال به دامنه‌های امنیتی مختلف

سیستم اطلاعاتی از آدرس‌های مختلف شبکه (یعنی زیرشبکه‌های مختلف) برای اتصال به سیستم‌ها در دامنه‌های امنیتی مختلف استفاده می‌کند.

راهنمایی‌های تکمیلی:تفکیک سیستم‌های اطلاعاتی به زیرشبکه‌ها سازمان را قادر می‌سازد تا سطح حفاظت مناسب را از اتصالات شبکه در دامنه‌های امنیتی مختلف فراهم آورد. این دامنه‌های امنیتی، دربردارنده اطلاعاتی با دسته‌بندی‌های امنیتی مختلف و سطوح محرمانگی متفاوت هستند.

(۲۳) حفاظت مرزی / غیر فعال کردن ارسال بازخورد برای فرستنده در صورت از کار افتادن تأیید پروتکل

سیستم اطلاعاتی قابلیت ارسال بازخورد به فرستنده را در صورت از کار افتادن قابلیت تأیید فرمت پروتکل، غیر فعال می‌کند.

راهنمایی‌های تکمیلی: غیر فعال کردن ارسال بازخورد برای فرستنده در صورت از کار افتادن قابلیت تأیید فرمت پروتکلباعث می‌شود که عوامل متخاصم نتوانند به اطلاعاتی که قرار نیست در دسترس آن‌ها قرار گیرد، دست یابند.

مراجع: نشریه FIPS 199؛ نشریه‌های ویژه شماره ۷۷-۸۰۰ و ۴۱-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-7 سطح تأثیرکم	SC-7(3)(4)(5)(7)سطح تأثیر متوسط	SC-7(3)(4)(5)(7)(8)(18)(21)سطح تأثیر زیاد

SC-8: محرمانگی و یکپارچگی انتقال

کنترل:سیستم اطلاعاتی از [انتخاب (یک یا دو مورد): محرمانگی؛ یکپارچگی] اطلاعات منتقل‌شده محافظت می‌کند.

راهنمایی‌های تکمیلی: این کنترل در مورد شبکه‌های داخلی و خارجی و همچنین برای همه انواع مختلف مؤلفه‌های سیستم‌های اطلاعاتی که اطلاعات می‌تواند از آن‌ها منتقل شود (مانند سرورها، دستگاه‌های همراه، لپ‌تاپ‌ها، چاپگرها، دستگاه‌های کپی، اسکنرها و دستگاه‌های فکس) اعمال می‌گردد. مسیرهای ارتباطی خارج از محدوده تحت حفاظت فیزیکی در معرض خطر سرقت و دستکاری اطلاعات قرار دارند. حفاظت از محرمانگی و/یا یکپارچگی اطلاعات سازمان را می‌توان با استفاده از ابزارهای فیزیکی (مثلاً با استفاده از سیستم‌های توزیع حفاظت‌شده) یا ابزارهای منطقی (مثلاً استفاده از روش‌های رمزگذاری) انجام داد. سازمان‌هایی که از خدمات انتقال اطلاعات ارائه‌شده توسط سازمان‌های دیگر استفاده می‌کنند و خدمات کاملاً سفارشی‌شده را به کار نمی‌گیرند، برای تأمین و پیاده‌سازی کنترل‌های امنیتی لازم برای تضمین محرمانگی و/یا یکپارچگی اطلاعات خود با دشواری‌های بیشتری روبرو خواهند بود. در این شرایط، سازمان‌ها بررسی می‌کنند که خدمات انتقال ارائه‌شده توسط سازمان‌های دیگر دارای چه ویژگی‌هایی برای تأمین محرمانگی و/یا یکپارچگی اطلاعات هستند. اگر نتوان کنترل‌های امنیتی و ضمانت‌های لازم را برای این خدمات یافت، سازمان‌ها استفاده از کنترل‌های امنیتی جبرانی را در دستور کار خود قرار خواهند داد یا مخاطرات را خواهند پذیرفت. کنترل‌های مربوطه: AC-17, PE-4.

کنترل‌های پیشرفته:

(۱) محرمانگی و یکپارچگی انتقال / رمزنگاری یا حفاظت فیزیکی

سیستم اطلاعاتی از سازوکارهای رمزنگاری برای [انتخاب (یک یا چند مورد): جلوگیری از افشای غیز مجاز اطلاعات؛ شناسایی تغییرات صورت‌گرفته در اطلاعات] در جریان انتقال اطلاعات استفاده می‌کند، مگر این که اطلاعات با استفاده از [اختصاص: ابزارهای حفاظت فیزیکی تعیین‌شده توسط سازمان] محافظت شده باشند.

راهنمایی‌های تکمیلی: رمزگذاری اطلاعات، از دستکاری یا افشای غیر مجاز اطلاعات جلوگیری می‌نماید. از جمله سازوکارهای رمزنگاری که برای حفاظت از یکپارچگی اطلاعات به کار می‌روند، می‌توان به توابع هش رمزنگاری، چک‌سام‌ها و کدهای احراز هویت پیام اشاره کرد. ابزارهای حفاظت فیزیکی نیز مواردی از جمله سیستم‌های توزیع حفاظت‌شده را در بر می‌گیرند. کنترل مربوطه: SC-13.

(۲) محرمانگی و یکپارچگی انتقال / فرانیدهای قبل و بعد از انتقال

سیستم اطلاعاتی در حین آماده‌سازی برای انتقال و همچنین در حین دریافت، [انتخاب (یک یا چند مورد): محرمانگی؛ یکپارچگی] اطلاعات را تأمین می‌نماید.

راهنمایی‌های تکمیلی: اطلاعات ممکن است در حین آماده‌سازی برای انتقال و همچنین در حین دریافت، به طور غیر ارادی یا به طور خرابکارانه افشا شوند. این موارد دستکاری و افشای غیر مجاز، محرمانگی و یکپارچگی اطلاعات را به خطر می‌اندازند. کنترل مربوطه: AU-10.

(۳) محرمانگی و یکپارچگی انتقال / حفاظت رمزنگاری برای اجزای پیام

سیستم اطلاعاتی از سازوکارهای رمزنگاری برای حفاظت از اجزای پیام استفاده می‌کند، مگر این که با استفاده از [اختصاص: ابزارهای حفاظت فیزیکی تعیین‌شده توسط سازمان] محافظت شده باشند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته به جلوگیری از افشای غیر مجاز اطلاعات می‌پردازد. منظور از اجزای پیام، مواردی از جمله اطلاعات مربوط به مسیر و سربرگ‌ها است. این کنترل پیشرفته از به خطر افتادن اجزای پیام جلوگیری می‌کند و در مورد شبکه‌های داخلی و خارجی یا لینک‌هایی که ممکن است توسط افراد غیر مجاز قابل مشاهده باشند، اعمال می‌گردد. اطلاعات مربوط به مسیر و سربرگ‌ها گاهی اوقات به صورت رمزگذاری‌نشده منتقل می‌شوند، زیرا چنین پنداشته می‌شود که این اطلاعات ارزش چندانی ندارند یا چنین تصور می‌شود که رمزگذاری این اطلاعات موجب پایین آمدن عملکرد شبکه یا بالا رفتن هزینه‌ها می‌گردد. ابزارهای حفاظت فیزیکی نیز مواردی از جمله سیستم‌های توزیع حفاظت‌شده را در بر می‌گیرند. کنترل‌های مربوطه: SC-12, SC-13.

(۴) محرمانگی و یکپارچگی انتقال / مخفی کردن یا تصادفی‌سازی ارتباطات

سیستم اطلاعاتی از سازوکارهای رمزنگاری برای مخفی کردن یا تصادفی‌سازی الگوهای ارتباطات استفاده می‌کند، مگر این که با استفاده از [اختصاص: ابزارهای حفاظت فیزیکی تعیین‌شده توسط سازمان] محافظت شده باشند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته به جلوگیری از افشای غیر مجاز اطلاعات می‌پردازد. منظور از الگوهای ارتباطات، مواردی از جمله فرکانس، دوره‌ها، مقدار یا قابلیت پیش‌بینی است. تغییر الگوهای ارتباطات می‌تواند منجر به افشای اطلاعات ارزشمند شود. این نکته به ویژه در مورد اطلاعاتی حائز اهمیت است که مربوط به مأموریت و کارکردهای کسب‌وکار سیستم‌های اطلاعاتی سازمان باشند. این کنترل پیشرفته از مانع از آن می‌شود که عوامل متخاصم بتوانند با استفاده از الگوهای ارتباطات، اقدام به استخراج اطلاعات ارزشمند نمایند. این کنترل پیشرفته در مورد شبکه‌های داخلی و خارجی یا لینک‌هایی که ممکن است توسط افراد غیر مجاز قابل مشاهده باشند، اعمال می‌گردد. با رمزگذاری لینک‌ها و انتقال اطلاعات در الگوهای مستمر، ثابت یا تصادفی، می‌توان مانع از استخراج اطلاعات از

الگوهای ارتباطات سیستم شد. ابزارهای حفاظت فیزیکی نیز مواردی از جمله سیستم‌های توزیع حفاظت‌شده را در بر می‌گیرند. کنترل‌های مربوطه: SC-12, SC-13.

مراجع: نشریه FIPS 140-2, 197؛ نشریه‌های ویژه شماره ۵۲-۸۰۰ و ۷۷-۸۰۰ و ۸۱-۸۰۰ و ۱۱۳-۸۰۰ سازمان NIST؛ خط‌مشی CNSS 15؛ NIST ISSI 7003.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب‌نشده، سطح تأثیرکم	SC-8(1)سطح تأثیر متوسط	SC-8(1) سطح تأثیر زیاد

SC-9: **محرمانگی انتقال**

[حذف شد: به بخش SC-8 انتقال داده شد].

SC-10: **قطع کردن اتصال شبکه**

کنترل: سیستم اطلاعاتی در پایان نشست یا پس از [اختصاص: مدت زمان غییر فعال بودن تعیین‌شده توسط سازمان]، اتصال شبکه را قطع می‌کند.

راهنمایی‌های تکمیلی: این کنترل هم در مورد شبکه‌های داخلی و هم در مورد شبکه‌های خارجی اعمال می‌شود. برای قطع کردن اتصال شبکه مربوط به نشست‌های ارتباطی، اقداماتی از قبیل اتمام تخصیص جفت پورت/آدرس TCP/IP در سطح سیستم‌عامل یا اتمام تخصیص وظایف شبکه در سطح برنامه کاربردی (اگر چند نشست برنامه کاربردی از یک اتصال شبکه واحد در سطح سیستم‌عامل استفاده می‌کنند) انجام می‌شود. مدت زمان غیر فعال بودن توسط سازمان مشخص می‌شود و می‌تواند به نوعغ دسترسی به شبکه یا موارد خاص دسترسی به شبکه بستگی داشته باشد.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب‌نشده، سطح تأثیرکم	SC-10سطح تأثیر متوسط	SC-10 سطح تأثیر زیاد

SC-11: **مسیر مورد اعتماد**

کنترل: سیستم اطلاعاتی یک مسیر ارتباطی مورد اعتماد را بین کاربر و این کارکردهای امنیتی سیستم برقرار می‌سازد: [اختصاص: کارکردهای امنیتی تعیین‌شده توسط سازمان، دست کم شامل احراز هویت سیستم اطلاعاتی و احراز هویت مجدد].

راهنمایی‌های تکمیلی: مسیرهای مورد اعتماد در واقع سازوکارهایی هستند که کاربران (از طریق دستگاه‌های ورودی) می‌توانند با استفاده از آن‌ها به طور مستقیم با کارکردهای امنیتی سیستم اطلاعاتی که دارای ابزارهای لازم برای پشتیبانی از خط‌مشی‌های امنیت اطلاعات هستند، ارتباط برقرار نمایند. این سازوکارها تنها توسط کاربران یا کارکردهای امنیتی سیستم‌های اطلاعاتی سازمان قابل دسترسی خواهند بود. پاسخ‌هایی که کاربران از طریق این مسیرهای مورد اعتماد می‌دهند، در برابر دستکاری یا افشا توسط برنامه‌های کاربردی غیر قابل اعتماد محافظت می‌شوند. سازمان‌ها از مسیرهای مورد اعتماد برای برقراری اتصالات امن بین کارکردهای امنیتی سیستم‌های اطلاعاتی و کاربران (مثلاً در جریان ورود به سیستم) استفاده می‌کنند. در هنگام استفاده از مسیرهای ارتباطی مورد اعتماد، به قوانین پایش توجه می‌شود. کنترل‌های مربوطه: AC-16, AC-25.

کنترل‌های پیشرفته:

(۱) مسیر مورد اعتماد / ایزوله کردن منطقی

سیستم اطلاعاتی یک مسیر ارتباطی مورد اعتماد را فراهم می‌آورد که به طور منطقی از سایر مسیرها ایزوله شده و قابل تشخیص است.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده،سطح تأثیرکم	انتخاب نشده،سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-12: **تبادل و مدیریت کلید رمزنگاری**

کنترل: سازمان کلیدهای رمزنگاری را برای دستیابی به قابلیت‌های رمزنگاری لازم در سیستم اطلاعاتی و بر اساس [اختصاص: الزامات تعیین‌شده توسط سازمان در زمینه تولید، توزیع، ذخیره‌سازی، دسترسی و توزیع کلید] مبادله و مدیریت می‌کند.

راهنمایی‌های تکمیلی: تبادل و مدیریت کلید رمزنگاری می‌تواند از طریق رویه‌های رمزی یا سازوکارهای خودکاری انجام شود که مجموعه‌ای از رویه‌های دستی نیز برای پشتیبانی از آن‌ها وجود دارد. سازمان‌ها الزامات مدیریت کلید را بر اساس قوانین، دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها و راهنمایی‌های فدرال تعیین می‌کنند. آن‌ها حافظه‌های اعتماد[۲۴۴] را به گونه‌ای مدیریت می‌کنند که اطمینان حاصل نمایند تنها زنجیره‌های اعتماد تأییدشده در این حافظه‌ها وجود دارند. این امر شامل گواهی‌های قابل مشاهده توسط سیستم‌های اطلاعاتی خارج از سازمان و گواهی‌های مربوط به عملیات داخلی سیستم نیز می‌شود. کنترل‌های مربوطه: SC-13, SC-17.

کنترل‌های پیشرفته:

(۱) تبادل و مدیریت کلید رمزنگاری / آماده کار بودن

در صورتی که کاربران کلیدهای رمزنگاری را از دست بدهند، سازمان اطلاعات را آماده کار نگه می‌دارد.

راهنمایی‌های تکمیلی: یکی از راه‌های تأمین آماده کار بودن در صورت از دست رفتن کلیده (مثلاً به دلیل فراموش کردن گذرواژه‌ها)، سپردن کلیدهای رمزنگاری به مراجع مورد اعتماد است.

(۲) تبادل و مدیریت کلید رمزنگاری / کلیدهای متقارن

سازمان کلیدهای رمزنگاری متقارن را با استفاده از فرایندها و فناوری‌های مدیریت کلید [انتخاب: منطبق با NIST FIPS؛ مورد تأییدNSA] تولید، کنترل و توزیع می‌کند.

(۳) تبادل و مدیریت کلید رمزنگاری / کلیدهای نامتقارن

سازمان کلیدهای رمزنگاری متقارن را با استفاده از [انتخاب: فرایندها و فناوری‌های مدیریت کلید مورد تأیید NSA؛ اطلاعات کلید ازپیش‌تعیین‌شده یا گواهی‌های PKI Class 3 تأییدشده؛ گواهی‌های PKI Class 3یا Class 4 تأییدشده و توکن‌های امنیت سخت‌افزار که از کلید خصوصی کاربر حفاظت می‌کنند] تولید، کنترل و توزیع می‌کند.

(۴) تبادل و مدیریت کلید رمزنگاری / گواهی‌های PKI

[حذف شد: به بخش SC-12 منتقل شد].

[244] trust store

(۵) تبادل و مدیریت کلید رمزنگاری / توکن‌های سخت‌افزار|گواهی‌های PKI
[حذف شد: به بخش SC-12 منتقل شد].

مراجع: نشریه‌های ویژه شماره ۵۶-۸۰۰ و ۵۷-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-12سطح تأثیرکم	SC-12سطح تأثیر متوسط	SC-12(1) سطح تأثیر زیاد

SC-13: **حفاظت رمزنگاری**

کنترل: سیستم اطلاعاتی [اختصاص: کاربردهای رمزنگاری تعیین‌شده توسط سازمان و انواع روش‌های رمزنگاری مورد نیاز برای هر یک از این کاربردها] را بر اساس قوانین، دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها و راهنمایی‌های فدرال پیاده‌سازی می‌کند.

راهنمایی‌های تکمیلی: رمزنگاری را می‌توان برای پشتیبانی از بسیاری از روش‌های امنیتی به کار گرفت که از آن جمله می‌توان به حفاظت از اطلاعات محرمانه و اطلاعات غیر محرمانه کنترل‌شده، تأمین امضاهای دیجیتال، و تفکیک اطلاعات در شرایطی که افراد مجاز دارای تأییدیه دسترسی به اطلاعات باشند اما تأییدیه دسترسی رسمی به اطلاعات نداشته باشند، اشاره نمود. روش‌های رمزنگاری همچنین می‌توانند برای پشتیبانی از تولید اعداد تصادفی و تولید هش به کار گرفته شوند. استانداردهای رمزنگاری به طور کلی عبارتند از رمزنگاری تأییدشده توسط FIPS و رمزنگاری مورد تأیید NSA. این کنترل سازمان‌ها را موظف به استفاده از رمزنگاری نمی‌کند. با این حال، اگر اگر بر اساس انتخاب‌هایی که در سایر کنترل‌های امنیتی انجام شده است نیاز به استفاده از رمزنگاری باشد، سازمان‌ها باید نوع رمزنگاری مورد نیاز را تعیین نمایند. به عنوان مثال برای حفاظت از اطلاعات محرمانه باید از رمزنگاری مورد تأیید NSA و برای تأمین امضای دیجیتال باید از رمزنگاری تأییدشده توسط FIPS استفاده نمود. کنترل‌های مربوطه: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

کنترل‌های پیشرفته: وجود ندارد.

(۱) حفاظت رمزنگاری / رمزنگاری تأییدشده توسط FIPS
[حذف شد: به بخش SC-13 منتقل شد].

(۲) حفاظت رمزنگاری / رمزنگاری مورد تأیید NSA

[حذف شد: به بخش SC-13 منتقل شد].

(۳) حفاظت رمزنگاری / افرادی که تأییدیه رسمی دسترسی به اطلاعات ندارند

[حذف شد: به بخش SC-13 منتقل شد].

(۴) حفاظت رمزنگاری / امضای دیجیتال

[حذف شد: به بخش SC-13 منتقل شد].

مراجع: نشریه FIPS 140؛ آدرس‌های اینترنتی: http://www.cnss.gov ,http://csrc.nist.gov/cryptval

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-13 سطح تأثیرکم	SC-13 سطح تأثیر متوسط	SC-13 سطح تأثیر زیاد

SC-14: **حفاظت از دسترسی عمومی**

[حذف شد: این قابلیت توسط AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10 ارائه شده است].

SC-15: **دستگاه‌های محاسباتی مشارکتی**

کنترل: سیستم اطلاعاتی:

الف. فعال کردن دستگاه‌های محاسباتی مشارکتی از راه دور را به جز در موارد روبرو ممنوع می‌کند: [اختصاص: استثنائات تعیین‌شده توسط سازمان در خصوص موارد مجاز فعال کردن دستگاه‌های محاسباتی مشارکتی از راه دور]؛ و

ب. نشانه‌های آشکار استفاده را به کاربرانی که به طور فیزیکی کنار دستگاه حضور دارند ارائه می‌نماید.

راهنمایی‌های تکمیلی: دستگاه‌های محاسباتی مشارکتی مواردی از جمله میکروفون‌ها، دوربین‌ها و وایت‌بوردهای شبکه‌شده را در بر می‌گیرند. به عنوان مثالی از نشانه‌های آشکار استفاده نیز می‌توان به سیگنال‌هایی اشاره کرد که برای کاربران ارسال می‌شوند و نشان می‌دهند که دستگاه‌های محاسباتی مشارکتی فعال شده‌اند.

کنترل‌های پیشرفته:

(۱) دستگاه‌های محاسباتی مشارکتی / قطع اتصال فیزیکی

سیستم اطلاعاتی قابلیت قطع آسان اتصال فیزیکی دستگاه‌های محاسباتی مشارکتی را فراهم می‌آورد.

راهنمایی‌های تکمیلی: شکست در قطع اتصال فیزیکی دستگاه‌هایمحاسباتی مشارکتی می‌تواند باعث به خطر افتادن اطلاعات سازمان شود. فراهم آوردن امکان قطع آسان اتصال فیزیکی دستگاه‌های محاسباتی مشارکتی پس از پایان یافتن یک نشست محاسباتی مشارکتی به سازمان کمک می‌کند تا اطمینان حاصل نماید کاربران و دست‌اندرکاران می‌توانند این قطع اتصال را به سادگی و بدون نیاز به استفاده از فرایندهای پیچیده انجام دهند.

(۲) دستگاه‌های محاسباتی مشارکتی / مسدود کردن ترافیک ارتباطی ورودی یا خروجی

[حذف شد: به بخش SC-7 منتقل شد].

(۳) دستگاه‌های محاسباتی مشارکتی / غیر فعال کردن و جدا کردن کردن در نواحی کاری امن

سازمان دستگاه‌های محاسباتی مشارکتی را در [اختصاص: نواحی کاری امن تعیین‌شده توسط سازمان] از [اختصاص: سیستم‌های اطلاعاتی یا مؤلفه‌های تعیین‌شده توسط سازمان] جدا می‌کند یا غیر فعال می‌نماید.

