چارچوب ارزیابی سایبری - نسخه ۳,۲

محتوا

لطفاً توجه داشته باشید: لیستی از تمام تغییرات ایجاد شده بین CAF V3.1 و V3.2 و تمام نسخه های قبلی CAF در وب سایت NCSC موجود است.

CAF – ابزاری برای ارزیابی انعطاف‌پذیری سایبری

چارچوب ارزیابی سایبری (CAF) یک رویکرد سیستماتیک و جامع برای ارزیابی میزان مدیریت ریسک های سایبری برای عملکرد(های) ضروری توسط سازمان ارائه می کند. ارزیابی‌های مبتنی بر CAF می‌تواند توسط خود سازمان (خودارزیابی) یا توسط یک نهاد خارجی مستقل، - احتمالاً یک تنظیم‌کننده / نهاد نظارت سایبری یا یک سازمان ذیصلاح- که از طرف یک رگولاتور عمل می‌کند، مانند ارائه دهندگان خدمات دارای تاییدیه NCSC انجام شود.

هدف و اصول امنیت سایبری و انعطاف پذیری NCSC CAF پایه های CAF را فراهم می کند. ۴ هدف سطح بالا و ۱۴ اصل براساس نتایج نوشته شده اند، یعنی مشخص کردن آنچه باید به دست آید به جای چک لیستی از آنچه باید انجام شود. CAF سطوح بیشتری از جزئیات را به اصول سطح بالا اضافه می‌کند، از جمله مجموعه‌ای از مجموعه‌های ساختاریافته از شاخص‌های عملکرد خوب (IGPs) که با جزئیات بیشتر در زیر توضیح داده شده است.

لازم به ذکر است که NCSC به عنوان مرجع فنی ملی CAF را برای امنیت سایبری با این انتظار که به همراه دیگر موارد، به عنوان ابزاری به منظور حمایت از مقررات موثر سایبری استفاده شود توسعه داد. NCSC خود هیچ مسئولیت رگولاتوری ندارد و سازمان‌های مشمول مقررات سایبری برای اطلاع از امکان استفاده از CAF در چارچوب الزامات نظارتی باید با رگولاتورهای خود مشورت کنند.

الزامات CAF

CAF برای برآوردن مجموعه ای از الزامات زیر ایجاد شده است:

۱. ارائه یک چارچوب مناسب برای کمک به انجام ارزیابی های انعطاف پذیری سایبری.

۲. حفظ رویکرد مبتنی بر نتیجه اصول امنیت و انعطاف پذیری سایبری NCSC و تغییر نحوه انجام ارزیابی ها از روش چک لیستی

۳. سازگاری با دستورالعمل ها و استانداردهای مناسب امنیت سایبری موجود

۴. ایجاد امکان شناسایی فعالیتهای بهبود موثر برامنیت و انعطاف سایبری

۵. در یک نسخه اصلی مشترک که sector-agnostic است موجود باشد.

۶. قابل توسعه به منظور تطبیق مورد نیاز عناصر مختص هر بخش.

۷. تعیین سطوح امنیتی هدف معنادار برای دستیابی سازمانها، که احتمالاً منعکس کننده دیدگاه تنظیم کننده از امنیت مناسب و متناسب است.

۸. به کارگیری تا حد امکان ساده و مقرون به صرفه

اصول CAF و نتایج کمک کننده

هر اصل امنیت و انعطاف پذیری NCSC سطح بالا، یک نتیجه امنیت سایبری گسترده را تعریف می کند. رویکرد دقیقی که سازمان‌ها برای دستیابی به هر اصل باید اتخاذ کنند، مشخص نشده است زیرا این رویکرد بسته به شرایط سازمانی متفاوت خواهد بود. با این حال، هر اصل را می‌توان به مجموعه‌ای از نتایج سطح پایین‌تر مرتبط با امنیت و انعطاف‌پذیری سایبری تقسیم کرد، که معمولاً برای برآورده کردن کامل اصل سطح بالا، باید به همه آن‌ها دست یافت.

ارزیابی میزان رعایت یک اصل خاص توسط یک سازمان با ارزیابی تمام نتایج کمک کننده برای آن اصل انجام می شود. به منظورآگاهی دادن به ارزیابی ها درسطح نتایج کمک کننده:

۱. هریک ازنتایج کمک کننده با مجموعه ای ازشاخص های عملکرد خوب (IGPs) همراه است و

۲. با استفاده از IGP های مربوطه، شرایطی که تحت آن نتیجه کمک کننده «به دست آمده»، «به دست نیامده» یا (در برخی موارد) «تا حدی به دست آمده» ارزیابی می شود، توصیف می شود.

برای هرنتیجه کمک کننده، IGP های مربوطه به راحتی درقالب جدول مرتب شده اند. جداول به دست آمده که به عنوان جداول IGP شناخته می شوند، بلوک های سازنده اساسی CAF را تشکیل می دهند. به این ترتیب، هر اصل با چندین جدول IGP مرتبط است، یک جدول به ازای هرنتیجه کمک کننده.

استفاده ازIGP

ارزیابی نتایج کمک در درجه اول یک موضوع قضاوت تخصصی است و IGP ها الزام استفاده آگاهانه ازتخصص امنیت سایبری و دانش بخش را حذف نمی کنند. IGP ها معمولاً نقاط شروع خوبی برای ارزیابی ها ارائه می دهند، اما باید به طورانعطاف پذیرو درارتباط با راهنمایی های NCSC مرتبط با اصول سطح بالای امنیت و انعطاف پذیری امنیتی استفاده شوند. نتیجه گیری در مورد امنیت سایبری و انعطاف پذیری یک سازمان تنها باید پس از در نظرگرفتن عوامل مرتبط جانبی و شرایط خاص انجام شود.

ستون «به‌دست‌آمده» (سبز) جدول IGP، ویژگی‌های معمول سازمانی را که به طورکامل به آن نتیجه دست می‌یابد، تعریف می‌کند. درنظرگرفته شده است که همه شاخص‌ها معمولاً برای پشتیبانی ازارزیابی «به‌دست‌آمده» وجود داشته باشند. استثناء زمانی است اگر اقدامات جبرانی وجود داشته باشد تا الزامات هدف مربوطه را برآورده کند ممکن است IGP قابل اجرا نباشد.

ستون «به دست نیامده» (RED) جدول IGP ویژگی‌های معمول سازمانی را که به آن نتیجه دست نمی‌یابد، تعریف می‌کند. درنظرگرفته شده است که وجود هریک ازشاخص‌ها معمولاً برای توجیه ارزیابی «حصول نشده» کافی باشد.

درصورت وجود، ستون "جزئی به دست آمده" (AMBER) یک جدول IGP مشخصه های معمول سازمانی است که تا حدی به آن نتیجه دست می یابد. همچنین مهم است که دستاورد جزئی، مزایای خاصی از امنیت سایبری و انعطاف پذیری ارزشمند را ارائه دهد.

جدول زیرنکات کلیدی مرتبط با هدف و ماهیت IGP ها را خلاصه می کند.

	IGP ها هستند...	IGP ها نیستند...
هدف	... قصد کمک به قضاوت کارشناسان را دارد	... چک لیستی برای استفاده در فرآیند ارزیابی غیرقابل انعطاف.
قلمرو	... نمونه های مهمی از آنچه که یک ارزیاب معمولاً باید در نظر بگیرد، که ممکن است دربرخی موارد نیازبه تکمیل داشته باشد.	... فهرستی جامع که همه چیزهایی را که یک ارزیاب باید درنظربگیرد را پوشش می دهد.
قابلیت کاربرد	... طراحی شده است تا به طورگسترده در سازمان های مختلف قابل اجرا باشد، اما قابلیت کاربرد باید ایجاد شود.	... تضمین شده است که به طورکلمه به کلمه درتمام سازمان ها اعمال شود.