راهنمایی‌های تکمیلی: شکست در غیر فعال کردن یا جدا کردن دستگاه‌هایمحاسباتی مشارکتی می‌تواند باعث به خطر افتادن اطلاعات سازمان شود. به عنوان مثالی از این خطرات، می‌توان به شنود مکالمات اشاره کرد.

(۴) دستگاه‌های محاسباتی مشارکتی / تعیین آشکار شرکت‌کنندگان فعلی

سیستم اطلاعاتی به طور آشکار بیان می‌کند که کدام کاربران در حال حاضر در [اختصاص: کنفرانس‌های راه دور یا نشست‌های آنلاین تعیین‌شده توسط سازمان] حضور دارند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته باعث می‌شود که افراد غیر مجاز نتوانند بدون اطلاع سایر شرکت‌کنندگان، در نشست‌های محاسباتی مشارکتی حضور یابند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-15 سطح تأثیرکم	SC-15 سطح تأثیر متوسط	SC-15 سطح تأثیر زیاد

SC-16: **انتقال ویژگی‌های امنیتی**

کنترل: سیستم اطلاعاتی [اختصاص: ویژگی‌های امنیتی تعیین‌شده توسط سازمان] را با اطلاعات مبادله‌شده بین سیستم‌های اطلاعاتی و بین مؤلفه‌های این سیستم‌ها پیوند می‌دهد.

راهنمایی‌های تکمیلی: ویژگی‌های امنیتی را می‌توان به طور آشکار یا ضمنی با اطلاعات موجود در سیستم‌های اطلاعاتی یا مؤلفه‌های این سیستم‌ها پیوند داد. کنترل‌های مربوطه: AC-3, AC-4, AC-16.

کنترل‌های پیشرفته:

(۱) انتقال ویژگی‌های امنیتی / تأیید یکپارچگی

سیستم اطلاعاتی یکپارچگی ویژگی‌های امنیتی منتقل‌شده را تأیید می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته باعث حصول اطمینان از تأیید یکپارچگی ویژگی‌های امنیتی منتقل‌شده می‌شود. کنترل‌های مربوطه: AU-10, SC-8.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخاب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-17: **گواهی‌های زیرساخت کلید عمومی**

کنترل: سازمان گواهی‌های کلید عمومی را بر اساس [اختصاص: خط‌مشی‌های تعیین‌شده توسط سازمان در زمینه گواهی‌ها] صادر می‌کند یا این گواهی‌ها را از یک تأمین‌کننده خدمات مورد تأیید دریافت می‌کند.

راهنمایی‌های تکمیلی: در مورد تمام گواهی‌ها، سازمان حافظه‌های اعتماد سیستم اطلاعاتی را به گونه‌ای مدیریت می‌کند که اطمینان حاصل نماید تنها مراجع اعتماد تأییدشده در این حافظه‌ها وجود داشته باشند. این کنترل هم در مورد گواهی‌های قابل مشاهده از خارج سیستم‌های اطلاعاتی سازمان و هم در مورد گواهی‌های مربوط به عملیات درونی سیستم‌ها اعمال می‌شود. کنترل مربوطه: SC-12.

کنترل‌های پیشرفته: وجود ندارد.

مراجع:تفهیم‌نامه OMB 05-24؛ نشریه‌های ویژه شماره ۳۲-۸۰۰ و ۶۳-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، سطح تأثیرکم	SC-17 سطح تأثیر متوسط	SC-17 سطح تأثیر زیاد

SC-18: **کد موبایل**

کنترل: سازمان:

الف. کدهای موبایل و فناوری‌های کد موبایل قابل قبول و غیر قابل قبول را تعریف می‌کند؛

ب. محدودیت‌هایی را برای کاربرد و راهنمایی‌هایی را برای پیاده‌سازی کدهای موبایل و فناوری‌های کد موبایل قابل قبول تعیین می‌نماید؛ و

پ. اجازه استفاده از کدهای موبایل را درون سیستم اطلاعاتی صادر می‌کند و موارد استفاده را پایش و کنترل می‌نماید.

راهنمایی‌های تکمیلی:تصمیم‌گیری در خصوص استفاده از کدهای موبایل درون سیستم اطلاعاتی به این بستگی دارد که در صورت استفاده مخرب از کد مذکور، چه خطراتی متوجه سیستم خواهد بود. فناوری‌های کد موبایا مواردی از این دست را شامل می‌شوند: جاوا، جاوااسکریپت، ActiveX، Postscript، PDF، فیلم‌های Shockwave، انیمیشن‌های Flash و VBScript. محدودیت‌های کاربرد و راهنمایی‌های پیاده‌سازی هم در مورد کدهای موبایل نصب‌شده روی سرورها و هم در مورد کدهای موبایل دانلودشده و اجراشده روی دستگاه‌ها و ایستگاه‌های کاری اعمال می‌شوند. رویه‌های و خط‌مشی‌های کدهای موبایل به گونه‌ای تنظیم می‌شوند که از توسعه، اکتساب و استفاده از کدهای موبایل غیر قابل قبول در سیستم‌های اطلاعاتی سازمان جلوگیری به عمل آید. کنترل‌های مربوطه: AU-2, AU-12, CM-2, CM-6, SI-3.

کنترل‌های پیشرفته:

(۱) کد موبایل / شناسایی کدهای غیر قابل قبول و انجام اقدامات اصلاحی

سیستم اطلاعاتی [اختصاص: کدهای موبایل غیر قابل قبول تعیین‌شده توسط سازمان] را شناسایی می‌کند و [اختصاص: اقدامات اصلاحی تعیین‌شده توسط سازمان] را انجام می‌دهد.

راهنمایی‌های تکمیلی: اقدامات اصلاحی در صورت غیر قابل قبول بودن کدهای موبایل، مواردی از جمله مسدود کردن، قرنطینه کردن یا اطلاع دادن به راهبران را در بر می‌گیرند. مسدود کردن مثلاً هنگامی به کار گرفته می‌شود که فایل‌های نرم‌افزارهای پردازشگر کلمه دارای ماکروهای تعبیه‌شده‌ای باشند که به عنوان کدهای موبایل غیر قابل قبول شناسایی شده‌اند. در این صورت، از انتقال این فایل‌ها جلوگیری به عمل می‌آید.

(۲) کد موبایل / اکتساب، توسعه و استفاده

سازمان اطمینان حاصل می‌نماید که توسعه، اکتساب و استفاده از کدهای موبایل در سیستم اطلاعاتی، با رعایت [اختصاص: الزامات تعیین‌شده توسط سازمان در خصوص کدهای موبایل] صورت می‌گیرد.

(۳) کد موبایل / جلوگیری از دانلود و اجرا

سیستم اطلاعاتی از دانلود و اجرا کردن [اختصاص: کدهای موبایل غیر قابل قبول تعیین‌شده توسط سازمان] جلوگیری می‌کند.

(۴) کد موبایل / جلوگیری از اجرای خودکار

سیستم اطلاعاتی از اجرای خودکار کدهای موبایل در [اختصاص: برنامه‌های نرم‌افزاری تعیین‌شده توسط سازمان] جلوگیری می‌کند و پیش از اجرای این کدها، [اختصاص: اقداماتتعیین‌شده توسط سازمان] را انجام می‌دهد.

راهنمایی‌های تکمیلی:به عنوان مثال، پیش از اجرای کدها از کاربران خواسته می‌شود که اطلاعاتی را وارد کنند و سپس پیوست‌های ایمیل خود را باز نمایند. برای جلوگیری از اجرای خودکار کدهای موبایل نیز به عنوان مثال چنین اقدامی صورت می‌گیرد: غیر فعال کردن ویژگی‌های اجرای خودکار روی آن دسته از مؤلفه‌های سیستم‌های اطلاعاتی که از دستگاه‌های ذخیره‌سازی قابل حمل از جمله CD، DVD و دستگاه‌های USB استفاده می‌کنند.

(۵) کد موبایل / صدور مجوز اجرا تنها در محیط محدود و کنترل‌شده

سازمان مجوز اجرای کدهای موبایل را تنها در محیط‌های محدود و کنترل‌شده ماشین مجازی صادر می‌نماید.

مراجع: نشریه ویژه شماره ۸۰۰-۲۸ سازمان NIST؛ دستورالعمل DoD 8552.01.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب نشده، سطح تأثیرکم	SC-18 سطح تأثیر متوسط	SC-18 سطح تأثیر زیاد

SC-19: **پروتکل** VoIP

کنترل: سازمان:

الف. بر اساس خسارات بالقوه به سیستم اطلاعاتی در صورت استفاده خرابکارانه، محدودیت‌هایی را برای کاربرد و راهنمایی‌هایی را برای پیاده‌سازی فناوری‌های VoIP تعیین می‌نماید؛ و

ب. اجازه استفاده از پروتکل VoIP را درون سیستم اطلاعاتی صادر می‌کند و موارد استفاده را پایش و کنترل می‌نماید.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: CM-6, SC-7, SC-15.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: نشریه ویژه شماره ۸۰۰-۵۸ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، سطح تأثیرکم	SC-19 سطح تأثیر متوسط	SC-19 سطح تأثیر زیاد

SC-20: **سرویس تعیین آدرس / نام امن (منبع راهبری)**

کنترل: سیستم اطلاعاتی:

الف. اطلاعاتی را درباره ابزارهای تأیید یکپارچگی، احراز هویت مبدأ و تعیین نام راهبری در پاسخ به کوئری‌های خارجی تعیین آدرس/نام ارائه می‌کند؛ و

ب. ابزاری را برای تعیین وضعیت امنیتی منطقه child ارائه می‌کند و در صورتی که این منطقه از خدمات تعیین امن پشتیبانی کند، امکان تأیید یک زنجیره اعتماد را بین منطقه‌های child و parent فراهم می‌آورد.

راهنمایی‌های تکمیلی: این کنترل به کلاینت‌های خارجی از جمله کلاینت‌های اینترنتی راه دور امکان می‌دهد تا مبدأ را احراز هویت و یکپارچگی را تأیید کنند. به عنوان مثالی از سیستم‌های اطلاعاتی ارائه‌دهنده خدمات تعیین آدرس و نام، می‌توان به خدمات DNS اشاره کرد. برخی ابزارهای مورد استفاده عبارتند از کلیدهای رمزنگاری و امضاهای دیجیتال امنیت DNS. سوابق منبع DNS از جمله داده‌های راهبری به شمار می‌آیند. ابزارهایی که برای تعیین وضعیت امنیتی منطقه‌های child به کار می‌روند نیز مواردی از جمله سوابق منبع امضاکننده در DNS را شامل می‌شوند. کنترل‌های امنیتی DNS مبتنی بر تفهیم‌نامه OMB 08-23 هستند. سیستم‌های اطلاعاتی که از فناوری‌هایی به جز DNS برای نگاشت بین نام‌های سرویس/میزبان و آدرس‌های شبکه استفاده می‌کنند،ابزارهای دیگری را برای تأیید یکپارچگی و احراز هویت داده‌ها به کار می‌گیرند. کنترل‌های مربوطه: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

کنترل‌های پیشرفته:

(۱) سرویس تعیین آدرس / نام امن (منبع راهبری) / سرویس تعیین آدرس (منبع راهبری) | زیرفضاهای child

[حذف شد: به بخش SC-20 منتقل شد].

(۲) سرویس تعیین آدرس / نام امن (منبع راهبری) / سرویس تعیین آدرس (منبع راهبری) | یکپارچگی و مبدأ داده‌ها

سیستم اطلاعاتی ابزارهایی را ارائه می‌کند تا در صورت کوئری داخلی برای تعیین آدرس/نام، بتوان یکپارچگی و مبدأ داده‌ها را تأیید کرد.

مراجع: بر تفهیم‌نامه OMB 08-23؛ نشریه ویژه شماره ۸۰۰-۸۱ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-20، سطح تأثیرکم	SC-20 سطح تأثیر متوسط	SC-20 سطح تأثیر زیاد

SC-21: **سرویس تعیین آدرس / نام امن** (RECURSIVE OR CACHING RESOLVER)

کنترل: سیستم اطلاعاتی فرایندهای تأیید یکپارچگی داده‌ها و احراز هویت مبدأ داده‌ها را روی پاسخ‌های تعیین آدرس/نام دریافت‌شده از منابع راهبری، درخواست و اجرا می‌نماید.

راهنمایی‌های تکمیلی: هر یک از کلاینت‌های تعیین خدمات نام یا این اقدامات تأییدی را خود انجام می‌دهند و یا از کانال‌های احرازهویت‌شده‌ای برای اتصال به تأمین‌کنندگان این خدمات استفاده می‌کنند. برخی سیستم‌های اطلاعاتی که از خدمات تعیین آدرس و نام برای کلاینت‌های محلی استفاده می‌کنند عبارتند از سرورهای DNS از نوع caching یا recursive. Resolverهای کلاینت DNS یا امضاهای DNSSEC را خود تأیید می‌کنند و یا برای این کار از recursive resolverها استفاده می‌نمایند. سیستم‌های اطلاعاتی که از فناوری‌هایی به جز DNS برای نگاشت بین نام‌های سرویس/میزبان و آدرس‌های شبکه استفاده می‌کنند، ابزارهای دیگری را برای تأیید یکپارچگی و احراز هویت داده‌ها توسط کلاینت‌ها به کار می‌گیرند. کنترل‌های مربوطه: SC-20, SC-22.

کنترل‌های پیشرفته: وجود ندارد.

(۱) سرویس تعیین آدرس (RECURSIVE OR CACHING RESOLVER) / یکپارچگی و مبدأ داده‌ها
[حذف شد: به بخش SC-21 منتقل شد].

مراجع: نشریه ویژه شماره ۸۱-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-21، سطح تأثیرکم	SC-21 سطح تأثیر متوسط	SC-21 سطح تأثیر زیاد

SC-22: معماری و تأمین خدمات تعیین نام/آدرس

کنترل:سیستم‌های اطلاعاتی که خدمات تعیین نام/آدرس را برای یک سازمان انجام می‌دهند، در مقابل خطا مقاوم هستند و تفکیک وظایف داخلی/خارجی را انجام می‌دهند.

راهنمایی‌های تکمیلی: سیستم‌های اطلاعاتی که خدمات تعیین نام/آدرس را برای یک سازمان انجام می‌دهند، مواردی از جمله سرورهای DNS را شامل می‌شوند. برای این که بروز یک خطا باعث از کار افتادن کل سیستم نشود و همچنین برای این که قابلیت جایگزینی ارتقا یابد، یک سرور به عنوان سرور اولیه و سرور دیگری به عنوان سرور ثانویه پیکربندی می‌شوند. علاوه بر این، سازمان‌ها معمولاً سرورها را در دو زیرشبکه قرار می‌دهند که مکان جغرافیایی متفاوتی دارند (یعنی سرورها در یک تأسیسات فیزیکی واحد مستقر نمی‌شوند). به منظور تفکیک وظایف، سرورهای DNS با نقش داخلی تنها به آن دسته از درخواست‌های تعیین آدرس و نام می‌پرازند که از درون سازمان مطرح شده‌اند (یعنی از جانب کلاینت‌های داخلی مطرح گشته‌اند). سرورهای DNS با نقش

خارجی نیز تنها به آن دسته از درخواست‌های تعیین آدرس و نام می‌پرازند که توسط کلاینت‌های خارج از سازمان (یعنی روی شبکه‌های خارجی مانند اینترنت) مطرح شده‌اند. سازمان‌ها تعیین می‌کنند که کدام کلاینت‌ها می‌توانند به سرورهای راهبری DNS در نقش‌های خاص دسترسی داشته باشند. برای تعیین این کلاینت‌ها، سازمان‌ها از محدوده‌های آدرس، لیست‌های آشکار یا روش‌های دیگری از این دست استفاده می‌کنند. کنترل‌های مربوطه: SC-2, SC-20, SC-21, SC-24.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: نشریه ویژه شماره ۸۰۰-۸۱ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-22، سطح تأثیرکم	SC-22 سطح تأثیر متوسط	SC-22 سطح تأثیر زیاد

SC-23: **اعتبار نشست**[۲۴۵]

کنترل: سیستم اطلاعاتی از اعتبار نشست‌های ارتباطی محافظت می‌کند.

راهنمایی‌های تکمیلی: این کنترل به حفاظت از ارتباطات در نشست می‌پردازد که در مقابل حفاظت از ارتباطات در سطح بسته[۲۴۶] (مثلاً نشست‌های معماری‌های سرویس‌گرا که خدمات مبتنی بر وب را ارائه می‌نمایند) قرار می‌گیرد. این کنترل دو طرف ارتباط را قادر می‌سازد تا هویت یکدیگر و اعتبار ارتباطات منتقل‌شده را تأیید نمایند. حفاظت از اعتبار نشست مواردی از این دست را در بر می‌گیرد: جلوگیری از حملات کسی در میانه، جلوگیری از سرقت نشست و جلوگیری از تزریق اطلاعات به نشست. کنترل‌های مربوطه: SC-8, SC-10, SC-11.

کنترل‌های پیشرفته:

(۱) اعتبار نشست / از اعتبار ساقط کردن شناسه‌های نشست پس از خروج کاربر از نشست

سیستم اطلاعاتی پس از خروج کاربر از نشست یا به اتمام رسیدن نشست، شناسه‌های کاربر را از اعتبار ساقط می‌کند.

[245] session authenticity
[246] packet level

راهنمایی‌های تکمیلی: این کنترل پیشرفته مانع از آن می‌شود که عوامل متخاصم پس از پایان نشست از شناسه‌های کاربر استفاده کنند.

(۲) اعتبار نشست / خروج کاربر از نشست و نمایش پیام

[حذف شد: به بخش AC-12(1) منتقل شد].

(۳) اعتبار نشست / شناسه‌های منحصربه‌فرد نشست با تصادفی‌سازی

سیستم اطلاعاتی با رعایت [اختصاص: الزامات تعیین‌شده توسط سازمان در خصوص تصادفی بودن]، یک شناسه منحصربه‌فرد را تولید می‌کند و تنها شناسه‌های تولیدشده توسط سیستم را به رسمیت می‌شناسد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته مانع از آن می‌شود که عوامل متخاصم پس از پایان نشست از شناسه‌هایی که پیشتر معتبر بوده‌اند استفاده کنند. پیاده‌سازی مفهوم تصادفی بودن در تولید شناسه‌های منحصربه‌فرد نشست باعث می‌شود که سازمان بتواند با حملات جستجوی فراگیر انجام‌شده برای شناسایی شناسه‌های بعدی نشست مقابله کند. کنترل مربوطه: SC-13.

(۴) اعتبار نشست / شناسه‌های منحصربه‌فرد نشست با تصادفی‌سازی

[حذف شد: به بخش SC-23(3) منتقل شد].

(۵) اعتبار نشست / مقامات مجاز صدور گواهی

سیستم اطلاعاتی تنها به [اختصاص: مقامات صدور گواهی تعیین‌شده توسط سازمان] اجازه می‌دهد که برقراری نشست‌های حفاظت‌شده را تأیید کنند.

راهنمایی‌های تکمیلی: به عنوان مثال، از گواهی‌های SSL و TLS استفاده می‌شود. این گواهی‌ها، پس از تأیید از جانب مقام صادرکننده، برقراری نشست‌های حفاظت‌شده بین کلاینت‌های وب و سرورهای وب را تسهیل می‌کنند. کنترل مربوطه: SC-13.

مراجع: نشریه‌های ویژه شماره ۵۲-۸۰۰ و ۷۷-۸۰۰ و ۹۵-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، سطح تأثیرکم	SC-23 سطح تأثیر متوسط	SC-23 سطح تأثیر زیاد

SC-24: **رفتن به حالت معلوم[۲۴۷] در صورت از کار افتادن**

کنترل: سیستم اطلاعاتی در هنگام [اختصاص: انواع از کار افتادن تعیین‌شده توسط سازمان] به [اختصاص: حالت معلوم تعیین‌شده توسط سازمان] وارد می‌شود تا از [اختصاص: اطلاعات وضعیت سیستم تعیین‌شده توسط سازمان] محافظت به عمل آید.

راهنمایی‌های تکمیلی: رفتن به حالت معلوم در صورت از کار افتادن باعث از بین رفتن دغدغه‌های امنیتی می‌شود که سازمان در زمینه نیازهای مأموریت و کسب‌وکار خود دارد. بدین ترتیب، در صورتی که سیستم اطلاعاتی سازمان یا مؤلفه‌های این سیستم از کار بیفتند، محرمانگی، یکپارچگی و آماده کار بودن اطلاعات به خطر نمی‌افتد. رفتن به حالت معلوم در صورت از کار افتادن باعث می‌شود که سیستم وارد حالتی نشود که خساراتی را برای افراد و سرمایه‌های سازمان در پی داشته باشد. بدین ترتیب، راه‌اندازی مجدد سیستم و بازگشت به حالت عملیاتی عادی نیز ساده‌تر خواهد بود. کنترل‌های مربوطه: CP-2, CP-10, CP-12, SC-7, SC-22.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	SC-24 سطح تأثیر زیاد

SC-25: **گره‌های لاغر[۲۴۸]**

کنترل: سازمان [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] را با حداقل کارکرد و ذخیره اطلاعاتی به کار می‌گیرد.