تعیین سطوح هدف امنیت و انعطاف پذیری سایبری

نتیجه اعمال CAF،39 ارزیابی منحصربفردی است که هرکدام ازقضاوت درمورد میزان بازتاب شرایط سازمان مورد ارزیابی توسط مجموعه ای از IGP ها حاصل شده است. CAF به گونه ای طراحی شده است که نتیجه ای که درآن تمام ۳۹ نتیجه کمک کننده به عنوان "به دست آمده" ارزیابی می شوند، سطحی از امنیت سایبری را تا حدی فراتر از حداقل سطح "بهداشت سایبری اولیه" نشان می دهد.

یک نهاد نظارتی سایبری باید سطوح هدفی از انعطاف‌پذیری سایبری را برای سازمان‌های درون بخش خود تعیین کند. یکی از راه های تنظیم این سطوح هدف در رابطه با توانایی مقاومت در برابر دسته های مشخصی از حملات سایبری (مانند انعطاف پذیری در برابر حملات قابلیت پایه، حملات با قابلیت متوسط و غیره) است و CAF برای حمایت از این رویکرد از طریق ایده پروفایل های CAF طراحی شده است. .

NCSC با تنظیم‌کننده‌ها و سایر سازمان‌هایی که نقش نظارتی بر انعطاف‌پذیری سایبری دارند، روی رویکردی برای تفسیر خروجی CAF بر اساس شناسایی آن دسته از نتایجی که بیشترین اهمیت را برای دستیابی به منظور مدیریت خطرات امنیتی برای عملکردهای اساسی آن سازمان در نظر گرفته‌اند، کارکرده است. آن نتایج کمک کننده اولویت بندی شده با دیدگاه اولیه امنیت سایبری مناسب و متناسب برای آن سازمان مطابقت دارد. زیرمجموعه‌ای از نتایج کمک‌کننده که به این ترتیب به‌عنوان مهم‌ترین آن‌ها شناسایی شده‌اند، نمونه‌ای از نمایه CAF را نشان می‌دهد – چیزی که می‌تواند به عنوان مبنایی برای تعیین هدف برای دستیابی سازمان‌ها استفاده شود.

درعمل، یک نمایه CAF شامل ترکیبی ازبرخی ازنتایج کمک کننده است که باید در«به دست آمده»، برخی در«تا حدی به دست آمده» و شاید برخی (نشان دهنده قابلیت‌های امنیت سایبری نامناسب در سطح نمایه) به‌عنوان «غیرقابل اجرا» شناسایی شوند.

این مسئولیت NCSC نیست که امنیت و انعطاف پذیری سایبری مناسب و متناسب (همانطورکه درمقررات NIS تعریف شده است) را نشان دهد. تعریف هرهدفی که به لحاظ نتایج CAF برای دستیابی درسازمان ها تعیین شود برعهده نهاد نظارت سایبری مربوطه می باشد.

خاص کردن بخش CAF

هسته مشترک CAF (شامل اصول، نتایج کمک‌کننده و شاخص‌های عملکرد خوب) sector-agnostic است به این معنا که طوری طراحی شده است تا به طورکلی برای همه سازمان‌هایی که مسئول عملکردهای اساسی درتمام بخش‌های کلیدی هستند، قابل اجرا باشد. ممکن است نیازبه برخی ازجنبه های خاص بخش CAF وجود داشته باشد که می تواند شامل موارد زیرباشد:

i) نمایه های CAF خاص بخش

برخی ازپروفایل های هدف ممکن است خاص بخش باشند. همانطورکه دربخش تعیین سطوح هدف ذکرشد، تفسیرنتایج CAF برعهده نهاد نظارت سایبری مربوطه خواهد بود که ممکن است ازدیدگاه نظارتی صورت پذیرد.

ii) تفسیرهای خاص بخش ازنتایج کمک کننده / IGP

ممکن است دربرخی موارد تفسیرخاص بخش ازنتایج کمک کننده و/یا IGPها برای روشن شدن بهترمعنا درداخل بخش ضروری باشد.

iii) پیامدهای کمک کننده اضافی/IGP های خاص بخش

ممکن است شرایطی وجود داشته باشد که درآن الزامات امنیت سایبری خاص بخش را نتوان به اندازه کافی با تفسیریک نتیجه کمک کننده عمومی یا IGP پوشش داد. دراین موارد، ممکن است نیازبه تعریف یک نتیجه کمک کننده خاص بخش یا IGP باشد.

NCSC به کاربا طیف کامل ذینفعان CAF ادامه خواهد داد تا تعیین کند که آیا جنبه‌های خاص CAF مورد نیازاست یا خیر، و درصورت لزوم درایجاد تغییرات کمک کند.

چارچوب ارزیابی سایبری

CAF - هدف A - مدیریت ریسک امنیتی

ساختارها، سیاست‌ها، فرآیندها و رویه‌های سازمانی مناسب برای درک، ارزیابی و مدیریت سیستماتیک خطرات امنیتی شبکه و سیستم‌های اطلاعاتی که از عملکردهای ضروری پشتیبانی می‌کنند.

اصل A1 حاکمیت

سازمان سیاست‌ها، فرآیندها و رویه‌های مدیریتی مناسبی را برای حاکمیت بر رویکرد خود نسبت به امنیت شبکه و سیستم‌های اطلاعاتی درنظرگرفته است.

A1.a هدایت هیئت مدیره

شما مدیریت امنیت سازمانی مؤثری دارید که در سطح هیئت مدیره رهبری می شود و به وضوح در سیاست های مربوطه بیان شده است.

محقق نشده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است
امنیت شبکه و سیستم های اطلاعاتی مرتبط با عملکرد(های) ضروری به طور مرتب در سطح هیئت مدیره مورد بحث و گزارش قرار نمی گیرد. مذاکرات سطح هیئت مدیره در مورد امنیت شبکه و سیستم های اطلاعاتی براساس اطلاعات جزئی یا قدیمی و بدون بهره مندی از راهنمایی های تخصصی است. امنیت شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، به طور موثر توسط جهت تعیین‌شده در سطح هیئت مدیره هدایت نمی‌شوند. مدیریت ارشد یا سایر بخش‌های سازمان، خود را از برخی سیاست‌ها مستثنی می‌دانند و یا انتظار دارند که تسهیلات ویژه‌ای درنظرگرفته شود.	رویکرد و خط مشی سازمان شما در رابطه با امنیت شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، در سطح هیئت مدیره مالکیت و مدیریت می‌شوند. و به شیوه ای معنادار به تصمیم گیرندگان مدیریت ریسک در سراسر سازمان ابلاغ می شوند. مذاکرات منظم در سطح هیئت مدیره در مورد امنیت شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، بر اساس اطلاعات به موقع و دقیق و با راهنمایی تخصصی انجام می شود. فردی در سطح هیئت مدیره وجود دارد که مسئولیت کلی امنیت شبکه و سیستم های اطلاعاتی را بر عهده دارد و بحث های منظم را در سطح هیئت مدیره هدایت میکند. دستورالعمل تنظیم شده در سطح هیئت مدیره به شیوه‌های سازمانی مؤثری تبدیل می‌شود که امنیت شبکه و سیستم‌های اطلاعاتی را که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، هدایت و کنترل می‌کنند.

A1.b نقش ها و مسئولیت ها

سازمان شما نقش ها و مسئولیت هایی را برای امنیت شبکه و سیستم های اطلاعاتی درهمه سطوح، با کانال های واضح و درک شده برای ارتباط و تشدید خطرات ایجاد کرده است.