راهنمایی‌های تکمیلی: به کار گرفتن مؤلفه‌های سیستم اطلاعاتی با حداقل کارکرد یا کارکرد محدود (مانند گره‌های بدون دیسک و فناوری‌های کلاینت لاغر)، نیاز به تأمین امنیت تمام نقاط انتهایی را کاهش می‌دهد و از

[247] known state
[248] thin nodes

قرار گرفتن اطلاعات، سیستم‌های اطلاعاتی و خدمات در معرض حملات سایبری نیز می‌کاهد. کنترل مربوطه: SC-30.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-26: **هانی‌پات‌ها**

کنترل:سیستم اطلاعاتی مؤلفه‌هایی را که به طور خاص به این منظور طراحی شده‌اند، به عنوان هدف حملات بدخواهانه قرار می‌دهد تا بتواند این حملات را شناسایی، منحرف و تحلیل کند.

راهنمایی‌های تکمیلی:هانی‌پات در واقع تله‌ای است که برای مهاجمان در نظر گرفته می‌شود تا حملات آن‌ها را از سیستم‌عامل‌های پشتیبان مأموریت‌ها و فرایندهای کسب‌وکار سازمان منحرف کند. بسته به این که از چه نوع هانی‌پاتی استفاده می‌شود، ممکن است نیاز به مشورت با دفتر مشاور کل وجود داشته باشد. کنترل‌های مربوطه: SC-30, SC-44, SI-3, SI-4.

کنترل‌های پیشرفته: وجود ندارد.

(۱) هانی‌پات‌ها / شناسایی کدهای مخرب
[حذف شد: به بخش SC-35 منتقل شد].

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-27: **برنامه‌های کاربردی مستقل از پلت‌فرم**

کنترل:سیستم اطلاعاتی شامل این موارد است: [اختصاص: برنامه‌های کاربردی مستقل از پلت‌فرم تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: پلت‌فرم‌ها ترکیبی از سخت‌افزارها و نرم‌افزارهای مورد استفاده برای اجرای برنامه‌های کاربردی هستند. پلت‌فرم‌ها شامل این موارد هستند: (۱) سیستم‌عامل‌ها؛ (۲) معماری رایانه‌ای مربوطه؛ یا (۳) هر دو مورد. منظور از برنامه‌های کاربردی مستقل از پلت‌فرم، آن دسته از برنامه‌های کاربردی است که روی پلت‌فرم‌های مختلف اجرا می‌شوند. این برنامه‌های کاربردی قابلیت جابجایی و بازسازی روی پلت‌فرم‌های مختلف را بهبود می‌دهند و سبب ارتقای آماده کار بودن کارکردهای اصلی سازمان در صورت حمله به سیستم‌های اطلاعاتی دارای سیستم‌عامل‌های خاص می‌شوند. کنترل مربوطه: SC-29.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-28: **حفاظت از اطلاعات بایگانی‌شده**[۲۴۹]

کنترل: سیستم اطلاعاتی از [انتخاب (یک یا چند مورد): محرمانگی؛ یکپارچگی] [اختصاص: اطلاعات بایگانی‌شده تعیین‌شده توسط سازمان] محافظت می‌کند.

راهنمایی‌های تکمیلی: این کنترل به محرمانگی و یکپارچگی اطلاعات بایگانی‌شده می‌پردازد و اطلاعات کاربری و اطلاعات سیستم را پوشش می‌دهد. منظور از اطلاعات بایگانی‌شده، اطلاعاتی است که روی دستگاه‌های ذخیره‌سازی از جمله مؤلفه‌های سیستم اطلاعاتی ذخیره شده‌اند. اطلاعات سیستمی که باید از آن‌ها محافظت شود، مواردی از جمله پیکربندی‌ها یا قوانین تعیین‌شده برای فایروال‌ها، گیت‌وی‌ها، سیستم‌های تشخیص ورود غیر مجاز، سیستم‌های جلوگیری از ورود غیر مجاز، مسیریاب‌های فیلترینگ و محتوای مورد استفاده برای احراز

[249] information at rest

هویت اشاره کرد. سازمان‌ها ممکن است از سازوکارهای مختلفی برای محافظت از محرمانگی و یکپارچگی اطلاعات استفاده کنند که از آن جمله می‌توان به سازوکارهای رمزنگاری و اسکن اشتراک‌گذاری فایل اشاره کرد. برای حفاظت از یکپارچگی می‌توان مثلاً از فناوری‌های WORM[۲۵۰] استفاده کرد. سازمان‌ها ممکن است از کنترل‌های امنیتی دیگر نیز استفاده کنند که از میان آن‌ها می‌توان به ذخیره‌سازی آفلاین امن به جای ذخیره‌سازی آنلاین (در صورتی که نتوان به روش‌های دیگر از اطلاعات محافظت به عمل آورد) و/یا پایش مستمر برای شناسایی کدهای مخرب بایگانی‌شده اشاره کرد. کنترل‌های مربوطه: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

کنترل‌های پیشرفته:

(۱) حفاظت از اطلاعات بایگانی‌شده / حفاظت رمزنگاری

سیستم اطلاعاتی از سازوکارهای رمزنگاری برای جلوگیری از دستکاری و افشای غیر مجاز [اختصاص: اطلاعات تعیین‌شده توسط سازمان] در [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: انتخاب سازوکارهای رمزنگاری بر اساس نیاز به حفاظت از یکپارچگی و محرمانگی اطلاعات سازمان انجام می‌شود. قدرت این سازوکارها متناسب با دسته‌بندی امنیتی و/یا میزان محرمانگی اطلاعات است. این کنترل پیشرفته در خصوص حجم زیاد رسانه‌های دیجیتال در بخش‌هایی از سازمان اعمال می‌شود که برای ذخیره‌سازی رسانه‌ها در نظر گرفته شده‌اند. کنترل حاضر همچنین در مورد کمیت‌های اندک رسانه‌ها اعمال نیز می‌شود. این شرایطمعمولاً در مورد مؤلفه‌های سیستم اطلاعاتی در محیط‌های عملیاتی (مانند دستگاه‌های ذخیره‌سازی قابل حمل و دستگاه‌های همراه) مشاهده می‌شود. سازمان‌ها این حق انتخاب را دارند که تمام اطلاعات موجود روی دستگاه‌های ذخیره‌سازی را رمزگذاری کنند یا این که تنها برخی ساختارهای خاص داده‌ها (مانند فایل‌ها، سوابق یا فیلدها) را رمزگذاری نمایند. سازمان‌هایی که از سازوکارهای رمزنگاری برای حفاظت از اطلاعات بایگانی‌شده استفاده می‌کنند، روش‌های مدیریت کلید رمزنگاری را نیز مد نظر قرار می‌دهند. کنترل‌های مربوطه: AC-19, SC-12.

(۲) حفاظت از اطلاعات بایگانی‌شده / ذخیره‌سازی آفلاین

[250] Write-Once-Read-Many

سازمان [اختصاص: اطلاعات تعیین‌شده توسط سازمان] را از حافظه‌های آنلاین خارج می‌کند و آن‌ها را در مکانی امن در حافظه‌های آفلاین قرار می‌دهد.

راهنمایی‌های تکمیلی: خارج کردن اطلاعات از حافظه‌های آنلاین و قرار دادن آن‌ها در حافظه‌های آفلاین باعث کاهش خطر دسترسی غیر مجاز به این اطلاعات از طریق شبکه می‌شود. بنابراین، ممکن است سازمان‌ها تصمیم بگیرند که اطلاعات را به حافظه‌های آفلاین منتقل نمایند.

مراجع: نشریه‌های ویژه شماره ۵۵-۸۰۰ و ۵۷-۸۰۰ و ۱۱۱-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، سطح تأثیرکم	SC-28 سطح تأثیر متوسط	SC-28 سطح تأثیر زیاد

SC-29: **عدم تجانس**

کنترل: سازمان برای پیاده‌سازی سیستم اطلاعاتی، از فناوری‌های اطلاعاتی مختلفی در [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: افزایش تنوع فناوری‌های اطلاعاتی در سیستم‌های اطلاعاتی سازمان، احتمال بهره‌گیری از آسیب‌پذیری‌های برخی فناوری‌های خاص از سوی مهاجمان را کاهش می‌دهد و از برخی حالت‌های خاص از کار افتادن، از جمله از کار افتادن در اثر حمله به زنجیره تأمین جلوگیری می‌نماید. تنوع این فناوری‌ها همچنین باعث می‌شود که مهاجمان به سادگی نتوانند ابزارهای حمله به یک مؤلفه سیستم را برای نفوذ به سایر مؤلفه‌ها نیز به کار گیرند. البته افزایش تنوع فناوری‌ها ممکن است باعث افزایش پیچیدگی و دشواری فرایندهای مدیریتی شود و در نتیجه، منجر به بروز خطا و پیکربندی‌های غیر مجاز گردد. کنترل‌های مربوطه: SA-12, SA-14, SC-27.

کنترل‌های پیشرفته:

(۱) عدم تجانس / شیوه‌های مجازی‌سازی

سازمان برای پشتیبانی از پیاده‌سازی برنامه‌های کاربردی و سیستم‌عامل‌های مختلف که در [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان] تغییر می‌کنند، از شیوه‌های مجازی‌سازی استفاده می‌کند.

راهنمایی‌های تکمیلی: با این که تغییرات مکرر در برنامه‌های کاربردی و سیستم‌عامل‌ها سبب چالش‌هایی برای مدیریت پیکربندی می‌شود، اما کار را برای مهاجمان نیز بسیار دشوار می‌کند و باعث می‌شود که انجام حملات موفق از سوی آن‌ها نیازمند تلاش بیشتری باشد. تغییر برنامه‌های کاربردی یا سیستم‌عامل‌های مجازی، در مقابل تغییر برنامه‌های کاربردی یا سیستم‌عامل‌های واقعی، سبب تغییرات مجازی می‌شود که موفقیت مهاجمان را با مشکل مواجه می‌کنند و همچنین مدیریت پیکربندی را تسهیل می‌نماید. علاوه بر این، شیوه‌های مجازی‌سازی سازمان‌ها را یاری می‌کنند تا نرم‌افزارهای قابل اعتماد را از نرم‌افزارهای مشکوک جدا کند و آن‌ها را در محیط‌های اجرایی محدودی قرار دهد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-30: اختفا[۲۵۱] و گمراه‌سازی[۲۵۲]

کنترل: سازمان برای اختفا و گمراه‌سازی مهاجمان، در [اختصاص: سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] و در [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان] از [اختصاص: شیوه‌های تعیین‌شده توسط سازمان در زمینه اختفا و گمراه‌سازی] استفاده می‌کند.

راهنمایی‌های تکمیلی: شیوه‌های اختفا و گمراه‌سازی می‌توانند توانایی مهاجمان برای آغاز و تکمیل حملات سایبری را تا حد زیادی کاهش دهند. به عنوان مثال، شیوه‌های مذکور سازمان‌ها را قادر می‌سازند تا سیستم‌های اطلاعاتی را از دید مهاجمان مخفی نمایند. بدین ترتیب، سازمان‌ها بدون نیاز به صرف هزینه برای داشتن چند پلت‌فرم مختلف، می‌توانند خطر حملات موفق را کاهش دهند. استفاده از شیوه‌های اختفا و گمراه‌سازی باعث کاهش احتمال موفقیت مهاجمان و افزایش احتمال به دام افتان آن‌ها می‌شود. این شیوه‌ها همچنین زمان کافی برای انجام مأموریت‌ها و فرایندهای اصلی کسب‌وکار را در اختیار سازمان‌ها قرار می‌دهند. به دلیل این که شیوه‌های اختفا و گمراه‌سازی نیازمند صرف زمان و تلاش‌های زیادی از سوی سازمان هستند، انتظار می‌رود که سازمان‌های محدودی از این شیوه‌ها استفاده نمایند. کنترل‌های مربوطه: SC-26, SC-29, SI-14.

[251] concealment
[252] misdirection

کنترل‌های پیشرفته:

(۱) اختفا و گمراه‌سازی / شیوه‌های مجازی‌سازی

[حذف شد: به بخش SC-29(1) منتقل شد].

(۲) اختفا و گمراه‌سازی / تصادفی‌سازی

سازمان برای تصادفی کردن دارایی‌ها و عملیات خود از [اختصاص: شیوه‌هایتعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: تصادفی‌سازی سبب افزایش عدم قطعیت برای عوامل متخاصم می‌شود، به گونه‌ای که به خوبی متوجه اقدامات سازمان برای دفاع در برابر حملات سایبری نخواهند شد. این اقدامات سبب می‌شوند که مهاجمان به راحتی نتوانند منابع اطلاعاتی پشتیبان مأموریت‌ها و فرایندهای اصلی کسب‌وکار را هدف قرار دهند. عدم قطعیت همچنین سبب می‌شود که مهاجمان پیش از آغاز یا ادامه دادن حملات خود، مکث و تعلل به خرج دهند. برخی روش‌هایی که برای تصادفی‌سازی به کار گرفته می‌شوند عبارتند از: انجام برخی اقدامات معمول در ساعت‌های مختلف شبانه‌روز، استفاده از فناوری‌های اطلاعاتی متفاوت (مانند مرورگرها، موتورهای جستجو و موارد دیگری از این دست)، استفاده از تأمین‌کنندگان مختلف و چرخش وظایف و مسئولیت‌های کارکنان سازمان.

(۳) اختفا و گمراه‌سازی / تغییر مکان پردازش یا ذخیره‌سازی

سازمان مکان [اختصاص: ذخیره‌سازی و/یا پردازش تعیین‌شده توسط سازمان] را در [انتخاب: [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان]؛ بازه‌های زمانی تصادفی] تغییر می‌دهد.

راهنمایی‌های تکمیلی: مهاجمان مأموریت‌ها و کارکردهای اصلی کسب‌وکار و منابع اطلاعاتی پشتیبان آن‌ها را هدف قرار می‌دهند و در عین حال تلاش می‌کنند تا موجودیت و فعالیت‌های خود را تا حد امکان مخفی کنند. ایستا، متجانس و قطعی بودن سیستم‌های اطلاعاتی سازمان باعث می‌شود که حمله به آن‌ها توسط مهاجمان ساده‌تر و نیازمند زمان و تلاش‌های کمتری باشد. سازمان با تغییر مکان پردازش یا ذخیره‌سازی اطلاعات، تلاش می‌کند تا با روش‌هایی مانند مجازی‌سازی، پردازش توزیع‌شده و استفاده از سیستم‌های جایگزین، با تهدیدات مداوم پیشرفته مقابله نماید. در این روش، سازمان مکان سیستم‌های پردازش یا ذخیره‌سازی که پشتیبان مأموریت‌ها و کارکردهای اصلی کسب‌وکار هستند را تغییر می‌دهد. بدین ترتیب، مهاجمان با عدم قطعیت در انتخاب اهداف خود مواجه خواهند شد. بدین ترتیب، مهاجمان باید زمان بیشتری صرف کنند و تلاش بسیار بیشتری به خرج دهند و این احتمال نیز

وجود خواهد داشت که در حین تلاش برای یافتن منابع اصلی سازمان، مکان آن‌ها آشکار شود و به دام افتند.

(۴) اختفا و گمراه‌سازی / اطلاعات گمراه‌کننده

سازمان در [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] از اطلاعات واقعی اما گمراه‌کننده درباره وضعیت امنیتی خود استفاده می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته مهاجمان را درباره وضعیت امنیتی و ابزارهای امنیتی مورد استفاده سازمان به اشتباه می‌اندازد. در نتیجه، ممکن است مهاجمان از روش‌های نامناسب و ناکارامدی برای حمله استفاده نمایند. یکی از روش‌های انجام این کار این است که سازمان اهداف بالقوه مهاجمان را شناسایی کند و اطلاعات گمراه‌کننده‌ای را درباره کنترل‌های امنیتی به‌کارگرفته‌شده در آن‌ها ارائه می‌کند. در روشی دیگر، می‌توان از شبکه‌های گمراه‌کننده‌ای استفاده کرد که جنبه‌های واقعی سیستم‌های اطلاعاتی سازمان را شبیه‌سازی می‌کنند اما در آن‌ها از پیکربندی‌های نرم‌افزاری قدیمی استفاده می‌شود.

(۵) اختفا و گمراه‌سازی / اختفای مؤلفه‌های سیستم

سازمان [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] را با استفاده از [اختصاص: شیوه‌های تعیین‌شده توسط سازمان] مخفی می‌کند.

راهنمایی‌های تکمیلی:با استتار یا مخفی کردن مؤلفه‌های مهم سیستم‌های اطلاعاتی، سازمان می‌تواند احتمال حمله به این مؤلفه‌ها و به خطر افتادن آن‌ها را کاهش دهد. برخی ابزارهایی که سازمان‌ها برای مخفی کردن مؤلفه‌های سیستم‌های اطلاعاتی به کار می‌گیرند عبارتند از: پیکربندی مسیریاب‌ها یا استفاده از هانی‌پات‌ها یا شیوه‌های مجازی‌سازی.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-31: تحلیل کانال‌های مخفی

کنترل: سازمان:

الف. تحلیل کانال‌های مخفی را انجام می‌دهد تا بخش‌هایی از ارتباطات در سیستم اطلاعاتی که می‌توانند محل کانال‌های مخفی [انتخاب (یک یا چند مورد): ذخیره‌سازی؛ زمان‌بندی] باشند را شناسایی کند؛ و

ب. حداکثر پهنای باند این کانال‌ها را تخمین می‌زند.

راهنمایی‌های تکمیلی:توسعه‌دهندگان بهتر از هر گروه دیگری می‌توانند کانال‌های مخفی سیستم را شناسایی نمایند. تحلیل کانال‌های مخفی هنگامی انجام می‌شود که احتمال جریان غیر مجاز اطلاعات در دامنه‌های امنیتی وجود داشته باشد. به عنوان مثال، در صورتی که سیستم‌های اطلاعاتی شامل اطلاعاتی باشد که نباید از سیستم خارج شوند و با شبکه‌های خارجی نیز ارتباط دارند (شبکه‌هایی که تحت کنترل سازمان نیستند). تحلیل کانال‌های مخفی در مورد سیستم‌های اطلاعاتی MLS، سیستم‌های MSL و سیستم‌های بین‌دامنه‌ای نیز انجام می‌شود. کنترل‌های مربوطه: AC-3, AC-4, PL-2.

کنترل‌های پیشرفته:

(۱) تحلیل کانال‌های مخفی / آزمون کردن امکان سوء استفاده از کانال‌های مخفی

سازمان زیرمجموعه‌ای از کانال‌های مخفی شناسایی‌شده را آزمون می‌کند تا تعیین نماید که کدام کانال‌ها قابل سوء استفاده هستند.

(۲) تحلیل کانال‌های مخفی / حداکثر پهنای باند

سازمان حداکثر پهنای باند کانال‌های مخفی [انتخاب (یک یا چند مورد): ذخیره‌سازی؛ زمان‌بندی] شناسایی‌شده را به [اختصاص: مقدار تعیین‌شده توسط سازمان] کاهش می‌دهد.

راهنمایی‌های تکمیلی:توسعه‌دهندگان سیستم‌های اطلاعاتی بهتر از هر گروه دیگری می‌توانند حداکثر پهنای باند کانال‌های مخفی زمان‌بندی و ذخیره‌سازی را کاهش دهند.

(۳) تحلیل کانال‌های مخفی / سنجش پهنای باند در محیط عملیاتی

سازمان پهنای باند [اختصاص: زیرمجموعه کانال‌های مخفی تعیین‌شده توسط سازمان] را در محیط عملیاتی سیستم اطلاعاتی اندازه‌گیری می‌کند.

راهنمایی‌های تکمیلی:این کنترل پیشرفته به پهنای باند کانال‌های مخفی در محیط‌های عملیاتی در مقابل محیط‌های توسعه‌ای می‌پردازد. اندازه‌گیری پهنای باند کانال‌های مخفی در محیط‌های عملیاتی سازمان را یاری می‌کند تا دریابد پیش از بروز تأثیر منفی در مأموریت‌ها و کارکردهای کسب‌وکار، چه

مقدار اطلاعات می‌تواند به طور مخفی نشت کند. پهنای باند کانال‌های مخفی در محیط‌های مستقل از محیط‌های خاص عملیاتی (مانند آزمایشگاه‌ها و محیط‌های توسعه‌ای) ممکن است بسیار متفاوت باشد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-32: بخش‌بندی سیستم‌های اطلاعاتی

کنترل: سازمان سیستم‌های اطلاعاتی را به [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] مستقر در محیط‌ها یا دامنه‌های فیزیکی مجزا بر اساس [اختصاص: شرایطی که سازمان برای بخش‌بندی فیزیکی مؤلفه‌ها تعیین کرده است] بخش‌بندی می‌کند.

راهنمایی‌های تکمیلی: بخش‌بندی سیستم‌های اطلاعاتی بخشی از راهبرد دفاع در عمق است. سازمان‌ها میزان جدایی فیزیکی مؤلفه‌های سیستم را تعیین می‌کنند. گاه ممکن است مؤلفه‌ها در بخش‌های جداگانه یک اتاق قرار داشته باشند و گاه نیز در مکان‌های مختلف جغرافیایی قرار گیرند. این بخش‌بندی بر اساس دسته‌بندی امنیتی مؤلفه‌ها انجام می‌شود. واسط‌های مدیریت‌شده، دسترسی به شبکه و جریان اطلاعات بین مؤلفه‌های بخش‌بندی‌شده را محدود یا ممنوع می‌کنند. کنترل‌های مربوطه: AC-4, SA-8, SC-2, SC-3, SC-7.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: FIPS 199.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-33: یکپارچگی آماده‌سازی انتقال

[حذف شد: به بخش SC-8 منتقل شد].

SC-34: برنامه‌های اجرایی غیر قابل تغییر

کنترل: سیستم اطلاعاتی در [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان]:

الف. محیط عملیاتی را از رسانه‌های صرفاً خواندنی مبتنی بر سخت‌افزار بارگذاری و اجرا می‌کند؛ و

ب. [اختصاص: برنامه‌های کاربردی تعیین‌شده توسط سازمان] را از رسانه‌های صرفاً خواندنی مبتنی بر سخت‌افزار بارگذاری و اجرا می‌کند.

راهنمایی‌های تکمیلی:منظور از محیط عملیاتی، کد ویژه‌ای است که میزبانی برنامه‌های کاربردی از جمله سیستم‌عامل‌ها، برنامه‌های اجرایی یا برنامه‌های پایشگر (مانند پایشگر ماشین مجازی) را بر عهده دارد. محیط عملیاتی همچنین می‌تواند شامل برنامه‌های کاربردی خاصی باشد که مستقیماً روی پلت‌فرم‌های سخت‌افزاری اجرا می‌شوند. رسانه‌های صرفاً خواندنی و مبتنی بر سخت‌افزار، مواردی از جمله CD، DVD و حافظه‌های صرفاً خواندنی قابل برنامه‌ریزی را شامل می‌شوند. با استفاده از حافظه‌های غیر قابل تغییر، می‌توان از یکپارچگی نرم‌افزارها اطمینان حاصل نمود. از حافظه‌های صرفاً خواندنی قابل برنامه‌ریزی مجدد نیز می‌توان به عنوان رسانه‌های صرفاً خواندنی استفاده کرد، مشروط بر این که: (۱) از زمان نوشته شدن اولیه اطلاعات روی حافظه تا زمان متصل شدن آن به سیستم اطلاعاتی، بتوان به خوبی از یکپارچگی آن محافظت نمود؛ و (۲) ابزارهای حفاظت فیزیکی لازم وجود داشته باشد که از برنامه‌ریزی مجدد حافظه در حالی که روی سیستم اطلاعاتی سازمان نصب است، جلوگیری نماید. کنترل‌های مربوطه: AC-3, SI-7.

کنترل‌های پیشرفته:

(۱) برنامه‌های اجرایی غیر قابل تغییر / عدم استفاده از حافظه‌های قابل نوشتن

سازمان از [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] بدون حافظه‌های قابل نوشتن استفاده می‌کند که در هنگام راه‌اندازی مجدد یا روشن و خاموش شدن نیز این ویژگی خود را حفظ می‌کنند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته: (۱) امکان انتقال یافتن کدهای مخرب به مؤلفه‌های سیستم اطلاعاتی از طریق حافظه‌های قابل نوشتن را از بین می‌برد؛ و (۲) هم در مورد حافظه‌های ثابت

و هم در مورد حافظه‌های قابل حمل اعمل می‌شود. الزامات حافظه‌های قابل حمل به طور مستقیم یا از طریق کنترل‌های دسترسی برای دستگاه‌های همراه بیان می‌شوند. کنترل‌های مربوطه: AC-19, MP-7.

(۲) برنامه‌های اجرایی غیر قابل تغییر / حفاظت از یکپارچکی و رسانه‌های صرفاً خواندنی

سازمان پیش از ذخیره‌سازی اطلاعات روی رسانه‌های صرفاً خواندنی از یکپارچگی آن‌ها حفاظت می‌کند و پس از ذخیره‌سازی نیز رسانه‌های مذکور را کنترل می‌نماید.

راهنمایی‌های تکمیلی: ابزارهای حفاظتی مانع از جایگزینی رسانه‌ها در سیستم‌های اطلاعاتی یا برنامه‌ریزی مجدد این رسانه‌ها پیش از نصب در سیستم می‌شوند. به عنوان مثال‌هایی از ابزارهای امنیتی می‌توان به ترکیب فرایندهای جلوگیری، ردیابی و اقدام اشاره کرد. کنترل‌های مربوطه: AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3.

(۳) برنامه‌های اجرایی غیر قابل تغییر / حفاظت مبتنی بر سخت‌افزار

سازمان:

الف. از ابزارهای مبتنی بر سخت‌افزار برای جلوگیری از نوشتن اطلاعات روی [اختصاص: مؤلفه‌های ثابت‌افزار سیستم اطلاعاتی تعیین‌شده توسط سازمان] استفاده می‌کند؛ و

ب. رویه‌های خاصی را برای [اختصاص: افراد مجاز تعیین‌شده توسط سازمان] در نظر می‌گیرد تا بتوانند ابزارهای حفاظتی فوق را به طور دستی غیر فعال کنند و پیش از بازگشت به حالت عملیاتی مجدداً فعال نمایند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-35: هانی‌کلاینت‌ها

کنترل: سیستم اطلاعاتی از مؤلفه‌هایی استفاده می‌کند که به صورت پیش‌دستانه، وب‌سایت‌های مخرب و/یا کدهای مخرب مبتنی بر وب را شناسایی می‌کنند.

راهنمایی‌های تکمیلی: تفاوت هانی‌کلاینت‌ها با هانی‌پات‌ها در این است که هانی‌کلاینت‌ها به صورت فعال اینترنت را جستجو می‌کنند تا کدهای مخرب (مانند کرم‌های رایانه‌ای) موجود در وب‌سایت‌های خارج از سازمان

را بیابند. با این حال، هانی‌کلاینت‌ها نیز مانند هانی‌پات‌ها نیازمند ابزارهای ایزوله‌سازی پشتیبان (مانند روش‌های مجازی‌سازی) هستند تا اطمینان حاصل شود که کدهای مخرب شناسایی‌شده در فرایند جستجو بر سیستم‌های اطلاعاتی سازمان تأثیر منفی نمی‌گذارند. کنترل‌های مربوطه: SC-26, SC-44, SI-3, SI-4.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-36: پردازش و ذخیره‌سازی توزیع‌شده

کنترل: سازمان فرایندهای [اختصاص: پردازش و ذخیره‌سازی تعیین‌شده توسط سازمان] را در مکان‌های فیزیکی مختلف توزیع می‌کند.

راهنمایی‌های تکمیلی: توزیع فرایندهای پردازش و ذخیره‌سازی در مکان‌های فیزیکی مختلف، قابلیت جایگزینی و همپوشانی را برای سازمان به دنبال خواهد داشت. بدین ترتیب، مهاجمان باید برای به خطر انداختن عملیات، دارایی‌ها و افراد سازمان، تلاش بیشتری به خرج دهند. این کنترل یک مکان پردازش یا ذخیره‌سازی را به عنوان مکان مرکزی در نظر نمی‌گیرد و در نتیجه، از سیستم‌های پردازش و ذخیره‌سازی موازی پشتیبانی می‌نماید. کنترل‌های مربوطه: CP-6, CP-7.

کنترل‌های پیشرفته:

(۱) پردازش و ذخیره‌سازی توزیع‌شده / شیوه‌های نظرسنجی

سازمان برای شناسایی معایب، خطاها یا خطرات بالقوه علیه [اختصاص: مؤلفه‌های پردازش و ذخیره‌سازی توزیع‌شده تعیین‌شده توسط سازمان]، از شیوه‌های نظرسنجی استفاده می‌کند.

راهنمایی‌های تکمیلی: فرایندهای پردازش و ذخیره‌سازی توزیع‌شده به این دلیل به کار گرفته می‌شوند که فرصت‌های مهاجمان برای به خطر انداختن محرمانگی، یکپارچگی یا آماده کار بودن اطلاعات و سیستم‌های اطلاعاتی کاهش یابد. با این حال، استفاده از روش‌های پردازش و ذخیره‌سازی توزیع‌شده، امکان به خطر افتادن یک (یا چند) مؤلفه توزیع‌شده را به طور کلی از بین نمی‌برد. در شیوه‌های نظرسنجی، نتایج پردازش و/یا محتوای ذخیره‌سازی مربوط به مؤلفه‌های توزیع‌شده مختلف با هم

مقایسه می‌گردند و در ادامه خروجی‌ها به رأی گذاشته می‌شوند. بدین ترتیب، معایب، خطاها یا خطرات بالقوه علیه مؤلفه‌های پردازش و ذخیره‌سازی توزیع‌شده شناسایی می‌شوند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-37: کانال‌های خارج از باند

کنترل: سازمان برای تحویل فیزیکی یا انتقال الکترونیک [اختصاص: اطلاعات، مؤلفه‌های سیستم اطلاعاتی یا دستگاه‌های تعیین‌شده توسط سازمان] به [اختصاص: سیستم‌های اطلاعاتی یا افراد تعیین‌شده توسط سازمان] از [اختصاص: کانال‌های خارج از باند تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: کانال‌های خارج از باند چنین مواردی را در بر می‌گیرند: دسترسی‌های محلی (غیر شبکه) به سیستم‌های اطلاعاتی، مسیرهای شبکه که به صورت فیزیکی از مسیرهای شبکه مورد استفاده برای ترافیک عملیاتی جدا شده‌اند، یا مسیرهای غیر الکترونیک مانند سرویس پستی US. این رویکرد در مقابل رویکردی قرار می‌گیرد که در آن از کانال‌های واحدی استفاده می‌شود (کانال‌های داخل باند) که ترافیک عملیاتی معمول را انتقال می‌دهند. کانال‌های خارج از باند مانند کانال‌های داخل باند نیستند که آسیب‌پذیری‌های واحدی داشته باشند، و در نتیجه عواملی که محرمانگی، یکپارچگی و آماده کار بودن کانال‌های داخل باند را تهدید می‌کنند، تهدیدی بر علیه آن‌ها به شمار نمی‌آیند. سازمان‌ها از کانال‌های خارج از باند برای تحویل و انتقال آیتم‌های فراوانی استفاده می‌کنند که از میان آن‌ها می‌توان به شناسه‌ها، عوامل احراز هویت، تغییرات مدیریت پیکربندی برای سخت‌افزارها، ثابت‌افزارها و نرم‌افزارها، اطلاعات مدیریت کلید رمزنگاری، به‌روزرسانی‌های امنیتی، نسخه‌های پشتیبان سیستم و داده‌ها، اطلاعات تعمیر و نگهداری، و به‌روزرسانی‌های مورد استفاده برای مقابله با کدهای مخرب اشاره کرد. کنترل‌های مربوطه: AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

کنترل‌های پیشرفته:

(۱) کانال‌های خارج از باند / تضمین صحت تحویل یا انتقال

سازمان با استفاده از [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] اطمینان حاصل می‌نماید که [اختصاص: اطلاعات، مؤلفه‌های سیستم‌های اطلاعاتی یا دستگاه‌های تعیین‌شده توسط سازمان] تنها توسط [اختصاص: سیستم‌های اطلاعاتی یا افراد تعیین‌شده توسط سازمان] دریافت می‌شود.

راهنمایی‌های تکمیلی: یکی از شیوه‌هایی که سازمان برای حصول اطمینان از این امر در نظر می‌گیرد این است که عوامل احراز هویت را از طریق پیک ارسال می‌کند اما از گیرندگان می‌خواهد که نوعی مدرک شناسایی دولتی را عرضه کنند.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-38: امنیت عملیات

کنترل: سازمان برای حفاظت از اطلاعات سازمانی مهم در سراسر چرخه عمر توسعه سیستم، از [اختصاص: ابزارهای امنیت عملیات تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: امنیت عملیات (OPSEC) یک فرایند سیستماتیک است که به واسطه آن اطلاعات غیر محرمانه مربوط به برنامه‌ریزی و اجرای فعالیت‌های حساس سازمان شناسایی، کنترل و محافظت می‌شوند و بدین ترتیب، مهاجمان بالقوه نمی‌توانند به اطلاعاتی درباره قابلیت‌ها و اهداف سازمان دست یابند. فرایند امنیت عملیات شامل پنج مرحله است: (۱) شناسایی اطلاعات حساس (مانند فرایند دسته‌بندی امنیتی)؛ (۲) تحلیل تهدیدات؛ (۳) تحلیل آسیب‌پذیری‌ها؛ (۴) ارزشیابی مخاطرات؛ و (۵) استفاده از ابزارهای امنیتی مناسب. ابزارهای امنیتی OPSEC هم در مورد سیستم‌های اطلاعاتی سازمان و هم در مورد محیط‌های عملیاتی این سیستم‌ها به کار گرفته می‌شوند. با استفاده از این ابزارها می‌توان از محرمانگی اطلاعات مهم حفاظت کرد. به عنوان مثال، سازمان‌ها با استفاده از این ابزارها اطلاعات کمتری را با تأمین‌کنندگان بالفعل یا بالقوه مؤلفه‌های سیستم‌های اطلاعاتی، خدمات و محصولات IT، و همچنین با افراد و موجودیت‌های غیر سازمانی به اشتراک می‌گذارند. از جمله اطلاعات مهم که باید از آن‌ها حفاظت نمود، می‌توان به هویت کاربران، موارد استفاده، فرایندهای مربوط به تأمین‌کنندگان و زنجیره تأمین، الزامات مالی و امنیتی، جزئیات طراحی سیستم،

پروتکل‌های آزمون، و اطلاعات مربوط به پیاده‌سازی کنترل‌های امنیتی اشاره کرد. کنترل‌های مربوطه: RA-2, RA-5, SA-12.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-39: ایزوله کردن فرایندها

کنترل: سیستم اطلاعاتی یک دامنه اجرایی مجزا را برای هر یک از فرایندهای اجرایی در نظر می‌گیرد.

راهنمایی‌های تکمیلی: سیستم‌های اطلاعاتی می‌توانند یک فضای آدرس مجزا را به هر فرایند اختصاص دهند و بدین ترتیب، یک دامنه اجرایی مجزا را برای هر یک از فرایندهای اجرایی در نظر گیرند. هر یک از فرایندهای سیستم اطلاعاتی دارای یک فضای آدرس مجزا است، به گونه‌ای که ارتباطات بین فرایندها در سراسر کارکردهای امنیتی به شکلی کنترل‌شده برقرار می‌شود و یک فرایند نمی‌تواند کد اجرایی فرایندهای دیگر را تغییر دهد. به منظور دستیابی به دامنه‌های اجرایی مجزا برای هر یک از فرایندهای اجرایی، می‌توان فضاهای آدرس جداگانه‌ای را برای آن‌ها در نظر گرفت. اکثر سیستم‌عامل‌های تجاری که از فناوری پردازنده‌های چندحالته استفاده می‌کنند، دارای این قابلیت هستند. کنترل‌های مربوطه: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3.

کنترل‌های پیشرفته:

(۱) ایزوله کردن فرایندها / تفکیک سخت‌افزاری

سیستم اطلاعاتی برای تسهیل تفکیک فرایندها، از سازوکارهای تفکیک سخت‌افزاری استفاده می‌نماید.

راهنمایی‌های تکمیلی: تفکیک مبتنی بر سخت‌افزار فرایندهای سیستم اطلاعاتی به طور کلی نسبت به تفکیک مبتنی بر نرم‌افزار امن‌تر است و در معرض خطرات کمتری قرار دارد. به عنوان مثالی از سازوکارهای تفکیک سخت‌افزاری می‌توان به مدیریت حافظه سخت‌افزاری اشاره کرد.

(۲) ایزوله کردن فرایندها / ایزوله کردن رشته‌ها[۲۵۳]

[253] threads

سیستم اطلاعاتی برای هر یک از رشته‌های موجود در [اختصاص: پردازش چندرشته‌ای تعیین‌شده توسط سازمان]، یک دامنه اجرایی مجزا در نظر می‌گیرد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SC-39 سطح تأثیرکم	SC-39 سطح تأثیر متوسط	SC-39 سطح تأثیر زیاد

SC-40: **حفاظت از لینک بی‌سیم**

سیستم اطلاعاتی از [اختصاص: لینک‌های بی‌سیم تعیین‌شده توسط سازمان] داخلی و خارجی در برابر [اختصاص: انواع حملات به پارامترهای سیگنال تعیین‌شده توسط سازمان یا ارجاع به منابع این حملات] محافظت می‌کند.

راهنمایی‌های تکمیلی: این کنترل در مورد لینک‌های ارتباطی بی‌سیم داخلی و خارجی اعمال می‌شود که ممکن است توسط افرادی که کاربر مجاز سیستم اطلاعاتی نیستند، قابل مشاهده باشند. اگر لینک‌های بی‌سیم به خوبی محافظت نشده باشند، مهاجمان می‌توانند به پارامترهای سیگنال این لینک‌ها حمله کنند. راه‌های زیادی برای حمله به پارامترهای سیگنال لینک‌های بی‌سیم به منظور سرقت اطلاعات از کاربران سیستم‌های اطلاعاتی سازمان وجود دارد. این کنترل از تأثیر حملاتی که مختص سیستم‌های بی‌سیم هستند، می‌کاهد. اگر سازمان‌ها به جای استفاده از خدمات کاملاً اختصاصی از خدمات تجاری برای انتقال اطلاعات استفاده کنند، ممکن است پیاده‌سازی این کنترل امکان‌پذیر نباشد. کنترل‌های مربوطه: AC-18, SC-5.

کنترل‌های پیشرفته:

(۱) حفاظت از لینک بی‌سیم / تداخل الکترومغناطیسی

سیستم اطلاعاتی برای دستیابی به [اختصاص: سطح حفاظت تعیین‌شده توسط سازمان] در برابر تأثیر تداخلات الکترومغناطیسی عمدی، از سازوکارهای رمزنگاری استفاده می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته برای دفاع در برابر تداخلات الکترومغناطیسی عمدی است که به دنبال اخلال در ارتباطات هستند. این کنترل پیشرفته اطمینان حاصل می‌نماید که شکل‌موج‌های طیف بی‌سیم مورد استفاده برای مقابله با این تداخلات، توسط افراد غیر مجاز قابل پیش‌بینی نیستند.

این کنترل پیشرفته ممکن است تأثیر منفی تداخلات غیر عمدی از سوی فرستنده‌های مجاز را نیز کاهش دهد. الزامات مأموریت سازمان، تهدیدات پیش‌بینی‌شده، مفهوم عملیات و قوانین، مقررات، رهنمودها، خط‌مشی‌ها، استانداردها و راهنمایی‌ها، تعیین‌کننده سطح آماده کار بودن لینک‌های بی‌سیم و عملکرد و رمزنگاری مورد نیاز هستند. کنترل‌های مربوطه: SC-12, SC-13.

(۲) حفاظت از لینک بی‌سیم / کاهش امکان شناسایی

سیستم اطلاعاتی برای کاهش امکان شناسایی لینک‌های بی‌سیم تا [اختصاص: سطح کاهش تعیین‌شده توسط سازمان]، از سازوکارهای رمزنگاری استفاده می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته امکان داشتن ارتباطات مخفی و جلوگیری از شناسایی مکان جغرافیایی فرستنده‌های بی‌سیم را فراهم می‌آورد. این کنترل پیشرفته اطمینان حاصل می‌نماید که شکل‌موج‌های طیف بی‌سیم مورد استفاده برای کاهش امکان شناسایی لینک‌های بی‌سیم، توسط افراد غیر مجاز قابل پیش‌بینی نیستند. الزامات مأموریت سازمان، تهدیدات پیش‌بینی‌شده، مفهوم عملیات و قوانین، مقررات، رهنمودها، خط‌مشی‌ها، استانداردها و راهنمایی‌ها، تعیین‌کننده سطح آماده کار بودن لینک‌های بی‌سیم و عملکرد و رمزنگاری مورد نیاز هستند. کنترل‌های مربوطه: SC-12, SC-13.

(۳) حفاظت از لینک بی‌سیم / ارتباطات بی‌سیم تقلیدگرانه یا متقلبانه

سیستم اطلاعاتی برای شناسایی و جلوگیری از تلاش‌های عمدی برای برقراری ارتباطات بی‌سیم تقلیدگرانه یا متقلبانه بر اساس پارامترهای سیگنال، از سازوکارهای رمزنگاری استفاده می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته اطمینان حاصل می‌نماید که پارامترهای سیگنال ارتباطات بی‌سیم، توسط افراد غیر مجاز قابل پیش‌بینی نیستند. این غیر قابل پیش‌بینی بودن احتمال برقراری ارتباطات بی‌سیم تقلیدگرانه یا متقلبانه بر اساس پارامترهای سیگنال را کاهش می‌دهد. کنترل‌های مربوطه: SC-12, SC-13.

(۴) حفاظت از لینک بی‌سیم / شناسایی پارامتر سیگنال

سیستم اطلاعاتی برای جلوگیری از شناسایی [اختصاص: فرستنده‌های بی‌سیم تعیین‌شده توسط سازمان] با استفاده از پارامترهای سیگنال فرستنده، از سازوکارهای رمزنگاری استفاده می‌کند.

راهنمایی‌های تکمیلی: شیوه‌های شناسایی یکتای رادیویی[۲۵۴]، پارامترهای منحصربه‌فرد سیگنال این فرستنده‌ها را شناسایی می‌کنند تا بتوان آن‌ها را ردیابی کرد. این کنترل پیشرفته اطمینان حاصل می‌نماید که تغییرات ایجادشده در پارامترهای سیگنال به منظور جلوگیری از شناسایی آن‌ها، توسط

[254] radio fingerprinting techniques

افراد غیر مجاز قابل پیش‌بینی نیستند. هنگامی که ناشناس بودن ضروری باشد، پیاده‌سازی این کنترل پیشرفته می‌تواند موفقیت مأموریت را تضمین کند. کنترل‌های مربوطه: SC-12, SC-13.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-41: دسترسی به دستگاه‌های ورودی/خروجی و پورت‌ها

سازمان [اختصاص: دستگاه‌های ورودی/خروجی یا پورت‌های اتصال تعیین‌شده توسط سازمان] روی [اختصاص: سیستم‌های اطلاعاتی یا مؤلفه‌های سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] را به طور فیزیکی قطع یا غیر فعال می‌کند.