محقق نشده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است
نقش‌های کلیدی از دست رفته، خالی مانده یا به صورت موقت یا غیررسمی انجام می شود. به کارکنان بدون اختیارات یا منابع کافی مسئولیت های امنیتی محول می شود. کارکنان از وظایف خود در قبال امنیت عملکرد(های) ضروری اطمینان ندارند.	نقش‌ها و مسئولیت‌های کلیدی برای امنیت شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، شناسایی شده‌اند و مرتبا جهت حصول اطمینان ازتناسب با اهداف مورد بررسی قرارمی گیرند. کارکنان توانا و آگاه آن نقش ها را برعهده گرفته و زمان، اختیارو منابع برای انجام وظایف به آن‌ها داده می شود. مسئول امنیت شبکه و سیستم های اطلاعاتی است که از عملکرد(های) ضروری پشتیبانی می کند درسازمان مشخص می باشد.

A1.c تصمیم گیری

شما درسطوح ارشد درقبال امنیت شبکه و سیستم های اطلاعاتی مسئولیت پذیرهستید (مسئول یا پاسخگو دارید) و اختیارات تصمیم گیری را به طورمناسب و موثر تفویض می کنید. خطرات شبکه و سیستم های اطلاعاتی مربوط به عملکرد(های) ضروری شما درچارچوب سایرریسک های سازمانی درنظرگرفته می شود.

محقق نشده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است
آنچه که باید تصمیمات ریسک نسبتاً ساده ای (سرراست - مستقیم) باشد دائماً به سطوح بالاترزنجیره ارجاع داده می شود یا اتخاذ نمی شود. زمانی که استفاده از یک مکانیسم رسمی‌تر گزارش‌دهی ریسک مناسب‌تراست، ریسک‌ها درسطح محلی و به‌طور غیررسمی حل و فصل می‌شوند (یا نادیده گرفته می‌شوند). تصمیم گیرندگان از میزان ریسک پذیری مدیران ارشد اطمینان ندارند یا فقط آن را با عبارات مبهمی مانند "بیزاری" یا "احتیاط" درک می کنند. ساختارسازمانی باعث می شود که تصمیمات ریسک به صورت مجزا گرفته شود. (به عنوان مثال، مهندسی و فناوری اطلاعات در مورد ریسک با یکدیگر صحبت نمی کنند). اولویت های ریسک برای ایجاد تمایز معنادار بین آنها بسیارمبهم هستند. (به عنوان مثال، تقریباً همه خطرات دارای رتبه "متوسط" یا "کهربا" هستند).	مدیریت ارشد تصمیمات ریسک کلیدی اتخاذ شده در سراسرسازمان را تحت نظردارد. تصمیم گیرندگان مدیریت ریسک مسئولیت های خود را برای تصمیم گیری موثرو به موقع درزمینه ریسک پذیری در رابطه با عملکرد(های) اساسی، همانطور که توسط مدیریت ارشد تعیین شده است، درک می کنند. تصمیم گیری مدیریت ریسک در صورت لزوم در سراسر سازمان به افرادی که مهارت ها، دانش، ابزارو اختیارلازم را دارند، تفویض و تشدید می شود. تصمیمات مدیریت ریسک به طور مرتب مورد بازبینی قرار می گیرند تا از ارتباط و اعتبار مستمر آنها اطمینان حاصل شود.

اصل A2 مدیریت ریسک

سازمان اقدامات مناسبی را برای شناسایی، ارزیابی و درک خطرات امنیتی شبکه و سیستم های اطلاعاتی که از عملکرد عملکردهای اساسی پشتیبانی می کنند، انجام می دهد. این شامل یک رویکرد سازمانی کلی برای مدیریت ریسک است.

A2.a فرآیند مدیریت ریسک

سازمان شما دارای فرآیندهای داخلی موثر برای مدیریت خطرات امنیت شبکه و سیستم های اطلاعاتی مربوط به عملکرد(های) ضروری شما و برقراری ارتباط بین فعالیت های مرتبط است.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
ارزیابی ریسک مبتنی بر مجموعه ای مشخص از مفروضات تهدید نیست. خروجی های ارزیابی ریسک آنقدر پیچیده یا سخت هستند که نمی توانند توسط تصمیم گیرندگان مورد استفاده قرار گیرند و به طور مؤثر و شفاف و به موقع ابلاغ نمی شوند. ارزیابی ریسک برای شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، یک فعالیت «یک‌باره» هستند یا اصلاً انجام نمی‌شوند. عناصر امنیتی پروژه ها یا برنامه ها صرفاً به تکمیل ارزیابی مدیریت ریسک بدون توجه به نتایج بستگی دارد. هیچ فرآیند سیستماتیکی برای اطمینان از مدیریت موثر ریسک های امنیتی شناسایی شده وجود ندارد. سیستم ها به صورت مجزا و بدون در نظر گرفتن وابستگی ها و تعاملات با سایر سیستم ها ارزیابی می شوند. (به عنوان مثال، تعامل بین محیط های IT و OT). الزامات امنیتی و اقدامات کاهشی دلخواه هستند یا از یک کاتالوگ کنترل بدون در نظر گرفتن اینکه چگونه به امنیت عملکرد(های) ضروری کمک می کنند، اعمال می شوند.	فرآیند سازمانی شما تضمین میکند که خطرات امنیتی شبکه و سیستم های اطلاعاتی مرتبط با عملکرد(های) ضروری شناسایی، تجزیه و تحلیل، اولویت بندی و مدیریت می شوند. اطلاع رسانی ارزیابی های ریسک شما با درک آسیب‌پذیری‌های شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، صورت می گیرد. خروجی فرآیند مدیریت ریسک شما مجموعه ای واضح از الزامات امنیتی است که خطرات را مطابق با رویکرد سازمانی شما نسبت به امنیت بررسی می کند. نتیجه‌گیری‌های مهمی که در طول فرآیند مدیریت ریسک شما به دست می‌آید به تصمیم‌گیرندگان کلیدی امنیتی و افراد پاسخگو اطلاع داده می‌شود. زمانی ارزیابی ریسک انجام میدهید که رویدادهای مهم به طور بالقوه بر عملکرد(های) اساسی تأثیر بگذارد، مانند جایگزینی یک سیستم یا تغییر در تهدید امنیت سایبری.	فرآیند سازمانی شما تضمین می کند که خطرات امنیتی شبکه و سیستم های اطلاعاتی مرتبط با عملکرد(های) ضروری شناسایی، تجزیه و تحلیل، اولویت بندی و مدیریت می شوند. رویکرد شما به ریسک بر احتمال تأثیر نامطلوب بر عملکرد(های) اساسی شما متمرکز است، که منجر به درک دقیقی از چگونگی ایجاد چنین تأثیری در نتیجه اقدامات احتمالی مهاجم و ویژگی‌های امنیتی شبکه و سیستم‌های اطلاعاتی شما می‌شود. ارزیابی‌های ریسک شما بر اساس مجموعه‌ای از مفروضات تهدید است که به وضوح درک شده‌اند، که با درک به‌روز از تهدیدات امنیتی برای عملکرد(های) ضروری و بخش شما اطلاع‌رسانی شده است. ارزیابی‌های ریسک شما با درک آسیب‌پذیری‌های شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، صورت می گیرد. خروجی فرآیند مدیریت ریسک شما مجموعه ای واضح از الزامات امنیتی است که خطرات را مطابق با رویکرد سازمانی شما نسبت به امنیت بررسی می کند. نتیجه‌گیری‌های مهمی که در طول فرآیند مدیریت ریسک شما به دست می‌آید به

خطرات برای مدت طولانی حل نشده باقی می مانند و در انتظار تصمیم گیری ارشد یا تخصیص منابع برای حل و فصل است.	شما تجزیه و تحلیل تهدید را انجام می دهید و چگونگی اثرگذاری تهدیدات عمومی بر سازمان را درک می کنید.	تصمیم‌گیرندگان کلیدی امنیتی و افراد پاسخگو اطلاع داده می‌شود. ارزیابی ریسک شما پویا هستند و با توجه به تغییرات مربوطه که ممکن است شامل تغییرات فنی در شبکه و سیستم های اطلاعاتی، تغییر کاربری و اطلاعات تهدید جدید شد، به روز می‌شود اثربخشی فرآیند مدیریت ریسک شما به طور منظم بررسی و در صورت لزوم، بهبودهایی انجام می شود. شما تجزیه و تحلیل دقیق تهدید را انجام می دهید و درک می کنید که چگونه این امر در سازمان شما در زمینه تهدید برای بخش شما و CNI گسترده تر اعمال می شود.

A2.b تضمین

شما نسبت به اثربخشی امنیت فناوری، افراد و فرآیندهای مرتبط با عملکرد(های) ضروری خود اطمینان پیدا کرده اید.

محقق نشده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است
یک محصول یا خدمات خاص به عنوان یک "گلوله نقره ای" در نظر گرفته می شود و ادعاهای فروشنده به ارزش اسمی در نظر گرفته می شود. روش‌های تضمین بدون درک نقاط قوت و محدودیت‌های آن‌ها، مانند خطرات آزمایش نفوذ در محیط‌های عملیاتی، اعمال می‌شوند. اطمینان فرض می شود زیرا تا به امروز هیچ مشکل شناخته شده ای وجود نداشته است.	شما تأیید می‌کنید که اقدامات امنیتی موجود برای محافظت از شبکه و سیستم‌های اطلاعاتی مؤثر بوده و در طول عمری که به آنها نیاز است، مؤثر باقی می‌مانند. شما روش های تضمینی موجود را درک می کنید و روش های مناسب را برای به دست آوردن اطمینان در امنیت عملکرد(های) ضروری انتخاب می کنید. اعتماد شما به امنیت در ارتباط با فناوری، افراد و فرآیندهای شما می‌تواند برای شخص ثالث توجیه و تأیید شود. کاستی‌های امنیتی کشف‌شده توسط فعالیت‌های تضمینی، ارزیابی، اولویت‌بندی و در صورت لزوم به‌موقع و مؤثر اصلاح می‌شوند. روش‌های مورد استفاده برای اطمینان مورد بازنگری قرار می‌گیرند تا اطمینان حاصل شود که طبق پیش‌بینی کار می‌کنند و مناسب‌ترین روش برای استفاده باقی می‌مانند.

اصل A3 مدیریت دارایی

همه چیزمورد نیازبرای ارائه، نگهداری یا پشتیبانی شبکه و سیستم های اطلاعاتی لازم برای عملکرد عملکردهای اساسی تعیین و درک می شود. این شامل داده ها، افراد و سیستم ها، و همچنین هرگونه زیرساخت پشتیبانی (مانند برق یا خنک کننده) می شود.

A3.a مدیریت دارایی

محقق نشده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است
موجودی دارایی های مربوط به عملکرد(های) اساسی ناقص، وجود ندارد، یا با جزئیات ناکافی است. فقط دامنه ها یا انواع خاصی از دارایی ها مستند و درک می شوند. وابستگی بین دارایی ها درک نمی شود (مانند وابستگی بین IT و OT). دارایی‌های اطلاعاتی، که می‌تواند شامل اطلاعات شناسایی شخصی و/یا داده‌های مهم/حیاتی باشد، برای مدت طولانی بدون نیاز تجاری یا خط‌مشی نگهداری مشخص ذخیره می‌شوند. دانش حیاتی برای مدیریت، بهره برداری، یا بازیابی عملکرد(های) ضروری توسط یک یا دو فرد کلیدی بدون برنامه جانشینی نگهداری می شود. موجودی دارایی ها نادیده گرفته شده و تاریخ گذشته است.	تمام دارایی های مربوط به کارایی ایمن عملکرد(های) ضروری شناسایی و ازآن‌ها لیستی تهیه (با سطح مناسبی ازجزئیات) و به روزنگه داشته می شود. وابستگی ها به زیرساخت های پشتیبانی (مانند برق، خنک کننده و غیره) شناسایی و ثبت می شوند. شما دارایی های خود را با توجه به اهمیت آنها برای عملکرد(های) ضروری اولویت بندی کرده اید. شما مسئولیت مدیریت همه دارایی‌ها، از جمله دارایی‌های فیزیکی، مرتبط با عملکرد(های) ضروری را به تعیین نموده اید. دارایی‌های مرتبط با عملکرد(های) ضروری با در نظر گرفتن امنیت سایبری در طول چرخه عمرشان، ازایجاد تا ازکارانداختن یا دفع نهایی، مدیریت می‌شوند.

اصل A4 زنجیره تامین

سازمان خطرات امنیتی ناشی از وابستگی به تامین کنندگان خارجی در رابطه با شبکه و سیستم های اطلاعاتی را که از عملکردهای اساسی پشتیبانی می کند را درک و مدیریت می کند. این شامل حصول اطمینان از استفاده از اقدامات مناسب درمواردی است که ازخدمات شخص ثالث استفاده می شود.

A4.a زنجیره تامین

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است	تمام عبارات زیردرست است
شما نمی دانید کدام داده های متعلق به شما توسط تامین کنندگان نگهداری می شود یا چگونه مدیریت می شود.	شما خطرات کلی که ممکن است تامین کنندگان برای عملکرد(های) ضروری شما ایجاد کنند را درک می کنید.	شما درک عمیقی از زنجیره تامین خود، از جمله پیمانکاران فرعی و خطرات گسترده‌تری دارید که با آن مواجه است. شما عواملی مانند مشارکت تامین کننده، رقبا، ملیت و دیگر سازمان هایی که با آن‌ها

اجزای زنجیره تامین برای عملکرد(های) ضروری به صورت قراردادی فرعی هستند و شما به پیمانکاران فرعی دسترسی کم یا اصلا دسترسی ندارید. شما نمی دانید کدام قراردادها مرتبط هستند و/یا قراردادهای مربوطه تعهدات امنیتی مناسبی را مشخص نمی کنند. تامین‌کنندگان به سیستم‌هایی دسترسی دارند که عملکرد(های) ضروری شما را ارائه می‌دهند که این دسترسی بدون نظارت نمی شود و کنترل‌های امنیتی شما را دور می‌زند.	شما وسعت زنجیره تامین خود که از عملکرد(های) ضروری شما پشتیبانی می کند از جمله پیمانکاران فرعی می‌دانید. شما درک می کنید که کدام قراردادها مرتبط هستند و تعهدات امنیتی مناسب را در قراردادهای مربوطه لحاظ می کنید. شما از تمام اتصالات شخص ثالث آگاه هستید و اطمینان دارید که آنها الزامات امنیتی سازمان شما را برآورده می کنند. رویکرد شما به مدیریت حوادث امنیتی، حوادثی که ممکن است در زنجیره تامین شما رخ دهد را در نظر می گیرد. شما مطمئن هستید که اطلاعات به اشتراک گذاشته شده با تامین کنندگان که برای عملکرد(های) ضروری شما مورد نیاز است به طور مناسب در برابر حملات شناخته شده و آسیب پذیری های شناخته شده محافظت می شود.	قرارداد می بندند را در نظر می گیرد. این به ارزیابی ریسک و فرآیندهای تدارکات شما کمک می کند. رویکرد شما برای مدیریت ریسک زنجیره تامین، خطرات مربوط به عملکرد(های) ضروری شما را در نظر می گیرد که ناشی از براندازی زنجیره تامین توسط مهاجمان توانمند و دارای منابع خوب است. شما اطمینان دارید که اطلاعات به اشتراک گذاشته شده با تامین کنندگان که برای عملکرد(های) شما ضروری است به طور مناسب در برابر حملات پیچیده محافظت می شود. شما درک می کنید که کدام قراردادها مرتبط هستند و تعهدات امنیتی مناسب را در قراردادهای مربوطه لحاظ می کنید. شما یک رویکرد پیشگیرانه برای مدیریت قرارداد دارید که ممکن است شامل یک برنامه مدیریت قرارداد برای قراردادهای مربوطه باشد. مسئولیت های مشتری / حق مالکیت تامین کننده در قراردادها مشخص شده است. تمام اتصالات شبکه و اشتراک داده با اشخاص ثالث به طور مؤثر و متناسب مدیریت می شوند. در صورت لزوم، فرآیند مدیریت حادثه شما و تامین کنندگان شما، پشتیبانی متقابلی را در حل و فصل حوادث ارائه می دهند.