راهنمایی‌های تکمیلی: به عنوان مثال‌هایی از پورت‌های اتصال می‌توان به پورت‌های USB و IEEE 1394 اشاره کرد. دستگاه‌های ورودی/خروجی نیز مواردی از جمله درایوهای CD و DVD را شامل می‌شوند. قطع یا غیر فعال کردن فیزیکی این پورت‌ها و دستگاه‌ها مانع خروج اطلاعات از سیستم‌های اطلاعاتی و ورود کدهای مخرب به آن‌ها می‌شود.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-42: داده‌ها و حسگرها

کنترل: سیستم اطلاعاتی:

الف. به اشتثنای موارد روبرو، از فعال‌سازی راه دور قابلیت حسگر محیطی جلوگیری به عمل می‌آورد: [اختصاص: موارد استثنا تعیین‌شده توسط سازمان در زمینه مجاز بودن فعال‌سازی راه دور حسگرها]؛ و

ب. نشانه‌های آشکار استفاده از حسگر را به [اختصاص: دسته‌های کاربران تعیین‌شده توسط سازمان] ارائه می‌نماید.

راهنمایی‌های تکمیلی: این کنترل معمولاً در مورد آن دسته از سیستم‌های اطلاعاتی و مؤلفه‌های سیستم اعمال می‌شود که دستگاه‌های همراه نامیده می‌شوند. به عنوان مثال، می‌توان به گوشی‌های هوشمند، تبلت‌ها و دستگاه‌های خواندن متون الکترونیک اشاره کرد. این سیستم‌ها معمولاً دارای حسگرهایی هستند که داده‌ها را از محیط جمع‌آوری و ثبت می‌کنند. برخی از حسگرهایی که در دستگاه‌های همراه تعبیه می‌شوند عبارتند از: دوربین‌ها، میکروفون‌ها، سازوکارهای GPS و شتاب‌سنج‌ها. هرچند که این حسگرها کارکرد بسیار مهم و مفیدی دارند، اما اگر به صورت مخفیانه به کار گرفته شوند، می‌توانند اطلاعات ارزشمندی را درباره افراد و سازمان‌ها در اختیار مهاجمان قرار دهند. به عنوان مثال، فعال‌سازی از راه دور GPS یک دستگاه همراه، مهاجم را قادر می‌سازد تا حرکت‌های فرد را ردیابی کند و از مکان وی اطلاع حاصل نماید.

کنترل‌های پیشرفته:

(۱) داده‌ها و حسگرها / گزارش‌دهی به کارکنان یا افراد مجاز

سازمان اطمینان حاصل می‌نماید که سیستم اطلاعاتی به گونه‌ای پیکربندی شده است که داده‌ها و اطلاعات گردآوری‌شده توسط [اختصاص: حسگرهای تعیین‌شده توسط سازمان]، تنها به کارکنان و افراد مجاز گزارش داده می‌شوند.

راهنمایی‌های تکمیلی: در صورتی که حسگرها توسط افراد مجاز (مانند کاربران نهایی) فعال شده باشند، کماکان این احتمال وجود دارد که داده‌ها و اطلاعات گردآوری‌شده به موجودیت‌های غیر مجاز گزارش داده شوند.

(۲) داده‌ها و حسگرها / کاربرد مجاز

سازمان به گونه‌ای از ابزارهای روبرو استفاده می‌کند که داده‌ها و اطلاعات گردآوری‌شده توسط [اختصاص: حسگرهای تعیین‌شده توسط سازمان] تنها برای مقاصد مجاز استفاده شوند: [اختصاص: ابزارهای تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: اطلاعات گردآوری‌شده توسط حسگرها برای یک مقصود خاص، ممکن است برای مقاصد غیر مجاز مورد سوء استفاده قرار گیرد. به عنوان مثال، حسگرهای GPS که برای پشتیبنی از ناوبری ترافیک به کار گرفته می‌شوند، ممکن است مورد سوء استفاده قرار گیرند و از آن‌ها برای ردیابی حرکات افراد استفاده شود. برای مقابله با این اقدامات می‌توان فعالیت‌هایی از این دست انجام داد: آموزش بیشتر برای حصول اطمینان از این که افراد و گروه‌های مجاز از اختیارات خود سوء استفاده نمی‌کنند، یا (در صورتی که داده‌ها و اطلاعات حسگرها توسط گروه‌های خارج از سازمان نگهداری می‌شوند) در نظر گرفتن محدودیت‌هایی در قراردادها در خصوص استفاده از اطلاعات و داده‌ها.

(۳) داده‌ها و حسگرها / منع استفاده از دستگاه‌ها

سازمان استفاده از دستگاه‌های پردازشگر [اختصاص: قابلیت‌های حسگر محیطی تعیین‌شده توسط سازمان] در [اختصاص: تأسیسات، نواحی و سیستم‌های تعیین‌شده توسط سازمان] را منع می‌کند.

راهنمایی‌های تکمیلی: به عنوان مثال، ممکن است سازمان به افراد اجازه ندهند که گوشی‌های همراه یا دوربین‌های دیجیتال خود را وارد محیط‌ها یا تأسیساتی کنند که اطلاعات حساس در آن‌ها نگهداری می‌شود یا گفتگوهای مهمی در آن‌ها صورت می‌گیرد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-43: محدودیت‌های کاربرد

کنترل: سازمان:

الف. بر اساس امکان وارد کردن خسارت به سیستم اطلاعاتی در صورت استفاده خرابکارانه، سازمان محدودیت‌هایی را برای کاربرد و راهنمایی‌هایی را برای پیاده‌سازی [اختصاص: مؤلفه‌های سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] در نظر می‌گیرد؛ و

ب. مجوز استفاده از این مؤلفه‌ها در سیستم اطلاعاتی را صادر و نحوه کاربرد آن‌ها را پایش و کنترل می‌کند.

راهنمایی‌های تکمیلی: مؤلفه‌های سیستم‌های اطلاعاتی، این موارد را در بر می‌گیرند: مؤلفه‌های سخت‌افزار، نرم‌افزار و ثابت‌افزار (مانند پروتکل VoIP، کد موبایل، دستگاه‌های کپی دیجیتال، چاپگرها، اسکنرها، دستگاه‌های نوری، فناوری‌های بی‌سیم و دستگاه‌های همراه). کنترل‌های مربوطه: CM-6, SC-7.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

SC-44: اتاق‌های انفجار[۲۵۵]

کنترل: سازمان از قابلیت اتاق انفجار در [اختصاص: سیستم‌های اطلاعاتی، مؤلفه‌های سیستم‌های اطلاعاتی، یا مکان‌های تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: اتاق‌های انفجار، که به آن‌ها محیط‌های اجرای پویا نیز گفته می‌شود، به سازمان اجازه می‌دهند تا در یک محیط ایزوله‌شده امن، پیوست‌های ایمیل‌ها را باز کند، برنامه‌های کاربردی مشکوک یا غیر قابل اعتماد را اجرا نماید و درخواست‌های URL را به اجرا در آورد. سازمان در این محیط‌های اجرایی ایزوله‌شده و محافظت‌شده تعیین می‌کند که آیا پیوست‌ها و برنامه‌های کاربردی مذکور دربردارنده کدهای مخرب هستند یا خیر. این کنترل که مربوط به مفهوم شبکه‌های فریبکار است، برای این طراحی نشده است که محیط مذکور به شکل طولانی‌مدت حفظ شود تا مهاجمان در آن فعالیت کنند و اقدامات آن‌ها رصد شود. بلکه، کنترل حاضر با این هدف طراحی شده است که کدهای مخرب به سرعت شناسایی شوند و از منتشر شدن آن‌ها در محیط‌های عملیاتی کاربری جلوگیری به عمل آید (یا این که از این انتشار به طور کلی ممانعت شود). کنترل‌های مربوطه: SC-7, SC-25, SC-26, SC-30.

کنترل‌های پیشرفته: وجود ندارد.

مراجع: وجود ندارد.

[255] detonation chambers

اولویت و تخصیص به مجموعه‌های پایه:

P0	انتخاب نشده، سطح تأثیرکم	انتخب نشده، سطح تأثیر متوسط	انتخاب نشده، سطح تأثیر زیاد

خانواده: یکپارچگی اطلاعات و سیستم

SI-1: خط‌مشی و رویه‌های یکپارچگی اطلاعات و سیستم

کنترل: سازمان:

الف. موارد زیر را تهیه و مستندسازی می‌کند و در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد:

۲۷. خط‌مشی برنامه‌ریزی برای رویدادهای آیندهشامل هدف، حیطه شمول، نقش‌ها، مسئولیت‌ها، تعهد مدیریتی، هماهنگی بین سازمان‌ها و تبعیت از استانداردها؛ و

۲۸. رویه‌های تسهیل پیاده‌سازیخط‌مشیبرنامه‌ریزی برای رویدادهای آینده و کنترل‌های مربوطه؛ و

ب. نسخه‌های موجود از موارد زیر را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] بازبینی و به‌روز می‌کند:

۲۷. خط‌مشی برنامه‌ریزی برای رویدادهای آینده؛ و

۲۸. رویه‌های برنامه‌ریزی برای رویدادهای آینده.

راهنمایی‌های تکمیلی: این کنترل توضیح می‌دهد که خط‌مشی و رویه‌های لازم برای پیاده‌سازی مؤثر کنترل‌های امنیتی چگونه تهیه می‌شوند و چگونه می‌توان کنترل‌های خانواده SI را ارتقا داد. خط‌مشی و رویه‌ها بازگو کننده دستورات اجرایی، رهنمودها، مقررات، خط‌مشی‌ها، استانداردها، رهنمون‌ها و قوانین فدرال هستند. رویه‌ها و خط‌مشی‌های برنامه امنیتی می‌توانند سازمان را از رویه‌ها و خط‌مشی‌های سیستمی بی‌نیاز کنند. این خط‌مشی را می‌توان به عنوان بخشی از خط‌مشی عمومی امنیت اطلاعات سازمان در نظر گرفت. خط‌مشی مذکور را همچنین می‌توان مجموعه‌ای از خط‌مشی‌های مختلف دانست که بازتاب‌دهنده ماهیت پیچیده برخی سازمان‌های خاص هستند. رویه‌ها را می‌توان به طور کلی برای برنامه امنیتی سازمان، و یا در صورت لزوم برای سیستم‌های اطلاعاتی خاص ایجاد نمود. راهبرد مدیریت مخاطرات سازمانی، عاملی اصلی در ایجاد این خط‌مشی و رویه‌ها است. کنترل‌های مربوطه: PM-9.

کنترل پیشرفته: وجود ندارد.

مراجع: نشریه‌های ویژه شماره ۱۲-۸۰۰ و ۱۰۰-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SI-1 سطح تأثیرکم	SI-1 سطح تأثیر متوسط	SI-1 سطح تأثیر زیاد

SI-2: **برطرف کردن معایب**

کنترل: سازمان:

الف. معایب سیستم اطلاعاتی را شناسایی، گزارش‌دهی و اصلاح می‌کند؛

ب. به‌روزرسانی‌های نرم‌افزارها و ثابت‌افزارها برای برطرف کردن معایب را آزمون می‌کند تا اثربخشی و اثرات جانبی بالقوه آن‌ها را پیش از نصب بسنجد؛

پ. به‌روزرسانی‌های نرم‌افزارها و ثابت‌افزارها را در [اختصاص: بازه زمانی تعیین‌شده توسط سازمان] پس از انتشار، نصب می‌کند؛ و

ت. راهکارهای برطرف کردن معایب را در فرایند مدریت پیکربندی سازمان می‌گنجاند.

راهنمایی‌های تکمیلی: سازمان آن دسته از سیستم‌های اطلاعاتی که تحت تأثیر معایب نرم‌افزاری اعلام‌شده قرار گرفته‌اند را شناسایی می‌کند و مراتب را به کارکنان مربوطه که مسئولیت‌های امنیتی را بر عهده دارند، گزارش می‌دهد. به عنوان مثال‌هایی از به‌روزرسانی‌های امنیتی می‌توان به این موارد اشاره کرد: بسته‌های به‌روزرسانی، بسته‌های خدماتی، بسته‌های تعمیری و امضاهای آنتی‌ویروس. سازمان همچنین تلاش می‌کند تا معایب شناسایی‌شده در جریان ارزشیابی‌های امنیتی، پایش مستمر، فعالیت‌های پاسخ به حوادث امنیتی و فرایندهای مدیریت خطاهای سیستم را برطرف نماید. بدین منظور، سازمان از منابع موجود از جمله پایگاه‌های داده CVE و CWE استفاده می‌کند. با استفاده از روش‌های برطرف کردن معایب در فرایندهای جاری مدیریت پیکربندی، می‌توان فعالیت‌های لازم یا پیش‌بینی‌شده برای این هدف را ردیابی و تأیید کرد. یکی از فعالیت‌هایی که می‌توان ردیابی و تأیید کرد این است که آیا سازمان از راهنمایی‌های US-CERT و هشدارهای آسیب‌پذیری ضمانت اطلاعات[۲۵۶] تبعیت می‌کند یا خیر. بازه زمانی تعیین‌شده توسط سازمان برای به‌روزرسانی ثابت‌افزارها و نرم‌افزارهای امنیتی به عوامل مختلفی بستگی دارد که از میان آن‌ها می‌توان به دسته امنیتی سیستم اطلاعاتی یا میزان اهمیت به‌روزرسانی (شدت آسیب‌پذیری مربوط به عیب شناسایی‌شده) اشاره کرد. برخی از روش‌های

[256] Information Assurance Vulnerability Alerts

مورد استفاده برای برطرف کردن معایب ممکن است نسبت به روش‌های دیگر به آزمون‌های بیشتری نیاز داشته باشند. سازمان تعیین می‌کند که روش مورد نظر برای برطرف کردن معایب به چه میزان و چه انواعی از آزمون‌ها نیاز دارد و همچنین مشخص می‌کند که پیکربندی کدام انواع تغییرات باید مدیریت شود. در برخی شرایط، ممکن است سازمان تعیین کند که آزمون کردن به‌روزرسانی‌های نرم‌افزارها و/یا سخت‌افزارها ضروری یا امکان‌پذیر نیست. این اتفاق مثلاً هنگامی رخ می‌دهد که از به‌روزرسانی‌های امضای آنتی‌ویروس ساده استفاده شود. سازمان همچنین ممکن است به این امر توجه کند که به‌رزورسانی‌های امنیتی نرم‌افزارها و ثابت‌افزارها از منابع مجاز تهیه شده و امضاهای دیجیتال معتبری دارند یا خیر. کنترل‌های مربوطه: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

کنترل‌های پیشرفته:

(۱) برطرف کردن معایب / مدیریت مرکزی

سازمان فرایند برطرف کردن معایب را به صورت مرکزی مدیریت می‌کند.

راهنمایی‌های تکمیلی: مدیریت مرکزی یعنی مدیریت و پیاده‌سازی فرایندهای برطرف کردن معایب در تمام سطح سازمان. مدیریت مرکزی شامل این مراحل است: برنامه‌ریزی، پیاده‌سازی، بررسی، صدور گواهی و پایش کنترل‌های امنیتی مربوط به برطرف کردن معایب که توسط سازمان تعیین شده و به صورت مرکزی مدیریت شده‌اند.

(۲) برطرف کردن معایب / وضعیت خودکار برطرف کردن معایب

سازمان برای تعیین وضعیت برطرف ساختن معایب در مؤلفه‌های سیستم اطلاعاتی، از سازوکارهای خودکار در [اختصاص: بازه‌های زمانی تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: CM-6, SI-4.

(۳) برطرف کردن معایب / زمان برطرف کردن معایب و معیارهایی برای انجام اقدامات اصلاحی

سازمان:

الف. زمان بین شناسایی و برطرف کردن معایب را اندازه‌گیری می‌کند؛ و

ب. [اختصاص: معیارهای تعیین‌شده توسط سازمان] را برای انجام اقدامات اصلاحی در نظر می‌گیرد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته از سازمان‌ها می‌خواهد تا تعیین کنند به طور میانگین چه مقدار زمان بین شناسایی و برطرف کردن معایب لازم است، و همچنین آن‌ها را ملزم می‌دارد تا

معیارهایی (یعنی چاچوب‌های زمانی) را برای انجام اقدامات اصلاحی در نظر گیرند. این معیارها را می‌توان بر اساس نوع معایب و/یا شدت آسیب‌پذیری حاصل از آن‌ها تعیین کرد.

(۴) برطرف کردن معایب / ابزارهای خودکار مدیریت به‌روزرسانی

[حذف شد: به بخش SI-2 منتقل شد].

(۵) برطرف کردن معایب / به‌روزرسانی خودکار نرم‌افزارها و ثابت‌افزارها

سازمان [اختصاص: به‌روزرسانی‌های امنیتی نرم‌افزارها و ثابت‌افزارهای تعیین‌شده توسط سازمان] را به صورت خودکار روی [اختصاص: مؤلفه‌های سیستم‌های اطلاعاتی تعیین‌شده توسط سازمان] نصب می‌کند.

راهنمایی‌های تکمیلی: به دلیل دغدغه‌های موجود درباره یکپارچگی و آماده کار بودن سیستم‌های اطلاعاتی، سازمان‌ها دقت زیادی به روش‌های مورد استفاده برای به‌روزرسانی خودکار دارند. سازمان‌ها باید بین نیاز به نصب هرچه سریع‌تر به‌روزرسانی‌ها، مدیریت پیکربندی، و تأثیرات به‌روزرسانی‌ها روی عملکرد سیستم تعادلی را برقرار نمایند.

(۶) برطرف کردن معایب / حذف کردن نسخه‌های قبلی نرم‌افزارها و ثابت‌افزارها

سازمان پس از نصب نسخه‌های به‌روز، [اختصاص: مؤلفه‌های ثابت‌افزار و نرم‌افزار تعیین‌شده توسط سازمان] را حذف می‌کند.

راهنمایی‌های تکمیلی: نسخه‌های قبلی ثابت‌افزارها و نرم‌افزارها که پس از نصب به‌روزرسانی‌ها هنوز از سیستم اطلاعاتی حذف نشده‌اند، در معرض خطر حمله مهاجمان قرار دارند. برخی محصولات IT به طور خودکار این نسخه‌های قدیمی را از سیستم حذف می‌کنند.

مراجع: نشریه‌های ویژه شماره ۴۰-۸۰۰ و ۱۲۸-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SI-2 سطح تأثیرکم	SI-2(2) سطح تأثیر متوسط	SI-2(1)(2) سطح تأثیر زیاد

SI-3: حفاظت در برابر کدهای مخرب

کنترل: سازمان:

الف. برای شناسایی و از بین بردن کدهای مخرب، در نقاط ورودی و خروجی سیستم‌های اطلاعاتی از سازوکارهای محافظت در برابر کدهای مخرب استفاده می‌کند؛

ب. در صورت منتشر شدن نسخه‌های جدید سازوکارهای محافظت در برابر کدهای مخرب، این سازوکارها را بر اساس خط‌مشی و رویه‌های مدیریت پیکربندی سازمان به‌روزرسانی می‌کند؛

پ. سازوکارهای محافظت در برابر کدهای مخرب را برای اهداف زیر به‌روزرسانی می‌کند:

۱. انجام اسکن دوره‌ای سیستم اطلاعاتی [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] و اسکن بلادرنگ فایل‌های منابع خارجی در [انتخاب (یک یا چند مورد): نقطه انتهایی؛ نقاط ورودی/خروجی شبکه] در هنگام دانلود شدن، باز شدن یا اجرا شدن این فایل‌ها بر اساس خط‌مشی‌های امنیتی سازمان؛ و

۲. [انتخاب (یک یا چند مورد): مسدود کردن کدهای مخرب؛ قرنطینه کردن کدهای مخرب؛ ارسال هشدار به راهبر؛ [اختصاص: اقدامات تعیین‌شده توسط سازمان]] در پاسخ به شناسایی کدهای مخرب؛ و

ت. مواردی که به اشتباه به عنوان کد مخرب شناسایی شده‌اند را مدیریت می‌کند و تأثیر این موارد بر آماده کار بودن سیستم اطلاعاتی را بررسی می‌نماید.