CAF - هدف B - محافظت در برابر حملات سایبری

تدابیر امنیتی متناسبی برای محافظت از شبکه و سیستم‌های اطلاعاتی که از عملکردهای ضروری در برابر حملات سایبری پشتیبانی می‌کنند، وجود دارد.

اصل B1 خط مشی ها، فرآیندها و رویه های حفاظت از خدمات

سازمان سیاست‌ها، فرآیندها و رویه‌های مناسبی را تعریف، اجرا، ابلاغ و لازم الاجرا می‌کند که رویکرد کلی آن را به سمت ایمن‌سازی سیستم‌ها و داده‌هایی که از عملکردهای اساسی پشتیبانی می‌کنند، هدایت می‌کند.

B1.a توسعه سیاست، فرآیند و رویه

شما مجموعه‌ای از سیاست‌ها، فرآیندها و رویه‌های امنیت و انعطاف‌پذیری سایبری را که خطر تأثیر نامطلوب بر عملکرد(های) ضروری شما را مدیریت و کاهش می‌دهد، توسعه داده‌اید و به بهبود آن ادامه می‌دهید .

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
خط‌مشی‌ها، فرآیندها و رویه‌های شما وجود ندارند یا ناقص هستند. خط‌مشی‌ها، فرآیندها و رویه‌ها به‌طور جامع یا پیوسته اعمال نمی‌شوند. مردم اغلب یا به طور معمول سیاست ها، فرآیندها و رویه ها را برای دستیابی به اهداف تجاری دور می زنند. رویکرد حاکمیت امنیتی و مدیریت ریسک سازمان شما هیچ تأثیری بر خط‌مشی‌ها، فرآیندها و رویه‌های شما ندارد. امنیت سیستم کاملاً به کاربرد دقیق و مداوم فرآیندهای امنیتی دستی توسط کاربران وابسته است. خط‌مشی‌ها، فرآیندها و رویه‌ها در نتیجه تغییرات عمده (مانند چارچوب فن آوری یا نظارتی)، یا در یک دوره مناسب بازنگری نشده‌اند. خط‌مشی‌ها، فرآیندها و رویه‌ها به‌راحتی در دسترس کارکنان قرار نمی‌گیرند، به قدری جزئی هستند که	خط‌مشی‌ها، فرآیندها و رویه‌های شما، رویکرد حاکمیت امنیتی و مدیریت ریسک، اقدامات فنی امنیتی و انطباق با مقررات خاص را مستند می‌کند. شما خط‌مشی‌ها، فرآیندها و رویه‌ها را در پاسخ به حوادث مهم امنیت سایبری بررسی و به‌روزرسانی می‌کنید	شما به طور کامل رویکرد حاکمیت امنیتی و مدیریت ریسک، عملکرد فنی امنیتی و انطباق مقررات خاص خود را مستند می کنید. امنیت سایبری در سرتاسر خط‌مشی‌ها، فرآیندها و رویه‌ها یکپارچه و تعبیه شده است و شاخص‌های عملکرد کلیدی به مدیریت اجرایی شما گزارش می‌شود. خط‌مشی‌ها، فرآیندها و رویه‌های سازمان شما به گونه‌ای طراحی شده‌اند که کاربردی، قابل استفاده و مناسب برای عملکرد(های) ضروری شما و فناوری‌های شما باشند. خط‌مشی‌ها، فرآیندها و رویه‌هایی که بر رفتار کاربر متکی هستند، کاربردی، مناسب و قابل دستیابی هستند. شما خط‌مشی‌ها، فرآیندها و رویه‌ها را در بازه‌های زمانی مناسب بررسی و به‌روزرسانی می‌کنید تا اطمینان حاصل کنید که مرتبط هستند. این علاوه بر بررسی های پس از یک حادثه بزرگ امنیت سایبری است.

امکان یادآوری ندارند، یا درک آن‌ها خیلی سخت است.		هرگونه تغییر یا تهدید عملکرد(های) ضروری موجب بازبینی سیاست ها، فرآیندها و رویه ها می گردد. سیستم‌های شما طوری طراحی شده‌اند که حتی زمانی که سیاست‌ها، فرآیندها و رویه‌های امنیتی کاربر همیشه رعایت نمی‌شوند، امن باقی می‌مانند.

B1.b اجرای سیاست، فرآیند و رویه

شما سیاست ها، فرآیندها و رویه های امنیتی خود را با موفقیت اجرا کرده اید و می توانید مزایای امنیتی به دست آمده را شرح دهید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
خط‌مشی‌ها، فرآیندها و رویه‌ها نادیده گرفته می‌شوند یا فقط تا حدی دنبال می‌شوند. اینکه چگونه خط‌مشی‌ها، فرآیندها و رویه‌های شما از انعطاف‌پذیری عملکرد(های) ضروری شما پشتیبانی می‌کنند به خوبی درک نشده است. کارکنان از مسئولیت های خود تحت خط مشی ها، فرآیندها و رویه های شما بی اطلاع هستند. شما سعی نمی کنید نقض خط مشی ها، فرآیندها و رویه ها را شناسایی کنید. خط‌مشی‌ها، فرآیندها و رویه‌ها فاقد یکپارچگی با سایر سیاست‌ها، فرآیندها و رویه‌های سازمانی هستند. خط‌مشی‌ها، فرآیندها و رویه‌های شما به خوبی در سراسر سازمان شما ابلاغ نشده است.	بیشتر خط‌مشی‌ها، فرآیندها و رویه‌های شما دنبال می‌شوند و استفاده از آن‌ها نظارت می‌شود. خط‌مشی‌ها، فرآیندها و رویه‌های شما با سایر سیاست‌ها، فرآیندها و رویه‌های سازمانی، از جمله ارزیابی‌های منابع انسانی از قابلیت اعتماد افراد، ادغام می‌شوند. همه کارکنان از مسئولیت های خود تحت خط مشی ها، فرآیندها و رویه های شما آگاه هستند. همه موارد نقض خط‌مشی‌ها، فرآیندها و رویه‌ها با پتانسیل تأثیر نامطلوب بر عملکرد(های) اساسی به طور کامل بررسی می‌شوند. سایر نقض‌ها ردیابی می‌شوند، از نظر روند ارزیابی می‌شوند و اقداماتی برای درک و رسیدگی انجام می‌شود.	تمام خط مشی ها، فرآیندها و رویه های شما دنبال می شود، کاربرد صحیح و کارایی امنیتی آنها ارزیابی می شود. خط‌مشی‌ها، فرآیندها و رویه‌های شما با سایر سیاست‌ها، فرآیندها و رویه‌های سازمانی، از جمله ارزیابی‌های منابع انسانی از قابلیت اعتماد افراد، ادغام می‌شوند. خط‌مشی‌ها، فرآیندها و رویه‌های شما به‌طور مؤثر و مناسب در تمام سطوح سازمان به اطلاع کارکنان می‌رسد که منجر به آگاهی کارکنان از مسئولیت‌های خود می‌شود. اقدامات مناسب برای رسیدگی به همه نقض‌های خط‌مشی‌ها، فرآیندها و رویه‌هایی از جمله نقض‌های انبوه که بالقوه تأثیر نامطلوب بر عملکرد(های) دارند، انجام می‌شود.

اصل B2 هویت و کنترل دسترسی

سازمان دسترسی به شبکه و سیستم های اطلاعاتی را که از عملکردهای ضروری پشتیبانی می کنند، درک، مستندسازی و مدیریت می کند. کاربران (یا اقدامات خودکار) که می توانند به داده ها یا سیستم ها دسترسی داشته باشند به طور مناسب تأیید، احراز هویت و مجاز می شوند.

B2.a تأیید هویت، احراز هویت و مجوز

شما به طور قوی دسترسی به شبکه و سیستم های اطلاعاتی را که از عملکرد(های) ضروری شما پشتیبانی می کنند، تأیید، احراز هویت و مجوز می دهید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
تأیید هویت اولیه به اندازه کافی قوی نیست تا سطح قابل قبولی از اطمینان نمایه هویت کاربر را ارائه دهد. کاربران و سیستم‌های مجاز با دسترسی به شبکه‌ها یا سیستم‌های اطلاعاتی که عملکرد(های) ضروری شما به آنها وابسته است را نمی‌توان به صورت جداگانه شناسایی کرد. افراد یا دستگاه‌های غیرمجاز می‌توانند به شبکه یا سیستم‌های اطلاعاتی شما دسترسی داشته باشند که عملکرد(های) ضروری شما به آن بستگی دارد. تعداد کاربران و سیستم های مجاز که به شبکه و سیستم های اطلاعاتی شما دسترسی دارند به حداقل های لازم محدود نمی شود. رویکرد شما برای احراز هویت کاربران، دستگاه‌ها و سیستم‌ها از بهترین روش‌های به روز پیروی نمی‌کند.	فرآیند تأیید هویت اولیه شما به اندازه کافی قوی است تا قبل از اجازه دسترسی کاربر مجاز به شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، سطح معقولی از اطمینان از نمایه هویت کاربر را فراهم کند. همه کاربران و سیستم‌های مجاز با دسترسی به شبکه یا سیستم‌های اطلاعاتی که عملکرد(های) ضروری شما به آنها وابسته است، به‌صورت جداگانه شناسایی و احراز هویت می‌شوند. تعداد کاربران و سیستم‌های مجاز که به شبکه و سیستم‌های اطلاعاتی و عملکرد(های) ضروری دسترسی دارند به حداقل لازم محدود شده است. شما از مکانیسم‌های احراز هویت اضافی، مانند احراز هویت چند عاملی (MFA) برای دسترسی ممتاز به تمام شبکه‌ها و سیستم‌های اطلاعاتی که عملکرد(های) ضروری شما را اداره یا پشتیبانی می‌کنند، استفاده می‌کنید. شما به طور جداگانه همه دسترسی های راه دور به شبکه ها و سیستم های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می کنند را تأیید و مجوز می دهید. فهرست کاربران و سیستم‌های دارای دسترسی به شبکه و سیستم‌های	فرآیند تأیید هویت اولیه شما به اندازه کافی قوی است تا قبل از اجازه دادن به کاربر مجاز برای دسترسی به شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، سطح بالایی از اطمینان از نمایه هویت کاربر را فراهم کند. فقط کاربران مجاز و دارای احراز هویت فردی می توانند به صورت فیزیکی و منطقی به شبکه یا سیستم های اطلاعاتی شما که عملکرد(های) ضروری به آن‌ها بستگی دارد دسترسی داشته باشند. تعداد کاربران و سیستم‌های مجاز که به تمام شبکه‌ها و سیستم‌های اطلاعاتی شما که از عملکرد(های) ضروری پشتیبانی می‌کنند دسترسی دارند به حداقل لازم محدود شده است. شما از مکانیسم‌های احراز هویت اضافی، مانند چند عاملی (MFA) برای همه دسترسی‌های کاربر، از جمله دسترسی از راه دور، به تمام شبکه‌ها و سیستم‌های اطلاعاتی که عملکرد(های) ضروری شما را اداره یا پشتیبانی می‌کنند، استفاده می‌کنید. فهرست کاربران و سیستم‌هایی که به شبکه‌ها و سیستم‌های اطلاعاتی دسترسی دارند که عملکرد(های) ضروری را پشتیبانی و ارائه می‌کنند، به

	اطلاعاتی که عملکرد(های) ضروری را پشتیبانی و ارائه می‌کنند، حداقل سالیانه به طور منظم بررسی می‌شود. رویکرد شما برای احراز هویت کاربران، دستگاه‌ها و سیستم‌ها از بهترین روش‌های به روز پیروی می‌کند.	طور منظم، حداقل هر شش ماه یکبار بررسی می‌شود. رویکرد شما برای احراز هویت کاربران، دستگاه‌ها و سیستم‌ها از بهترین روش‌های به روز پیروی می‌کند

B2.b مدیریت دستگاه

شما تجهیزاتی که برای دسترسی به شبکه‌ها، سیستم‌های اطلاعاتی و داده‌هایی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، و استفاده می‌شوند را کاملاً می‌شناسید و به آن‌ها اعتماد دارید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
کاربران می توانند با استفاده از دستگاه هایی که مالکیت و مدیریت شرکتی ندارند، به شبکه و سیستم های اطلاعاتی شما که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، متصل شوند. کاربران ممتاز می‌توانند عملیات ممتاز را از دستگاه‌هایی که تحت مالکیت و مدیریت شرکت نیستند، انجام دهند. شما از امنیت دستگاه ها یا شبکه های شخص ثالث متصل به سیستم های خود اطمینان کسب نکرده اید. اتصال فیزیکی یک دستگاه به شبکه و سیستم های اطلاعاتی شما به آن دستگاه امکان دسترسی بدون احراز هویت دستگاه یا کاربر را می دهد	فقط دستگاه‌های تحت مالکیت و مدیریت شرکت می‌توانند به شبکه و سیستم‌های اطلاعاتی شما دسترسی داشته باشند. تمام عملیات ممتاز از دستگاه های تحت مالکیت و مدیریت شرکت انجام می شود. این دستگاه ها با استفاده از رویکرد مبتنی بر ریسک، جداسازی کافی از فعالیت های کاربران استاندارد را فراهم می کنند. شما به دنبال درک ویژگی های امنیتی دستگاه ها و شبکه های شخص ثالث قبل از اینکه به سیستم شما متصل شوند، بوده اید. شما اقدامات مناسب را برای کاهش خطرات شناسایی شده انجام داده اید. عمل اتصال به پورت یا کابل شبکه به هیچ سیستمی اجازه دسترسی نمی دهد. شما می توانید دستگاه های ناشناخته متصل به شبکه و سیستم های اطلاعاتی خود را شناسایی کرده و چنین حوادثی را بررسی کنید.	تمام عملیات ممتاز انجام شده در شبکه و سیستم‌های اطلاعاتی شما که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، از دستگاه‌های بسیار قابل اعتماد، مانند ایستگاه‌های کاری دسترسی ممتاز، که صرفاً به آن عملیات اختصاص داده شده است، انجام می‌شوند. شما یا تضمین مستقل و حرفه ای از امنیت دستگاه ها یا شبکه های شخص ثالث را قبل از اتصال به شبکه و سیستم های اطلاعاتی خود دریافت می کنید، یا فقط به دستگاه ها یا شبکه های شخص ثالثی که برای پشتیبانی از شبکه و سیستم های اطلاعاتی شما اختصاص داده شده اند اجازه اتصال می دهید. شما مدیریت هویت دستگاه مبتنی بر گواهی را انجام می‌دهید و فقط به دستگاه‌های شناخته شده اجازه می‌دهید به سیستم‌های لازم برای عملکرد(های) ضروری شما دسترسی داشته باشند. شما به طور منظم اسکن می کنید تا دستگاه های ناشناخته را شناسایی کرده و یافته ها را بررسی کنید.