راهنمایی‌های تکمیلی: نقاط ورودی و خروجی سیستم اطلاعاتی مواردی از این دست را شامل می‌شوند: فایروال‌ها، سرورهای ایمیل، سرورهای وب، سرورهای پراکسی، سرورهای دسترسی از راه دور، ایستگاه‌های کاری، لپتاپ‌ها و دستگاه‌های همراه. کدهای مخرب نیز مواردی از جمله ویروس‌ها، کرم‌های رایانه‌ای، تروجان‌ها و جاسوس‌افزارها را در بر می‌گیرند. کدهای مخرب ممکن است در فرمت‌های مختلفی رمزگذاری شوند، درون فایل‌های مخفی یا فشرده قرار گیرند، یا با استفاده از روش‌های پنهان‌نگاری[۲۵۷] در فایل‌ها مخفی شوند. کدهای مخرب می‌توانند با استفاده از ابزارهای مختلفی منتقل شوند که از آن جمله می‌توان به دسترسی وب، ایمیل‌ها، پیوست ایمیل‌ها و دستگاه‌های ذخیره‌سازی قابل حمل اشاره کرد. مهاجمان با نفوذ به آسیب‌پذیری‌های سیستم اطلاعاتی، کدهای مخرب را وارد سیستم می‌نمایند. برخی ابزارهایی که برای محافظت در برابر کدهای مخرب به کار گرفته می‌شوند عبارتند از: امضاهای آنتی‌ویروس و فناوری‌های مبتنی بر اعتبار[۲۵۸]. دسته متنوعی از روش‌ها و فناوری‌ها برای محدود کردن یا از بین بردن اثرات کدهای مخرب ارائه شده‌اند. کنترل‌های جامع یکپارچگی نرم‌افزار و کنترل‌های مدیریت پیکربندی می‌توانند ابزارهای مناسبی برای جلوگیری از اجرای کدهای غیر مجاز

[257] steganography
[258] reputation-based technologies

باشند. علاوه بر نرم‌افزارهای تجاری موجود در بازار، کدهای مخرب ممکن است در نرم‌افزارهای سفارشی نیز وجود داشته باشند. این امر می‌تواند منجر به انجام حمله از طریق بمب‌های منطقی، دریچه‌های مخفی و روش‌های دیگر شود و مأموریت‌ها و کارکردهای کسب‌وکار سازمان را تحت تأثیر قرار دهد. روش‌های قدیمی شناسایی کدهای مخرب نمی‌توانند همواره در شناسایی این کدها مؤثر باشند. در این شرایط، سازمان‌ها از ابزارهای دیگری از جمله فعالیت‌های مبتنی بر کدهای مرجع، کنترل و مدیریت پیکربندی، فرایندهای تأمین و تدارک مورد اعتماد و پایش فعالیت‌ها استفاده می‌کنند تا اطمینان حاصل نمایند که نرم‌افزارها تنها کارکردهایی را انجام می‌دهند که برای آن‌ها در نظر گرفته شده است. سازمان‌ها ممکن است در صورت شناسایی کدهای مخرب، اقدامات مختلفی را مد نظر قرار دهند. به عنوان مثال، ممکن است شناسایی کدهای مخرب در جریان اسکن‌های دوره‌ای، دانلودهای مخرب و باز کردن پیوست‌ها، اقدامات مختلفی را از جانب سازمان در پی داشته باشد. کنترل‌های مربوطه: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

کنترل‌های پیشرفته:

(۱) حفاظت در برابر کدهای مخرب / مدیریت مرکزی

سازمان سازوکارهای حفاظت در برابر کدهای مخرب را به صورت مرکزی مدیریت می‌کند.

راهنمایی‌های تکمیلی: مدیریت مرکزی یعنی مدیریت و پیاده‌سازی سازوکارهای حفاظت در برابر کدهای مخرب در تمام سطح سازمان. مدیریت مرکزی شامل این مراحل است: برنامه‌ریزی، پیاده‌سازی، بررسی، صدور گواهی و پایش کنترل‌های امنیتی مربوط به حفاظت در برابر کدهای مخرب که توسط سازمان تعیین شده و به صورت مرکزی مدیریت شده‌اند. کنترل‌های مربوطه: AU-2, SI-8.

(۲) حفاظت در برابر کدهای مخرب / به‌روزرسانی خودکار

سیستم اطلاعاتی سازوکارهای حفاظت در برابر کدهای مخرب را به صورت خودکار به‌روزرسانی می‌کند.

راهنمایی‌های تکمیلی: به عنوان مثالی از سازوکارهای حفاظت در برابر کدهای مخرب، می‌توان به فرایندهای تعیین امضا اشاره کرد. به دلیل دغدغه‌های موجود درباره یکپارچگی و آماده کار بودن سیستم‌های اطلاعاتی، سازمان‌ها دقت زیادی به روش‌های مورد استفاده برای به‌روزرسانی خودکار دارند. کنترل مربوطه: SI-8.

(۳) حفاظت در برابر کدهای مخرب / کاربران بدون سطح دسترسی ویژه

[حذف شد: به بخش AC-6(10) منتقل شد].

(۴) حفاظت در برابر کدهای مخرب / به‌روزرسانی صرفاً توسط کاربران دارای سطح دسترسی ویژه

سیستم اطلاعاتی تنها در صورتی سازوکارهای حفاظت در برابر کدهای مخرب را به‌روزرسانی می‌کند که دستور این کار توسط کاربری با سطح دسترسی ویژه صادر شده باشد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته برای شرایطی مناسب است که به دلایل امنیتی یا به منظور ادامه یافتن عملیات، به‌روزرسانی تنها هنگامی صورت گیرد که دستور مربوطه توسط کارکنان خاصی صادر شده باشد. کنترل‌های مربوطه: AC-6, CM-5.

(۵) حفاظت در برابر کدهای مخرب / دستگاه‌های ذخیره‌سازی قابل حمل

[حذف شد: به بخش MP-7 منتقل شد].

(۶) حفاظت در برابر کدهای مخرب / آزمون و تأیید

سازمان:

الف. با وارد کردن یک نمونه آزمایشی بی‌خطر و غیر قابل انتشار به سیستم اطلاعاتی، سازوکارهای حفاظت در برابر کدهای مخرب را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] آزمون می‌کند؛ و

ب. تأیید می‌کند که نمونه آزمایشی شناسایی شده و حوادث امنیتی مربوطه نیز گزارش‌دهی شده‌اند.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: CA-2, CA-7, RA-5.

(۷) حفاظت در برابر کدهای مخرب / شناسایی غیر مبتنی بر امضا

سیستم اطلاعاتی از سازوکارهای شناسایی کدهای مخرب غیر مبتنی بر امضا استفاده می‌کند.

راهنمایی‌های تکمیلی: برخی سازوکارهای شناسایی کدهای مخرب غیر مبتنی بر امضا عبارتند از: استفاده از روش‌های اکتشافی برای شناسایی، تحلیل و توصیف ویژگی‌ها یا رفتارهای کدهای مخرب و ارائه ابزارهای امنیتی برای محافظت در برابر کدهای مخرب که هنوز امضایی برای آن‌ها ارائه نشده است یا امضاهای ارائه‌شده برای آن‌ها مؤثر نیستند. این امر شامل کدهای مخرب چندشکلی نیز می‌شود (یعنی کدهایی که امضای آن‌ها در هنگام انتشار عوض می‌شود). این کنترل پیشرفته استفاده از سازوکارهای شناسایی مبتنی بر امضا را منع نمی‌کند.

(۸) حفاظت در برابر کدهای مخرب / شناسایی دستورات غیر مجاز

سیستم اطلاعاتی [اختصاص: دستورات غیر مجاز سیستم‌عامل تعیین‌شده توسط سازمان] را از طریق وایط برنامه‌ریزی برنامه کاربردی کرنل در [اختصاص: مؤلفه‌های سخت‌افزار سیستم اطلاعاتی تعیین‌شده

توسط سازمان] شناسایی می‌کند و [انتخاب (یک یا چند مورد): هشداری را صادر می‌کند؛ اجرای دستور را ممیزی می‌کند؛ از اجرای دستور جلوگیری به عمل می‌آورد].

راهنمایی‌های تکمیلی: این کنترل پیشرفته را می‌توان در مورد واسط‌های مهم دیگری به جز واسط‌های مبتنی بر کرنل نیز به کار گرفت. به عنوان مثال، می‌توان به واسط‌های با ماشین مجازی و برنامه‌های کاربردی ویژه اشاره کرد. دستورات غیر مجاز سیستم‌عامل نیز مواردی از این دست را در بر می‌گیرند: دستورات مربوط به توابع کرنل از سوی فرایندهای سیستم اطلاعاتی که مجوز چنین کاری را ندارند یا مورد اعتماد نیستند، یا دستورات مربوط به توابع کرنل که حتی با وجود مجاز بودن باز هم مشکوک هستند. سازمان‌ها می‌توانند دستورات مخرب را با توجه به نوع دستور، دسته دستور یا نمونه‌های خاصی از دستورات شناسایی نمایند. سازمان‌ها همچنین می‌توانند مؤلفه‌های سخت‌افزاری را بر اساس مؤلفه‌های خاص، نوع مؤلفه‌ها، مکان آن‌ها در شبکه یا ترکیبی از این عوامل شناسایی کنند. ممکن است سازمان‌ها اقدامات مختلفی را برای انواع، دسته‌ها یا نمونه‌های خاص دستورات مخرب انجام دهند. کنترل مربوطه: AU-6.

(۹) حفاظت در برابر کدهای مخرب / احراز هویت دستورات راه دور

سیستم اطلاعاتی برای احراز هویت [اختصاص: دستورات راه دور تعیین‌شده توسط سازمان] از [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] استفاده می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته از سیستم در برابر دستورات غیر مجاز و بازپخش دستورات مجاز محافظت می‌کند. این قابلیت به ویژه برای آن دسته از سیستم‌های اطلاعاتی راه دور حائز اهمیت است که از کار افتادن، عملکرد نادرست یا به خطر افتادن آن‌ها عواقب جدی و/یا بلادرنگی برای سازمان دارد (مثلاً منجر به جراحت یا فوت افراد، وارد آمدن خسارت به سرمایه‌های سازمان، از دست رفتن دارایی‌های ارزشمند یا اطلاعات حساس، یا از کار افتادن مأموریت‌ها و کارکردهای اصلی کسب‌وکار می‌شود). ابزارهای مورد استفاده برای احراز هویت دستورات راه دور، سازمان را مطمئن می‌سازد که سیستم‌های اطلاعاتی دستورات را به شکل صحیح می‌پذیرند و اجرا می‌کنند، تنها دستورات مجاز را می‌پذیرند و دستورات غیر مجاز را کنار می‌گذارند. برای احراز هویت دستورات راه دور می‌توان از روش‌هایی مانند سازوکارهای رمزنگاری استفاده کرد. کنترل‌های مربوطه: SC-12, SC-13, SC-23.

(۱۰) حفاظت در برابر کدهای مخرب / تحلیل کدهای مخرب

سازمان:

الف. [اختصاص: شیوه‌ها و ابزارهای تعیین‌شده توسط سازمان] را برای تحلیل ویژگی‌ها و رفتار کدهای مخرب به کار می‌گیرد؛ و

ب. نتایج تحلیل کدهای مخرب را در فرایندهای پاسخ به حوادث امنیتی و برطرف کردن معایب مد نظر قرار می‌دهد.

راهنمایی‌های تکمیلی: استفاده از ابزارها و شیوه‌های مناسب تحلیل کدهای مخرب، سازمان را به درک عمیق‌تری از روش‌های مورد استفاده عوامل متخاصم و کارکرد و هدف کدهای مخرب رهنمون می‌سازد. درک ویژگی‌های کدهای مخرب نیز به نوبه خود سازمان را قادر می‌سازد تا واکنش‌های مؤثرتری نسبت به تهدیدات فعلی و بالقوه از خود نشان دهد. سازمان‌ها می‌توانند برای تحلیل کدهای مخرب از شیوه‌های مهندسی معکوس یا از پایش رفتار کدهای در حال اجرا استفاده کنند.

مراجع: نشریه ویژه شماره ۸۰۰-۸۳ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SI-3 سطح تأثیرکم	SI-3(1)(2) سطح تأثیر متوسط	SI-3(1)(2) سطح تأثیر زیاد

SI-4: پایش سیستم اطلاعاتی

کنترل: سازمان:

الف. سیستم اطلاعاتی را پایش می‌کند تا موارد زیر را شناسایی نماید:

۱. حملات و نشانه‌های حملات بالقوه بر اساس [اختصاص: اهداف پایش تعیین‌شده توسط سازمان]؛ و

۲. اتصالات محلی، شبکه و از راه دور غیر مجاز؛

ب. موارد کاربرد غیر مجاز سیستم اطلاعاتی را با استفاده از [اختصاص: شیوه‌ها و روش‌های تعیین‌شده توسط سازمان] شناسایی می‌کند؛

پ. دستگاه‌های پایش را به اشکال زیر به کار می‌گیرد:

۱. به صورت راهبردی در سیستم اطلاعاتی و به منظور جمع‌آوری اطلاعات ضروری تعیین‌شده توسط سازمان؛ و

۲. در مکان‌های موقتی در سیستم و به منظور ردیابی انواع خاصی از تراکنش‌ها با سازمان؛

ت. از اطلاعات به‌دست‌آمده از ابزارهای پایش ورود غیر مجاز درباره دسترسی، دستکاری و حذف غیر مجاز، محافظت می‌کند؛

ث. در صورتی که اطلاعات اجرایی، اطلاعات امنیتی و سایر منابع اطلاعاتی معتبر نشان دهند که خطری متوجه دارایی‌ها، افراد، سایر سازمان‌ها یا ملت است، سطح فعالیت‌های پایش سیستم اطلاعاتی را ارتقا می‌دهد؛

ج. با توجه به قوانین فدرال، دستورات اجرایی، رهنودها، خط‌مشی‌ها و مقررات، نظر قانون را درباره فعالیت‌های پایش سیستم اطلاعاتی کسب می‌نماید؛ و

چ. [اختصاص: اطلاعات تعیین‌شده توسط سازمان در زمینه پایش سیستم‌های اطلاعاتی] را [انتخاب (یک یا چند مورد): در صورت نیاز؛ [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان]] در اختیار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] قرار می‌دهد.

راهنمایی‌های تکمیلی: پایش سیستم‌های اطلاعاتی شامل پایش داخلی و خارجی است. پایش خارجی یعنی نظارت بر رویدادهایی که در مرز سیستم اطلاعاتی (یعنی بخشی از دفاع محیطی و حفاظت مرزی) رخ می‌دهند. پایش داخلی نیز شامل نظارت بر رویدادهایی است که درون سیستم اطلاعاتی به وقوع می‌پیوندند. سازمان‌ها برای پایش سیستم‌های اطلاعاتی می‌توانند فعالیت‌های ممیزی را به صورت بلادرنگ نظارت کنند یا بر سایر جنبه‌های سیستم از جمله الگوهای دسترسی، ویژگی‌های دسترسی و سایر اقدامات نظارت نمایند. اهداف پایش تعیین‌کننده رویدادهایی هستند که باید تحت نظارت قرار گیرند. قابلیت پایش سیستم‌های اطلاعاتی با استفاده از ابزارها و روش‌های مختلفی محقق می‌شود که از آن جمله می‌توان به سیستم‌های تشخیص ورود غیر مجاز، سیستم‌های جلوگیری از ورود غیر مجاز، نرم‌افزارهای حفاظت در برابر کدهای مخرب، ابزارهای اسکن، نرم‌افزارهای پایش سوابق ممیزی و نرم‌افزارهای پایش شبکه اشاره کرد. برخی مکان‌های راهبردی برای پایش دستگاه‌ها عبارتند از: مکان‌های منتخب روی محیط شبکه و مکان‌های نزدیک به سرور که از برنامه‌های کاربردی اصلی پشتیبانی می‌کنند. این دستگاه‌ها معمولاً در واسط‌های مدیریت‌شده مربوط به کنترل‌های SC-7 و AC-17 به کار گرفته می‌شوند. دستگاه‌های پایش شبکه Einstein متعلق به وزارت امنیت داخلی را نیز می‌توان در زمره دستگاه‌های پایش در نظر گرفت. دانه‌بندی پایش اطلاعات گردآوری‌شده، مبتنی بر اهداف پایش سازمان و قابلیت سیستم‌های اطلاعاتی برای پشتیبانی از این اهداف است. یکی از تراکنش‌های مورد نظر، ترافیک HTTP است که پراکسی‌های HTTP را دور می‌زند. پایش سیستم‌های اطلاعاتی بخشی از برنامه‌های پاسخ به حوادث

امنیتی و پایش مستمر سازمان است. خروجی فرایند پایش سیستم‌های اطلاعاتی، در واقع ورودی برنامه‌های پاسخ به حوادث امنیتی و پایش مستمر سازمان است. منظور از اتصال شبکه، هر نوع اتصال با دستگاهی است که ارتباطات خود را از طریق یک شبکه (مانند LAN یا اینترنت) انجام می‌دهد. منظور از اتصال راه دور، هر نوع اتصال با دستگاهی است که ارتباطات خود را از طریق یک شبکه خارجی (مانند اینترنت) انجام می‌دهد. اتصالات محلی، شبکه یا راه دور می‌توانند سیمی یا بی‌سیم باشند. کنترل‌های مربوطه: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

کنترل‌های پیشرفته:

(۱) پایش سیستم اطلاعاتی / سیستم تشخیص ورود غیر مجاز در سطح سیستم اطلاعاتی

سازمان تمام ابزارهای تشخیص ورود غیر مجاز را در قالب یک سیستم یکپارچه در سطح سیستم اطلاعاتی ترکیب و پیکربندی می‌کند.

(۲) پایش سیستم اطلاعاتی / ابزارهای خودکار برای تحلیل بلادرنگ

سازمان از ابزارهای خودکار برای پشتیبانی از تحلیل تقریباً بلادرنگ رویدادها استفاده می‌کند.

راهنمایی‌های تکمیلی: برخی ابزارهای خودکار عبارتند از: ابزارهای پایش رویداد مبتنی بر میزبان، مبتنی بر شبکه، مبتنی بر انتقال یا مبتنی بر ذخیره‌سازی، یا فناوری‌های مدیریت رویدادها و اطلاعات امنیتی (SIEM) [۲۵۹] که هشدارها و/یا نوتیفیکیشن‌های تولیدشده توسط سیستم‌های اطلاعاتی سازمان را به صورت بلادرنگ تحلیل می‌کنند.

(۳) پایش سیستم اطلاعاتی / یکپارچه‌سازی ابزارهای خودکار

سازمان با استفاده از ابزارهای خودکار، ابزارهای تشخیص ورود غیر مجاز را با سازوکارهای کنترل جریان و کنترل دسترسی ترکیب می‌کند تا در صورت رخ دادن حملات، این سازوکارها را به سرعت پیکربندی مجدد نماید و فرایندهای ایزوله‌سازی و از بین بردن حملات را به مرحله اجرا در آورد.

(۴) پایش سیستم اطلاعاتی / ترافیک ارتباطی ورودی و خروجی

سیستم اطلاعاتی ترافیک ارتباطی ورودی و خروجی را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] برای یافتن شرایط یا فعالیت‌های غیر مجاز یا غیر معمول پایش می‌کند.

راهنمایی‌های تکمیلی: به عنوان مثالی از شرایط یا فعالیت‌های غیر مجاز یا غیر معمول مربوط به ترافیک ارتباطی ورودی و خروجی، می‌توان به این موارد اشاره کرد: ترافیک داخلی که نشان‌دهنده

[259] Security Information and Event Management

وجود کدهای مخرب درون سیستم‌های اطلاعاتی سازمان یا انتشار این کدها بین مؤلفه‌های سیستم است، وارد شدن غیر مجاز اطلاعات به سیستم، یا سیگنال‌دهی به سیستم‌های اطلاعاتی خارجی. شواهد وجود کدهای مخرب برای شناسایی آن دسته از سیستم‌های اطلاعاتی یا مؤلفه‌های سیستم به کار گرفته می‌شود که احتمالاً به خطر افتاده‌اند.

(۵) پایش سیستم اطلاعاتی / هشدارهای تولیدشده توسط سیستم

هنگامی که نشانه‌های روبرو دال بر به خطر افتادن سیستم یا احتمال این امر وجود داشته باشند، سیستم اطلاعاتی به [اختصاص: کارکنان یا نقش‌های تعیین‌شده توسط سازمان] هشدار می‌دهد: [اختصاص: نشانه‌های به خطر افتادن تعیین‌شده توسط سازمان].

راهنمایی‌های تکمیلی: هشدارها ممکن است توسط منابع مختلفی تولید شوند که از آن جمله می‌توان به این موارد اشاره کرد: ورودی‌ها یا سوابق ممیزی مربوط به سازوکارهای حفاظت در برابر کدهای مخرب، سازوکارهای تشخیص یا جلوگیری از ورود غیر مجاز، یا دستگاه‌های حفاظت مرزی مانند فایروال‌ها، گیت‌وی‌ها یا مسیریاب‌ها. هشدارها می‌توانند به وسیله تلفن، ایمیل، یا پیام متنی ارسال شوند. هشدارهای برای گروه‌های مختلفی از کارکنان سازمان فرستاده می‌شوند که از میان آن‌ها می‌توان به راهبران سیستم، مالکان مأموریت و کسب‌وکار، مالکان سیستم یا مأموران امنیت سیستم اطلاعاتی اشاره کرد. کنترل‌های مربوطه: AU-5, PE-6.

(۶) پایش سیستم اطلاعاتی / محدود کردن کاربران بدون سطح دسترسی ویژه

[حذف شد: به بخش AC-6(10) منتقل شد].

(۷) پایش سیستم اطلاعاتی / پاسخ خودکار به رویدادهای مشکوک

سیستم اطلاعاتی رویدادهای مشکوک شناسایی‌شده را به [اختصاص: کارکنان تعیین‌شده توسط سازمان در زمینه پاسخ به رویدادهای امنیتی (که با نام و/یا با نقش به آن‌ها اشاره می‌شود)] اطلاع و [اختصاص: اقدامات تعیین‌شده توسط سازمان که با ایجاد کمترین اخلال در فعالیت‌ها، رویدادهای مشکوک را متوقف کنند] را انجام می‌دهد.

راهنمایی‌های تکمیلی: منظور از اقداماتی که کمترین اخلال را در فعالیت‌ها ایجاد کنند مثلاً این است که درخواستی برای ارائه پاسخ از سوی یک کاربر انسانی صورت گیرد.

(۸) پایش سیستم اطلاعاتی / حفاظت از اطلاعات پایش

[حذف شد: به بخش SI-4 انتقال داده شد].