B2.c مدیریت کاربر ممتاز

شما دسترسی ممتاز کاربر به شبکه و سیستم های اطلاعاتی را که از عملکرد(های) ضروری شما پشتیبانی می کنند، از نزدیک مدیریت می کنید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
هویت افراد دارای دسترسی ممتاز به شبکه و سیستم‌های اطلاعاتی (زیرساخت‌ها، پلتفرم‌ها، نرم‌افزار، پیکربندی و غیره) که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، معلوم نیست یا مدیریت نمی‌شوند. دسترسی کاربر ممتاز به شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند از طریق مکانیسم‌های احراز هویت ضعیف (مانند. فقط رمزهای عبور ساده). لیست کاربران ممتاز اخیراً بررسی نشده است (به عنوان مثال در ۱۲ ماه گذشته). دسترسی کاربر ممتاز به جای نقش یا عملکرد(ها) بر اساس سیستم گسترده اعطا می شود. دسترسی کاربر ممتاز به عملکرد(های) ضروری شما از طریق حساب های نام عمومی، مشترک یا پیش فرض است. در جایی که پایانه‌های «همیشه روشن» وجود دارند که می‌توانند اقدامات ممتاز را انجام دهند (مانند اتاق کنترل)، هیچ کنترل اضافی (مانند کنترل‌های فیزیکی) برای اطمینان از محدود شدن دسترسی مناسب وجود ندارد. هیچ تفکیک منطقی بین نقش‌هایی که یک فرد ممکن است داشته باشد و در نتیجه اقداماتی که انجام می‌دهد (مانند دسترسی به ایمیل شرکت و اقدامات کاربر امتیاز) وجود ندارد.	تمام دسترسی کاربران ممتاز به شبکه و سیستم های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می کنند، نیاز به احراز هویت قوی، مانند چند عاملی (MFA) دارند. هویت افراد دارای دسترسی ممتاز به شبکه و سیستم‌های اطلاعاتی (زیرساخت، پلتفرم، نرم‌افزار، پیکربندی و غیره) که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، شناخته شده و مدیریت می‌شوند. این شامل اشخاص ثالث می شود. فعالیت توسط کاربران ممتاز به طور معمول بررسی و تأیید می شود (به عنوان مثال حداقل سالانه). به کاربران ممتاز فقط حقوق دسترسی ویژه کاربران ممتاز مورد نیاز آن‌ها برای نقش یا عملکرد تجاری مربوطه اعطا می شود	دسترسی کاربر ممتاز به شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند از حساب‌های جداگانه اختصاصی که به دقت نظارت و مدیریت می‌شوند انجام می‌شود. صدور حقوق موقت و محدود به زمان برای دسترسی کاربر ممتاز و/یا دسترسی پشتیبانی خارجی شخص ثالث برقرار است. حقوق دسترسی ممتاز کاربر به‌عنوان بخشی از فرآیند پیوستن، جابجایی و ترک‌کردن به‌طور مرتب بررسی و همیشه به‌روزرسانی می‌شود. تمام فعالیت‌های کاربر ممتاز به طور معمول برای تجزیه و تحلیل و بررسی آفلاین بررسی، تأیید و ثبت می‌شوند.

B2.d مدیریت هویت و دسترسی (IdAM)

شما از نزدیک هویت و دسترسی کاربران، دستگاه‌ها و سیستم‌هایی متصل به شبکه و سیستم‌های اطلاعاتی پشتیبانی کننده از عملکرد(های) ضروری را مدیریت و نگهداری می کنید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
حقوق دسترسی بیشتر از آنچه لازم است اعطا می شود. اعتبارسنجی هویت و الزام برای دسترسی کاربر، دستگاه یا سیستم ها انجام نمی شود. هنگام تغییر نقش کاربران، حقوق دسترسی کاربر بررسی نمی شود. هنگامی که کاربران سازمان شما را ترک می کنند، حقوق دسترسی کاربر فعال باقی می ماند. حقوق دسترسی اعطا شده به دستگاه ها یا سیستم ها برای دسترسی به سایر دستگاه ها و سیستم ها به طور منظم (حداقل سالانه) بررسی نمی شود.	برای تأیید هر کاربر و صدور حداقل حقوق دسترسی مورد نیاز، از یک روش قوی پیروی می کنید. شما به طور منظم حقوق دسترسی را بررسی می کنید و آنهایی که دیگر مورد نیاز نیستند لغو می شوند. حقوق دسترسی کاربر زمانی بررسی می‌شود که کاربران نقش‌های خود را از طریق فرآیند پیوستن، ترک و جابجایی شما تغییر دهند. تمام دسترسی کاربر، دستگاه و سیستم به سیستم‌هایی که از عملکرد(های) ضروری پشتیبانی می‌کنند ثبت و نظارت می‌شوند، اما با سایر داده‌های گزارش یا سوابق دسترسی مقایسه نمی‌شوند.	برای تأیید هر کاربر و صدور حداقل حقوق دسترسی مورد نیاز، از یک رویه قوی پیروی می‌کنید و کاربرد این رویه مرتباً بررسی می‌شود. حقوق دسترسی کاربر هر دو زمانی که افراد نقش را تغییر می دهند بررسی می شود از طریق فرآیند اتصال دهنده ها، ترک ها و جابجایی ها و در فواصل زمانی منظم - حداقل سالیانه. تمام دسترسی کاربران، دستگاه ها و سیستم ها به سیستم هایی که از عملکرد(های) ضروری پشتیبانی می کنند ثبت و نظارت می شود. شما به طور منظم گزارش های دسترسی را بررسی می کنید و این داده ها را با سایر سوابق دسترسی و فعالیت های مورد انتظار مرتبط می کنید. تلاش کاربران، دستگاه ها یا سیستم های غیرمجاز برای اتصال به سیستم هایی که از عملکرد(های) ضروری پشتیبانی می کنند هشدار داده می شوند، به سرعت ارزیابی و بررسی می شوند.

اصل B3 امنیت داده ها

داده هایی که به صورت الکترونیکی ذخیره یا منتقل می شوند دربرابراقداماتی مانند دسترسی غیرمجاز، اصلاح یا حذف که ممکن است تأثیرنامطلوبی برعملکردهای اساسی داشته باشد محافظت می شود. چنین حفاظتی درمورد ابزارهایی که توسط آن کاربران، دستگاه ها و سیستم های مجازبه داده های حیاتی لازم برای عملکرد عملکردهای ضروری دسترسی دارند، صدق می کند و همچنین اطلاعاتی مانند جزئیات طراحی شبکه و سیستم های اطلاعاتی که به مهاجم کمک می کند را پوشش می دهد.

B3.a درک داده ها

شما درک خوبی از داده های مهم برای عملکرد(های) ضروری خود دارید، جایی که ذخیره می شود، کجا حرکت می کند و اینکه چگونه ممکن است دسترسی غیرمجاز، (تغییر یا حذف) بر عملکرد(های) ضروری تأثیر منفی می گذارد. این موضوع همچنین شامل اشخاص ثالثی که داده‌های مهم برای عملکرد(های) ضروری شما را ذخیره می‌کنند یا به آنها دسترسی دارند، نیز می‌شود.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
شما اطلاعات کاملی در مورد اینکه چه داده هایی توسط عملکرد(های) ضروری استفاده و تولید می شوند، ندارید. شما داده های مهمی را که عملکرد(های) ضروری شما بر آنها تکیه دارد، شناسایی نکرده اید. شما اشخاص دارای دسترسی به داده های مهم برای عملکرد(های) ضروری را شناسایی نکرده اید. شما تأثیر به خطر افتادن داده ها یا عدم دسترسی به آنها را به وضوح بیان نکرده اید.	شما تمام داده‌های مهم برای عملکرد(های) ضروری و یا داده هایی که به مهاجم کمک می‌کند را شناسایی و فهرست‌بندی کرده‌اید. شما افرادی را که به داده های مهم برای عملکرد(های) ضروری دسترسی دارند، شناسایی و فهرست بندی کرده اید. شما به طور منظم مکان، انتقال، کمیت و کیفیت داده های مهم برای عملکرد(های) ضروری را بررسی می کنید. شما همه دستگاه‌های سیار و قابل حمل و رسانه‌هایی که داده‌های مهمی برای عملکرد(های) ضروری دارند، را شناسایی کرده‌اید. شما تأثیر همه سناریوهای مربوط به عملکرد (های) ضروری خود، از جمله دسترسی غیرمجاز، اصلاح یا حذف داده، یا زمانی که کاربران مجاز قادر به دسترسی مناسب به این	شما تمام داده‌های مهم برای عملکرد(های) ضروری و یا داده هایی که به مهاجم کمک می‌کند را شناسایی و فهرست‌بندی کرده‌اید. شما افرادی را که به داده های مهم برای عملکرد(های) ضروری دسترسی دارند، شناسایی و فهرست بندی کرده اید. شما درک فعلی از مکان، کمیت و کیفیت داده های مهم برای عملکرد(های) ضروری را حفظ می کنید. شما اقداماتی را برای حذف یا به حداقل رساندن کپی های غیر ضروری یا داده های تاریخی غیرضروری انجام می دهید. شما همه دستگاه‌های سیار و قابل حمل و رسانه‌هایی که داده‌های مهمی برای عملکرد(های) ضروری دارند، را شناسایی کرده‌اید. شما درک فعلی از پیوندهای داده ای برای انتقال داده های مهم که برای عملکرد(های) ضروری شما مهم هستند را حفظ می کنید.