(۹) پایش سیستم اطلاعاتی / آزمون کردن ابزارهای پایش

سازمان ابزارهای پایش ورود غیر مجاز را [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان] آزمون می‌کند.

راهنمایی‌های تکمیلی: با آزمون ابزارهای پایش ورود غیر مجاز می‌توان اطمینان حاصل کرد که این ابزارها عملکرد صحیحی دارند و اهداف سازمان در زمینه پایش ورود غیر مجاز را برآورده می‌سازند. تناوب این آزمون‌ها بستگی به نوع ابزارها و نحوه به‌کارگیری آن‌ها دارد. کنترل مربوطه: CP-9.

(۱۰) پایش سیستم اطلاعاتی / قابل مشاهده بودن ارتباطات رمزگذاری‌شده

سازمان شرایط لازم را فراهم می‌آورد تا [اختصاص: ترافیک ارتباطی رمزگذاری‌شده تعیین‌شده توسط سازمان] توسط [اختصاص: ابزارهای تعیین‌شده توسط سازمان برای پایش سیستم‌های اطلاعاتی] قابل مشاهده باشند.

راهنمایی‌های تکمیلی: سازمان‌ها بین نیاز به رمزگذاری ترافیک ارتباطی و درک این ترافیک از چشم‌انداز پایش اطلاعات، تعادل برقرار می‌کنند. برای برخی از سازمان‌ها، نیاز به حفظ محرمانگی ترافیک ارتباطی در اولویت قرار دارد و برای برخی دیگر نیز تضمین مأموریت سازمان دغدغه مهم‌تری به شمار می‌آید. سازمان تعیین می‌کند که کدام انواع ترافیک باید قابل مشاهده باشند: ترافیک رمزگذاری‌شده داخلی، ترافیک رمزگذاری‌شده برای مقاصد خارجی، یا زیرمجموعه‌ای از این انواع ترافیک.

(۱۱) پایش سیستم اطلاعاتی / تحلیل موارد غیر معمول در ترافیک ارتباطی

سازمان ترافیک ارتباطی خروجی را در مرز بیرونی سیستم اطلاعاتی و [اختصاص: نقاط داخلی درون سیستم که توسط سازمان تعیین شده‌اند (مانند زیرشبکه‌ها یا زیرسیستم‌ها)] منتخب تحلیل می‌کند تا موارد غیر معمول را شناسایی نماید.

راهنمایی‌های تکمیلی: برخی از موارد غیر معمول در سیستم‌های اطلاعاتی سازمان عبارتند از: انتقال فایل‌های بزرگ، برقراری اتصال‌ها به صورت طولانی‌مدت، استفاده شدن پورت‌ها و پروتکل‌های غیر مرسوم، و تلاش برای برقراری ارتباط با آدرس‌های مشکوک خارجی.

(۱۲) پایش سیستم اطلاعاتی / هشدارهای خودکار

سازمان با استفاده از سازوکارهای خودکار، فعالیت‌های غیر معمول یا نامناسب روبرو که تأثیرات امنیتی دارند را به کارکنان امنیتی اطلاع می‌دهد: [اختصاص: فعالیت‌های تعیین‌شده توسط سازمان که منجر به ارسال هشدار می‌شوند].

راهنمایی‌های تکمیلی: این کنترل پیشرفته بر آن دسته از هشدارهایی تمرکز دارد که توسط سازمان تولید می‌شوند و با استفاده از ابزارهای خودکار ارسال می‌گردند. بر خلاف هشدارهای تولیدشده توسط سیستم‌های اطلاعاتی که در بخش SI-4(5) به آن‌ها اشاره شد (و تمرکز آن‌ها بر منابع اطلاعاتی داخلی سیستم از جمله سوابق ممیزی بود)، منابع اطلاعات این کنترل پیشرفته می‌توانند از سایر موجودیت‌ها نیز نشأت گیرند (مانند گزارش فعالیت‌های مشکوک و گزارشات مربوط به تهدیدات داخلی بالقوه). کنترل‌های مربوطه: AC-18, IA-3.

(۱۳) پایش سیستم اطلاعاتی / تحلیل الگوهای رویدادها و ترافیک

سازمان:

الف. الگوهای رویدادها و ترافیک ارتباطی سیستم اطلاعاتی را تحلیل می‌کند؛

ب. پروفایل‌هایی را تهیه می‌کند که نشان‌دهنده الگوهای معمول ترافیک و/یا رویدادها هستند؛ و

پ. از پروفایل‌های ترافیک و رویدادها برای تنظیم دستگاه‌های پایش سیستم استفاده می‌کند تا تعداد موارد تشخیص نادرست را کاهش دهد.

(۱۴) پایش سیستم اطلاعاتی / تشخیص ورود غیر مجاز بی‌سیم

سازمان با استفاده از یک سیستم تشخیص ورود غیر مجاز بی‌سیم، دستگاه‌های بی‌سیم بدخواه که در پی حمله به سیستم اطلاعاتی یا به خطر انداختن آن هستند را شناسایی می‌کند.

راهنمایی‌های تکمیلی: سیگنال‌های بی‌سیم ممکن است در خارج از محدوده تأسیسات کنترل‌شده توسط سازمان نیز منتشر شوند. سازمان‌ها تمام نقاط دسترسی بی‌سیم غیر مجاز را به دقت بررسی می‌کنند تا اتصالات بی‌سیم غیر مجاز را شناسایی نمایند. این بررسی‌ها تنها در مناطقی انجام نمی‌شوند که سیستم‌های اطلاعاتی در آن‌ها قرار گرفته‌اند؛ بلکه در صورت نیاز نواحی خارج از این مناطق را نیز شامل می‌شوند. هدف سازمان این است که تأیید کند اتصال بی‌سیم غیر مجازی برقرار نشده است. کنترل‌های مربوطه: AC-18, IA-3.

(۱۵) پایش سیستم اطلاعاتی / ارتباطات شبکه‌های بی‌سیم به شبکه‌های سیمی

سازمان ترافیک ارتباطی بی‌سیم را در هنگام انتقال از شبکه‌های بی‌سیم به شبکه‌های سیمی، توسط یک سیستم تشخیص ورود غیر مجاز پایش می‌کند.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: AC-18.

(۱۶) پایش سیستم اطلاعاتی / ترکیب کردن اطلاعات پایش

سازمان اطلاعات به‌دست‌آمده از ابزارهای پایش که در نقاط مختلف سیستم اطلاعاتی به کار گرفته شده‌اند را با یکدیگر ترکیب می‌نماید.

راهنمایی‌های تکمیلی: ترکیب کردن اطلاعات به‌دست‌آمده از ابزارهای پایش مختلف می‌تواند چشم‌انداز جامع‌تری از فعالیت‌های سیستم اطلاعاتی ارائه نماید. بدین ترتیب، چشم‌اندازی از سراسر سازمان در دست خواهد بود که می‌تواند الگوهای حمله‌ای که در غیر این صورت دیده نمی‌شوند را مشهود سازد. درک قابلیت‌ها و محدودیت‌های ابزارهای پایش مختلف و چگونگی استفاده بهینه از اطلاعات گردآوری‌شده توسط این ابزارها، سازمان‌ها را یاری می‌کند تا برنامه‌های پایش مؤثری را تهیه، اجرا و حفظ کنند. کنترل مربوطه: AU-6.

(۱۷) پایش سیستم اطلاعاتی / آگاهی یکپارچه از شرایط

سازمان اطلاعات به‌دست‌آمده از فعالیت‌های فیزیکی، سایبری و زنجیره تأمین را کنار هم قرار می‌دهد تا به یک آگاهی یکپارچه از شرایط سراسر سازمان دست یابد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته اطلاعات پایش به‌دست‌آمده از منابع اطلاعاتی مختلف را با هم ترکیب می‌کند تا به یک آگاهی یکپارچه از شرایط سراسر سازمان دست یابد. این آگاهی از شرایط، سازمان را قادر می‌سازد تا حملات سایبری پیشرفته را به سرعت شناسایی کند و روش‌ها و شیوه‌های انجام این حملات را بررسی نماید. بر خلاف کنترل امنیتی SI-4(16) که اطلاعات پلیش مختلف را با هم ترکیب می‌کند، این کنترل پیشرفته اطلاعات مربوط به دامنه‌هایی فراتر از دامنه‌های سایبری را نیز در کنار هم قرار می‌دهد. بدین ترتیب، سازمان قادر خواهد بود حملاتی را شناسایی کند که بردارهای حمله مختلف را شامل می‌شوند. کنترل مربوطه: SA-12.

(۱۸) پایش سیستم اطلاعاتی / تحلیل ترافیک و خروج مخفیانه اطلاعات از سیستم

سازمان ترافیک ارتباطی خروجی را در مرز خارجی سیستم اطلاعاتی (یعنی محیط سیستم) و همچنین در [اختصاص: نقاط تعیین‌شده توسط سازمان در داخل سیستم (مانند زیرسیستم‌ها و زیرشبکه‌ها)] تحلیل می‌کند تا خروج مخفیانه اطلاعات را شناسایی نماید.

راهنمایی‌های تکمیلی: منظور از خروج مخفیانه اطلاعات، مواردی است که می‌توانند منجر به خروج غیر مجاز اطلاعات از سازمان شوند. به عنوان مثال، می‌توان به پنهان‌نگاری اشاره کرد.

(۱۹) پایش سیستم اطلاعاتی / افرادی که مخاطرات بالاتری را برای سازمان دارند

سازمان فعالیت‌های آن دسته از افرادی که بر اساس یافته‌های [اختصاص: منابع تعیین‌شده توسط سازمان]، مخاطرات بالاتری دارند را با استفاده از [اختصاص: اقدامات اضافه پایش تعیین‌شده توسط سازمان] بررسی می‌کند.

راهنمایی‌های تکمیلی: نشانه‌های وجود مخاطرات بیشتر از سوی برخی افراد خاص را می‌توان از منابع مختلفی به دست آورد که از آن جمله می‌توان به سوابق منابع انسانی، نهادهای امنیتی، سازمان‌های مجری قانون و/یا سایر منابع معتبر اشاره کرد. فرایندهای پایش فعالیت‌های افراد به دقت با مقامات مدیریتی، قانونی، امنیتی و منابع انسانی هماهنگ می‌شود و مطابق با قوانین فدرال، دستورات اجرایی، خط‌مشی‌ها، رهنمودها، مقررات و استانداردها صورت می‌گیرد.

(۲۰) پایش سیستم اطلاعاتی / کاربران دارای سطح دسترسی ویژه

سازمان فعالیت‌های کاربران دارای سطح دسترسی ویژه را با استفاده از [اختصاص: اقدامات اضافه پایش تعیین‌شده توسط سازمان] بررسی می‌کند.

(۲۱) پایش سیستم اطلاعاتی / دوره آزمایشی

سازمان فعالیت‌های افراد را در [اختصاص: دوره آزمایشی تعیین‌شده توسط سازمان] با استفاده از [اختصاص: اقدامات اضافه پایش تعیین‌شده توسط سازمان] بررسی می‌کند.

(۲۲) پایش سیستم اطلاعاتی / خدمات غیر مجاز شبکه

سیستم اطلاعاتی آن دسته از خدمات شبکه که توسط [اختصاص: فرایندهای تأیید یا صدور مجوز تعیین‌شده توسط سازمان] تأیید نشده‌اند را شناسایی می‌کند و [انتخاب (یک یا چند مورد): اقدامات ممیزی مربوطه را انجام می‌دهد؛ مراتب را به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] اطلاع می‌دهد].

راهنمایی‌های تکمیلی: فعالیت‌های غیر مجاز شبکه مواردی از جمله خدمات ارائه‌شده در معماری‌های خدمت‌گرا را در بر می‌گیرند که دارای تأییدیه سازمانی نیستند و در نتیجه، قابل اعتماد نیستند و می‌توانند به خدمات معتبر نیز آسیب برسانند. کنترل‌های مربوطه: AC-6, CM-7, SA-5, SA-9.

(۲۳) پایش سیستم اطلاعاتی / دستگاه‌های مبتنی بر میزبان

سازمان [اختصاص: سازوکارهای پایش مبتنی بر میزبان تعیین‌شده توسط سازمان] را در [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان] پیاده‌سازی می‌کند.

راهنمایی‌های تکمیلی: از جمله مؤلفه‌های سیستم اطلاعاتی که می‌توان سازوکارهای پایش مبتنی بر میزبان را در آن‌ها پیاده‌سازی کرد عبارتند از: سرورها، ایستگاه‌های کاری و دستگاه‌های همراه. سازمان‌ها این سازوکارها را از تأمین‌کنندگان IT مختلف تهیه می‌کنند.

(۲۴) پایش سیستم اطلاعاتی / نشانه‌های به خطر افتادن سیستم

سیستم اطلاعاتی نشانه‌های به خطر افتادن سیستم را شناسایی، گردآوری، توزیع و استفاده می‌کند.

راهنمایی‌های تکمیلی: نشانه‌های به خطر افتادن (IOC) در واقع عوامل جرم‌شناسی دال بر ورود به سیستم هستند که در سیستم‌های اطلاعاتی سازمان (در سطح میزبان یا در سطح شبکه) شناسایی می‌شوند. این نشانه‌ها اطلاعات ارزشمندی را در اختیار سازمان قرار می‌دهند و بیان می‌کنند که کدام موجودیت‌های غیر فعال یا سیستم‌های اطلاعاتی در معرض خطر قرار گرفته‌اند. به عنوان مثالی از یک IOC که برای شناسایی میزبان‌های به‌خطرافتاده به کار گرفته می‌شود، می‌توان به تولید مقادیر کلید ثبت اشاره کرد. IOCهای مربوط به ترافیک شبکه نیز URL یا عناصر پروتکلی هستند که وجود دستورات بدافزار یا سرورهای کنترل را نشان می‌دهند. توزیع و به‌کارگیری سریع IOCها می‌تواند امنیت سیستم‌های اطلاعاتی را ارتقا دهد، زیرا زمان قرار داشتن سیستم‌های اطلاعاتی یا سازمان در معرض یک اکسپلویت یا حمله را کم می‌کند.

مراجع: نشریه‌های ویژه شماره ۸۰۰-۶۱، ۸۰۰-۸۳، ۸۰۰-۹۲، ۸۰۰-۹۴ و ۸۰۰-۱۳۷ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SI-4 سطح تأثیرکم	SI-4(2)(4)(5) سطح تأثیر متوسط	SI-4(2)(4)(5) سطح تأثیر زیاد

SI-5: هشدارها، مشاوره‌ها و رهنمودهای امنیتی

کنترل: سازمان:

الف. هشدارها، مشاوره‌ها و رهنمودهای امنیتی مربوط به سیستم اطلاعاتی را به طور منظم از [اختصاص: سازمان‌های خارجی تعیین‌شده توسط سازمان] دریافت می‌کند؛

ب. در صورت لزوم، هشدارها، مشاوره‌ها و رهنمودهای امنیتی داخلی را تولید می‌کند؛

پ. هشدارها، مشاوره‌ها و رهنمودهای امنیتی را در اختیار این افراد و نهادها قرار می‌دهد: [انتخاب (یک یا چند مورد): [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان]؛ [اختصاص: عناصر درون‌سازمانی تعیین‌شده توسط سازمان]؛ [اختصاص: سازمان‌های خارجی تعیین‌شده توسط سازمان]]؛ و

ت. رهنمودهای امنیتی را بر اساس چارچوب تعیین‌شده اجرا می‌کند یا سازمان صادرکننده این رهنمودها را در جریان میزان عدم انطباق با این چارچوب قرار می‌دهد.

راهنمایی‌های تکمیلی: US-CERT مشاوره‌ها و هشدارهای امنیتی را ارائه می‌نماید تا آگاهی از شرایط در سراسر دولت فدرال را تأمین کند. رهنمودهای امنیتی توسط OMB یا سایر سازمان‌های مجاز صادر می‌شوند. به دلیل ماهیت حساس رهنمودهای امنیتی و خسارت‌های وارده به دارایی‌ها و عملیات سازمان، افراد، سایر سازمان‌ها و ملت در صورت عدم پیاده‌سازی به‌هنگام آن‌ها، تبعیت از این رهنمودها کاملاً ضروری است. برخی سازمان‌های خارجی عبارتند از شرکای تجاری خارجی، شرکای زنجیره تأمین، تأمین‌کنندگان خدمات خارجی و سایر سازمان‌های همتا یا پشتیبان. کنترل مربوطه: SI-2.

کنترل‌های پیشرفته:

(۱) هشدارها، مشاوره‌ها و رهنمودهای امنیتی / مشاوره‌ها و هشدارهای خودکار

سازمان با استفاده از سازوکارهای خودکار، مشاوره‌ها و هشدارهای امنیتی را در سراسر سازمان تأمین و ارائه می‌نماید.

راهنمایی‌های تکمیلی: تغییرات زیادی که در سیستم‌های اطلاعاتی سازمان و محیط‌های عملیاتی آن‌ها رخ می‌دهند، توزیع اطلاعات امنیتی بین موجودیت‌های سازمانی مختلف و ذی‌نفع در مأموریت‌ها و کارکردهای کسب‌وکار سازمان را ضروری می‌سازد. بر اساس اطلاعات ارائه‌شده توسط مشاوره‌ها و هشدارهای امنیتی، ممکن است لازم باشد که تغییراتی در یک یا چند مورد از سه مرحله مدیریت مخاطرات امنیت اطلاعات صورت گیرد. این سه مرحله عبارتند از: سطح مدیریت و وضع قوانین؛ سطح معماری سازمان، فرایند کسب‌وکار و مأموریت؛ و سطح سیستم اطلاعاتی.

مراجع: نشریه ویژه شماره ۴۰-۸۰۰ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	SI-5 سطح تأثیرکم	SI-5 سطح تأثیر متوسط	SI-5(1) سطح تأثیر زیاد

SI-6: تأیید کارکرد امنیتی

کنترل: سیستم اطلاعاتی:

الف. عملکرد صحیح [اختصاص: کارکردهای امنیتی تعیین‌شده توسط سازمان] را تأیید می‌کند؛

ب. این تأیید را [انتخاب (یک یا چند مورد): [اختصاص: در حالت‌های انتقالی تعیین‌شده توسط سازمان]؛ در صورت دستور توسط کاربر دارای سطح دسترسی مناسب؛ [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان]] اجرا می‌کند؛

پ. در صورت منفی بودن نتیجه آزمون‌های تأیید امنیت، مراتب را به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] اطلاع می‌دهد؛

ت. در صورت مشاهده موارد غیر معمول، [انتخاب (یک یا چند مورد): سیستم اطلاعاتی را خاموش می‌کند؛ سیستم اطلاعاتی را راه‌اندازی مجدد می‌کند؛ [اختصاص: اقدامات دیگر تعیین‌شده توسط سازمان]].

راهنمایی‌های تکمیلی: برخی حالت‌های انتقالی برای سیستم‌های اطلاعاتی عبارتند از: راه‌اندازی سیستم، راه‌اندازی مجدد سیستم، خاموش کردن سیستم و توقف عملیات سیستم. برخی نوتیفیکیشن‌های ارائه‌شده توسط سیستم اطلاعاتی عبارتند از: هشدارهای الکترونیک به راهبران سیستم، پیام به کنسول‌های رایانه‌ای محلی، و/یا نشانه‌های سخت‌افزاری مانند چراغ. کنترل‌های مربوطه: CA-7, CM-6.

کنترل‌های پیشرفته:

(۱) تأیید کارکرد امنیتی / نوتیفیکیشن نتیجه منفی آزمون امنیتی
[حذف شد: به بخش SI-6 منتقل شد].

(۲) تأیید کارکرد امنیتی / پشتیبانی خودکار از آزمون‌های توزیع‌شده
سیستم اطلاعاتی سازوکارهای خودکار را برای پشتیبانی از مدیریت آزمون‌های امنیتی توزیع‌شده به کار می‌گیرد.
راهنمایی‌های تکمیلی: کنترل مربوطه: SI-2.

(۳) تأیید کارکرد امنیتی / گزارش‌دهی نتایج تأیید

سازمان نتایج تأیید کارکردهای امنیتی را به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] گزارش می‌دهد.

راهنمایی‌های تکمیلی: برخی کارکنان سازمان که ممکن است نتایج تأیید کارکردهای امنیتی را دریافت کنند عبارتند از: مسئولان ارشد امنیت اطلاعات، مدیران امنیت سیستم‌های اطلاعاتی و مسئولان امنیتی سیستم‌های اطلاعاتی. کنترل‌های مربوطه: SA-12, SI-4, SI-5.

مراجع: وجود ندارد.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، سطح تأثیرکم	انتخاب نشده، سطح تأثیر متوسط	SI-6 سطح تأثیر زیاد

SI-7: یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات

کنترل: سازمان با استفاده از ابزارهای تأیید یکپارچگی، تغییرات غیر مجاز در [اختصاص: نرم‌افزارها، ثابت‌افزارها و اطلاعات تعیین‌شده توسط سازمان] را شناسایی می‌کند.

راهنمایی‌های تکمیلی: تغییرات غیر مجاز در نرم‌افزارها، ثابت‌افزارها و اطلاعات به دلیل خطاها یا اقدامات بدخواهانه روی می‌دهند. منظور از نرم‌افزارها، مواردی از جمله سیستم‌عامل‌ها (با مؤلفه‌های کلیدی از جمله کرنل‌ها و درایورها)، میان‌افزارها و برنامه‌های کاربردی است. ثابت‌افزارها نیز مواردی از جمله BIOS را در بر می‌گیرند. اطلاعات شامل مواردی از جمله ابرداده‌ها است که به نوبه خود داده‌هایی از قبیل ویژگی‌های امنیتی اطلاعات را شامل می‌شود. سازوکارهای بررسی یکپارچگی و ابزارهای مربوطه می‌توانند یکپارچگی سیستم‌های اطلاعاتی و برنامه‌های کاربردی میزبانی‌شده را به صورت خودکار پایش کنند. کنترل‌های مربوطه: SA-12, SC-8, SC-13, SI-3.

کنترل‌های پیشرفته:

(۱) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / بررسی یکپارچگی

سیستم اطلاعاتی یکپارچگی [اختصاص: نرم‌افزارها، ثابت‌افزارها و اطلاعات تعیین‌شده توسط سازمان] را [انتخاب (یک یا چند مورد): در هنگام راه‌اندازی سیستم؛ در [اختصاص: حالت‌های انتقالی یا رویدادهای

امنیتی تعیین‌شده توسط سازمان]؛ [اختصاص: در بازه‌های زمانی تعیین‌شده توسط سازمان]] بررسی می‌کند.

راهنمایی‌های تکمیلی: منظور از رویداد امنیتی، شناسایی تهدید جدیدی که سیستم‌های اطلاعاتی سازمان در معرض خطر آن قرار دارند، و سپس نصب سخت‌افزارها، ثابت‌افزارها یا نرم‌افزارهای جدید است. برخی حالت‌های انتقالی برای سیستم‌های اطلاعاتی عبارتند از: راه‌اندازی سیستم، راه‌اندازی مجدد سیستم، خاموش کردن سیستم و توقف عملیات سیستم.

(۲) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / نوتیفیکیشن خودکار در صورت نقض یکپارچگی

سازمان در صورت مشاهده موارد نقض یکپارچگی، نوتیفیکشن‌هایی را با استفاده از ابزارهای خودکار به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] ارائه می‌نماید.

راهنمایی‌های تکمیلی: استفاده از ابزارهای خودکار برای گزارش دادن به‌هنگام موارد نقض یکپارچگی به کارکنان سازمان، یکی از اجزای اصلی یک برنامه مؤثر پاسخگویی به مخاطرات به شمار می آید. برخی از کارکنانی که چنین مواردی به آن‌ها گزارش می‌شود عبارتند از: مالکان مأموریت و کسب‌وکار، مالکان سیستم اطلاعاتی، راهبران سیستم، توسعه‌دهندگان نرم‌افزار، یکپارچه‌سازان سیستم و مسئولان امنیت اطلاعات.

(۳) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / ابزارهای یکپارچه‌سازی با مدیریت مرکزی

سازمان از ابزارهای تأیید یکپارچگی با مدیریت مرکزی استفاده می‌کند.

راهنمایی‌های تکمیلی: کنترل‌های مربوطه: AU-3, SI-2, SI-8.

(۴) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / بسته‌بندی جلوگیری از دستکاری

[حذف شد: به بخش SA-12 منتقل شد].

(۵) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / پاسخ خودکار به موارد نقض یکپارچگی

در صورت مشاهده موارد نقض یکپارچگی، سیستم اطلاعاتی به صورت خودکار [انتخاب (یک یا چند مورد): سیستم اطلاعاتی را خاموش می‌کند؛ سیستم اطلاعاتی را راه‌اندازی مجدد می‌کند؛ [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] را پیاده‌سازی می‌کند].

راهنمایی‌های تکمیلی: سازمان‌ها ممکن است انواع مختلفی از بررسی یکپارچگی و پاسخ به موارد غیر معمول را انجام دهند: (۱) بر اساس نوع اطلاعات (مثلاً داده‌های کاربر، نرم‌افزار یا ثابت‌افزار)؛ (۲) بر اساس اطلاعات خاص (مثلاً ثابت‌افزار بوت یا نرم‌افزار بوت برای انواع خاصی از ماشین‌ها)؛ یا (۳) ترکیبی از این دو مورد. پیاده‌سازی خودکار برخی ابزارهای امنیتی درون سیستم اطلاعاتی سازمان نیز مواردی

از این دست را در بر می‌گیرد: برعکس کردن تغییرات، متوقف کردن عملیات سیستم اطلاعاتی، یا ارسال هشدارهای ممیزی در صورتی که دستکاری‌های غیر مجازی در فایل‌های امنیتی حساس صورت گرفته باشد.

(۶) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / حفاظت رمزنگاری

سیستم اطلاعاتی برای شناسایی تغییرات غیر مجاز در نرم‌افزارها، ثابت‌افزارها یا اطلاعات، از سازوکارهای رمزنگاری استفاده می‌کند.

راهنمایی‌های تکمیلی: برخی سازوکارهای رمزنگاری برای حفاظت از یکپارچگی عبارتند از: امضاهای دیجیتال و محاسبه و اجرای هش‌های امضاشده با استفاده از رمزنگاری نامتقارن، حفاظت از محرمانگی کلید مورد استفاده برای تولید هش، و استفاده از کلید عمومی برای تأیید اطلاعات هش. کنترل مربوطه: SC-13.

(۷) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / یکپارچگی شناسایی و پاسخ

سازمان قابلیت شناسایی [اختصاص: تغییرات امنیتی در سیستم اطلاعاتی بنا به تعریف سازمان] غیر مجاز را با قابلیت پاسخ به حوادث امنیتی ترکیب می‌کند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته سازمان را یاری می‌کند تا اطمینان حاصل نماید که رویدادهای شناسایی‌شده به شکل صحیح ردیابی، پایش و اصلاح شده‌اند و امکان ثبت آن‌ها برای مصارف آینده وجود دارد. حفظ سوابق تاریخی سازمان را قادر می‌سازد تا اقدامات عوامل متخاصم در یک بازه زمانی را شناسایی کند و در صورت لزوم اقدامات قانونی مقتضی را صورت دهد. برخی تغییرات امنیتی عبارتند از: تغییر غیر مجاز تنظیمات پیکربندی یا حذف غیر مجاز سطوح دسترسی ویژه به سیستم اطلاعاتی. کنترل‌های مربوطه: IR-4, IR-5, SI-4.

(۸) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / قابلیت ممیزی برای رویدادهای مهم

در صورت مشاهده مواد نقض یکپارچگی، سیستم اطلاعاتی قابلیت ممیزی این رویداد را فراهم می‌آورد و اقدامات روبرو را شروع می‌کند: [انتخاب (یک یا چند مورد): سوابق ممیزی را تولید می‌کند؛ به کاربر فعلی هشدار می‌دهد؛ به [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] هشدار می‌دهد؛ [اختصاص: سایر اقدامات تعیین‌شده توسط سازمان]].

راهنمایی‌های تکمیلی: سازمان نوع اقدام پاسخ را بر اساس نوع نرم‌افزار، نرم‌افزار خاص یا اطلاعاتی تعیین می‌کند که موارد نقض یکپارچگی در مورد آن‌ها رخ داده‌اند. کنترل‌های مربوطه: AU-2, AU-6, AU-12.

(۹) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / تأیید فرایند بوت

سیستم اطلاعاتی یکپارچگی فرایند بوت [اختصاص: دستگاه‌های تعیین‌شده توسط سازمان] را تأیید می‌کند.

راهنمایی‌های تکمیلی: حصول اطمینان از یکپارچگی فرایند بوت، برای آغاز به کار دستگاه در یک حالت معلوم یا قابل اعتماد اهمیت زیادی دارد. سازوکارهای تأیید یکپارچگی به کارکنان سازمان تضمین می‌دهند که در جریان فرایند بوت، تنها کدهای مورد اعتماد اجرا شده‌اند.

(۱۰) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / حفاظت از ثابت‌افزار بوت

سیستم اطلاعاتی [اختصاص: ابزارهای امنیتی تعیین‌شده توسط سازمان] را پیاده‌سازی می‌کند تا از یکپارچگی ثابت‌افزار بوت در [اختصاص: دستگاه‌های تعیین‌شده توسط سازمان] اطمینان حاصل نماید.

راهنمایی‌های تکمیلی: تغییرات غیر مجاز در ثابت‌افزار بوت می‌توانند آغازگر حملات سایبری پیشرفته و هدفمند باشند. این نوع حملات سایبری می‌توانند سبب شوند که خدمات به صورت مستمر از دسترس خارج گردند (مثلاً اگر ثابت‌افزار از کار افتاده باشد) یا کدهای مخرب به صورت پیوسته در سیستم وجود داشته باشند (مثلاً اگر کد مخرب درون ثابت‌افزار تعبیه شده باشد). دستگاه‌ها می‌توانند به روش‌های روبرو از یکپارچگی ثابت‌افزار بوت در سیستم‌های اطلاعاتی سازمان حفاظت کنند: (۱) تأیید یکپارچگی و اعتبار تمام به‌روزرسانی‌های ثابت‌افزار بوت پیش از اعمال تغییرات در دستگاه بوت؛ و (۲) جلوگیری از دستکاری ثابت‌افزار بوت توسط فرایندهای غیر مجاز.

(۱۱) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / محیط‌های محدود با سطح دسترسی محدود

سازمان لازم می‌دارد که [اختصاص: نرم‌افزارهای تعیین‌شده توسط سازمان که توسط کاربر نصب شده‌اند] در یک محیط فیزیکی یا یک محیط ماشین مجازی محدود با سطح دسترسی محدود اجرا شوند.

راهنمایی‌های تکمیلی: سازمان‌ها تعیین می‌کنند که کدام نرم‌افزارها بیشتر از بقیه در معرض کدهای مخرب قرار دارند یا احتمال وجود کدهای مخرب در آن‌ها بیشتر است. در مورد این دسته از نرم‌افزارها، نصب به‌روزرسانی‌ها توسط کاربر در یک محیط عملیاتی محدود صورت می‌گیرد تا خسارت‌های احتمالی ناشی از اجرای کدهای مخرب به کمترین حد برسد.

(۱۲) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / تأیید یکپارچگی

سازمان لازم می‌دارد که یکپارچگی [اختصاص: نرم‌افزارهای تعیین‌شده توسط سازمان] پیش از اجرا، تأیید شود.

راهنمایی‌های تکمیلی: سازمان‌ها یکپارچگی نرم‌افزارهای نصب‌شده توسط کاربر را پیش از اجرا تأیید می‌کنند تا احتمال اجرای کدهای مخرب یا کدهای شامل خطاهای ناشی از دستکاری‌های غیر مجاز را کاهش دهند. سازمان‌ها برای این کار از روش‌های مختلفی استفاده می‌کنند. به عنوان مثال، آیتم‌های محصولات سازندگان یا ارائه‌دهندگان نرم‌افزارها را بررسی می‌کنند تا تأیید نمایند که آیا این محصولات قابل اعتماد هستند یا خیر.

(۱۳) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / اجرای کد در محیط‌های حفاظت‌شده

سازمان اجازه اجرای کدهای باینری یا قابل اجرا توسط ماشین که از منابع نه چندان مورد اعتماد به دست آمده‌اند را تنها در محیط‌های فیزیکی یا محیط‌های ماشین مجازی محدود و با تأیید آشکار [اختصاص: نقش‌ها یا کارکنان تعیین‌شده توسط سازمان] صادر می‌نماید.

راهنمایی‌های تکمیلی: این کنترل پیشرفته در مورد تمام منابع کدهای باینری یا قابل اجرا توسط ماشین از جمله ثابت‌افزارها و نرم‌افزارهای تجاری و نرم‌افزارهای کدباز اعمال می‌شود.

(۱۴) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / کدهای باینری یا قابل اجرا توسط ماشین سازمان:

الف. استفاده از کدهای باینری یا قابل اجرا توسط ماشین که چندان قابل اعتماد نیستند و کدهای مرجع آن‌ها ارائه نشده است را منع می‌کند؛ و

ب. تنها در مورد الزامات مهم عملیات یا کسب‌وکار و آن هم با تأیید مقام مربوطه، استثنائاتی را برای الزامات کد مرجع در نظر می‌گیرد.

راهنمایی‌های تکمیلی: این کنترل پیشرفته در مورد تمام منابع کدهای باینری یا قابل اجرا توسط ماشین از جمله ثابت‌افزارها و نرم‌افزارهای تجاری و نرم‌افزارهای کدباز اعمال می‌شود. سازمان محصولات نرم‌افزاری بدون کد مرجع که از منابع نه چندان مورد اعتماد تأمین شده‌اند را بررسی می‌کند تا اطمینان حاصل نماید که تأثیر امنیتی منفی ندارند. در این بررسی‌ها در نظر گرفته می‌شود که بازبینی، تعمیر یا توسعه این نوع محصولات نرم‌افزاری می‌تواند بسیار دشوار باشد، زیرا سازمان‌ها در اکثر موارد به کد مرجع دسترسی ندارند و ممکن است مالکی نیز وجود نداشته باشد که تعمیرات مذکور را از سوی سازمان انجام دهد. کنترل مربوطه: SA-5.

(۱۵) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / احراز هویت کد

سیستم اطلاعاتی سازوکارهای رمزنگاری را به کار می‌گیرد تا پیش از نصب [اختصاص: مؤلفه‌های سیستم اطلاعاتی تعیین‌شده توسط سازمان]، آن‌ها را احراز هویت کند.

راهنمایی‌های تکمیلی: برای احراز هویت رمزنگاری، سازمان می‌تواند تأیید کند که مؤلفه‌های ثابت‌افزار و نرم‌افزار با استفاده از گواهی‌های مورد تأیید سازمان امضا شده‌اند. امضای کد یکی از روش‌های مؤثر برای حفاظت در برابر کدهای مخرب است.

(۱۶) یکپارچگی نرم‌افزارها، ثابت‌افزارها و اطلاعات / محدودیت زمانی برای اجرای بدون نظارت فرایندها

سازمان اجازه نمی‌دهد که فرایندهای به صورت بدون مجوز برای مدت‌زمانی بیشتر از [اختصاص: مدت‌زمان تعیین‌شده توسط سازمان] اجرا شوند.

راهنمایی‌های تکمیلی: این کنترل پیشرفته به فرایندهایی می‌پردازد که مدت زمان عادی اجرای آن‌ها را می‌توان تعیین کرد و همچنین شرایطی را پوشش می‌دهد که سازمان‌ها از این مدت مان تعیین‌شده فراتر روند. نظارت به اشکال مختلف انجام می‌شود که از آن جمله می‌توان به استفاده از تایمر سیستم‌عامل، پاسخ‌های خودکار یا نظارت و پاسخ دستی در صورت رخ دادن موارد غیر عادی در فرایندهای سیستم اطلاعاتی اشاره کرد.

مراجع: نشریه‌های ویژه شماره ۸۰۰-۱۴۷ و ۸۰۰-۱۵۵ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P1	انتخاب نشده، سطح تأثیرکم	SI-7(1)(7) سطح تأثیر متوسط	SI-7(1)(2)(5)(7)(14) سطح تأثیر زیاد

SI-8: حفاظت در برابر هرزنامه‌ها[۲۶۰]

کنترل: سازمان:

الف. در نقاط ورودی و خروجی سیستم اطلاعاتی از سازوکارهای حفاظت در برابر هرزنامه‌ها استفاده می‌کند تا پیام‌های ناخواسته را شناسایی کند و اقدامات لازم را در خصوص آن‌ها انجام دهد؛ و

ب. در صورت ارائه شدن به‌روزرسانی‌های جدیدی از سازوکارهای حفاظت در برابر هرزنامه‌ها، این سازوکارها را بر اساس رویه‌ها و خط‌مشی مدیریت پیکربندی سازمان به‌روز می‌نماید.

[260] spam

راهنمایی‌های تکمیلی: نقاط ورودی و خروجی سیستم اطلاعاتی شامل فایروال‌ها، سرورهای ایمیل، سرورهای وب، سرورهای پراکسی، سرورهای دسترسی از راه دور، ایستگاه‌های کاری، دستگاه‌های همراه، لپتاپ‌ها و مواردی از این دست هستند. هرزنامه‌ها به طرق مختلف منتشر می‌شوند که از آن جمله می‌توان به ایمیل‌ها، پیوست‌های ایمیل‌ها و دسترسی‌های وب اشاره کرد. سازوکارهای حفاظت در برابر هرزنامه‌ها شامل مواردی از جمله تعیین امضا هستند. کنترل‌های مربوطه: AT-2, AT-3, SC-5, SC-7, SI-3.

کنترل‌های پیشرفته:

(۱) حفاظت در برابر هرزنامه‌ها / مدیریت مرکزی

سازمان سازوکارهای حفاظت در برابر هرزنامه‌ها را به صورت مرکزی مدیریت می‌کند.

راهنمایی‌های تکمیلی: مدیریت مرکزی یعنی مدیریت و پیاده‌سازی سازوکارهای حفاظت در برابر هرزنامه‌ها در سطح سازمان. مدیریت مرکزی شامل برنامه‌ریزی، پیاده‌سازی، بررسی، صدور مجوز و پایش کنترل‌های امنیتی حفاظت در برابر هرزنامه‌ها است که توسط سازمان تعیین و به صورت مرکزی مدیریت می‌شوند. کنترل‌های مربوطه: AU-3, SI-2, SI-7.

(۲) حفاظت در برابر هرزنامه‌ها / به‌روزرسانی‌های خودکار

سیستم اطلاعاتی سازوکارهای حفاظت در برابر هرزنامه‌ها را به صورت خودکار به‌روزرسانی می‌کند.

(۳) حفاظت در برابر هرزنامه‌ها / قابلیت یادگیری مستمر

سیستم اطلاعاتی سازوکارهای حفاظت در برابر هرزنامه‌ها را با قابلیت یادگیری پیاده‌سازی می‌کند تا بتوانند ترافیک ارتباطی مجاز را به خوبی شناسایی نمایند.

راهنمایی‌های تکمیلی: مثالی از سازوکارهای یادگیری، فیلترهای بیزی هستند[۲۶۱] که ورودی‌های کاربر در خصوص تفکیک ترافیک قانونی و هرزنامه را مبنای پاسخ‌های خود قرار می‌دهند. پارامترهای الگوریتم این فیلترها به‌روز می‌شود تا ترافیک را به شکل دقیق‌تری از هم جدا کنند.

مراجع: نشریه ویژه شماره ۸۰۰-۴۵ سازمان NIST.

اولویت و تخصیص به مجموعه‌های پایه:

P2	انتخاب نشده، سطح تأثیرکم	SI-8(1)(2) سطح تأثیر متوسط	SI-8(1)(2) سطح تأثیر زیاد

[261] Bayesian filters

SI-9: محدودیت‌های ورودی اطلاعات

[حذف شد: به بخش‌های AC-2، AC-3، AC-5 و AC-6 منتقل شد].

SI-10: تأیید ورودی اطلاعاتی

کنترل: سیستم اطلاعاتی اعتبار [اختصاص: مدت‌زمان تعیین‌شده توسط سازمان] را بررسی می‌کند.

راهنمایی‌های تکمیلی: سازمان با بررسی ساختار ورودی‌های سیستم اطلاعاتی (مانند مجموعه کاراکترها، طول، محدوده عددی و مقادیر قابل قبول)، تأیید می‌کند که ورودی‌ها منطبق با فرمت و محتوای تعیین‌شده هستند. برنامه‌های کاربردی نرم‌افزاری معمولاً از پروتکل‌های تعریف‌شده‌ای تبعیت می‌کنند که از پیام‌های ساختارمندی (یعنی دستورات و کوئری‌ها) برای برقراری ارتباط بین ماژول‌های نرم‌افزاری یا مؤلفه‌های سیستم استفاده می‌نمایند. پیام‌های ساختارمند می‌توانند دربردارنده داده‌های غیر ساختاریافته یا خامی باشند که همراه با ابرداده‌ها یا اطلاعات کنترل منتشر می‌شوند. اگر برنامه‌های کاربردی نرم‌افزاری از ورودی‌های تأمین‌شده توسط مهاجمین برای ساختن پیام‌های ساختارمند استفاده کنند و این پیام‌ها را به درستی رمزگشایی ننمایند، مهاجم می‌تواند دستورات مخرب یا کاراکترهای ویژه‌ای را در پیام تعبیه نمایند که سبب شود داده‌ها به عنوان اطلاعات کنترل یا ابرداده‌ها تفسیر شوند. در نتیجه، ماژول یا مؤلفه‌ای که خروجی دستکاری‌شده را دریافت می‌کند، عملیات اشتباهی را انجام می‌دهد یا داده‌ها را به شکل نادرست تفسیر می‌نماید. غربال ورودی‌ها پیش از ارسال آن‌ها برای اینترپرترها مانع از آن می‌شود که محتوا به اشتباه به عنوان دستور تفسیر گردد. تأیید ورودی‌ها سازمان را یاری می‌کند تا اطمینان حاصل نماید که ورودی‌های صحیح و دقیقی به سیستم ارائه شده‌اند. بدین ترتیب، از شمار زیادی از حملات از جمله حملات تزریقی مختلف جلوگیری به عمل خواهد آمد.

کنترل‌های پیشرفته:

(۱) تأیید ورودی اطلاعاتی / قابلیت بازنویسی دستی

سیستم اطلاعاتی:

الف. قابلیت بازنویسی دستی را برای تأیید ورودی [اختصاص: ورودی‌های تعیین‌شده توسط سازمان] فراهم می آورد؛

ب. امکان استفاده از قابلیت بازنویسی دستی را تنها برای [اختصاص: افراد تعیین‌شده توسط سازمان] فراهم می‌آورد؛ و

پ. استفاده از قابلیت بازنویسی دستی را ممیزی می‌نماید.