	داده ها نیستند، را درک کرده و مستند می کنید. شما گاهی اوقات این عبارات تأثیر مستند را تأیید می کنید	شما زمینه، محدودیت ها و وابستگی های داده های مهم خود را درک می کنید. شما تأثیر همه سناریوهای مربوط به عملکرد (های) ضروری خود، از جمله دسترسی غیرمجاز، اصلاح یا حذف داده، یا زمانی که کاربران مجاز قادر به دسترسی مناسب به این داده ها نیستند، را درک کرده و مستند می کنید. شما این اظهارات تأثیر مستند را به طور مرتب، حداقل سالیانه تأیید می کنید.

B3.b داده درحال انتقال

شما ازانتقال داده های مهم برای عملکرد(های) ضروری خود محافظت کرده اید. این شامل انتقال داده ها به اشخاص ثالث است.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است	تمام عبارات زیردرست است
شما همه پیوندهای داده خود را نمی شناسید یا نمی دانید کدام یک داده های مهم برای عملکرد(های) ضروری را حمل می کنند. داده‌های مهم برای عملکرد(های) ضروری بدون حفاظت فنی و با استفاده از حامل‌های غیرقابل اعتماد یا با دسترسی عمومی جابجا می شوند. جایگزینی برای مسیرهای داده حیاتی که ممکن است ازکار بیفتند، مسدود شوند، بیش از حد بارگذاری شوند و غیره وجود ندارند.	شما تمام پیوندهای داده ای که داده های مهم برای عملکرد(های) ضروری شما را حمل می کنند، شناسایی و محافظت کرده اید (به طورموثر و متناسب). شما از ابزارهای فنی مناسب (مانند رمزنگاری) برای محافظت از داده‌هایی استفاده می‌کنید که از طریق حامل‌های غیرقابل اعتماد یا در دسترس آشکار جابجا می شوند، اما به استحکام حفاظت اعمال‌شده اعتماد محدودی دارید یا هیچ اطمینانی ندارید.	شما تمام پیوندهای داده ای که داده های مهم برای عملکرد(های) ضروری شما را حمل می کنند، شناسایی و محافظت کرده اید (به طور موثر و متناسب). شما از ابزارهای فیزیکی و/یا فنی مناسب برای محافظت از داده‌هایی که ازطریق حامل‌های غیرقابل اعتماد یا در دسترس آشکار جابجا می شوند، با اطمینان از استحکام حفاظت اعمال‌شده، استفاده می‌کنید. جایی که ریسک قابل توجهی برای تاثیر برکارکرد عملکرد(های) ضروری به دلیل محدودیت منابع وجود دارد (مانند خرابی تجهیزات یا عمل انتقال، یا مسدود یا مختل شدن داده های مهم) مسیرهای انتقال جایگزین مناسبی در دسترس هستند. (مانند خرابی تجهیزات انتقال یا عملکرد، یا مسدود شدن یا مسدود شدن داده های مهم).

B3.c داده های ذخیره شده

شما ازکپی های نرم و سخت ذخیره شده داده های مهم برای عملکرد(های) ضروری خود محافظت کرده اید .

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است	تمام عبارات زیردرست است
شما اطلاعاتی درمورد مکان ذخیره داده های مهم برای عملکرد(های) ضروری ندارید یا محدود است. شما از داده های ذخیره شده آسیب پذیر که برای عملکرد(های) ضروری مهم هستند به روشی مناسب محافظت نکرده اید. پشتیبان‌گیری‌ها ناقص هستند، آزمایش نشده‌اند، به اندازه کافی امن نیستند یا در شرایط بازیابی فاجعه یا وضعیت تداوم کسب‌وکارغیرقابل دسترسی هستند.	همه کپی های داده های مهم برای عملکرد(های) ضروری شما لازم است. در جایی که این داده‌های مهم به سیستم‌هایی با امنیت کمتر منتقل می‌شوند، داده‌ها با جزئیات محدود و/یا به عنوان یک کپی فقط خواندنی ارائه می‌شوند. شما از ابزارهای فیزیکی و/یا فنی مناسب برای محافظت از این داده های ذخیره شده مهم در برابر دسترسی، تغییر یا حذف غیرمجازاستفاده کرده اید. اگر از محافظت های رمزنگاری استفاده می شود، ازابزارهای فنی و رویه ای مناسب استفاده می کنید، اما به استحکام حفاظت اعمال شده اعتماد محدودی دارید یا هیچ اطمینانی ندارید. درصورتی که داده های اصلی در دسترس نباشد شما دارای پشتیبان‌گیری مناسب و ایمن از داده‌ها هستید تا امکان ادامه عملکرد(های) ضروری فراهم باشد. این ممکن است شامل پشتیبان‌گیری آفلاین یا جدا، یا فرم‌های جایگزین مناسب مانند کپی‌های کاغذی باشد.	همه کپی های داده های مهم برای عملکرد(های) ضروری شما لازم است. در جایی که این داده‌های مهم به سیستم‌هایی با امنیت کمتر منتقل می‌شوند، داده‌ها با جزئیات محدود و/یا به عنوان یک کپی فقط خواندنی ارائه می‌شوند. شما از ابزارهای فیزیکی و/یا فنی مناسب برای محافظت ازاین داده های ذخیره شده مهم در برابر دسترسی، تغییر یا حذف غیرمجاز استفاده کرده اید. اگر از حفاظت های رمزنگاری استفاده می شود، از ابزارهای فنی و رویه ای مناسب استفاده می کنید، و به استحکام حفاظت اعمال شده اطمینان دارید. شما پشتیبان‌گیری مناسب و ایمن از داده‌ها دارید تا در صورت در دسترس نبودن داده‌های اصلی، عملکرد(های) ضروری ادامه یابد. این ممکن است شامل پشتیبان‌گیری آفلاین یا جدا، یا فرم‌های جایگزین مناسب مانند کپی‌های کاغذی باشد. داده های تاریخی یا بایگانی ضروری به طورمناسب درمحل های ذخیره سازی ایمن شده اند.

B3.d داده های قابل انتقال –سیار

شما از داده های مهم برای عملکرد(های) ضروری خود در دستگاه های قابل حمل محافظت کرده اید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
نمی‌دانید کدام دستگاه‌های قابل حمل ممکن است داده‌های مهم برای عملکرد(های) ضروری داشته باشند. به داده‌های مهم برای عملکرد(های) ضروری اجازه می‌دهید در دستگاه‌هایی که توسط سازمان شما یا حداقل با استانداردی معادل مدیریت نمی‌شوند، ذخیره شوند. داده های دستگاه های قابل حمل از نظر فنی ایمن نیستند یا فقط برخی از آنها ایمن هستند	شما می دانید کدام دستگاه های قابل حمل داده های مهم برای عملکرد(های) ضروری نگه می دارند. داده‌های مهم برای عملکرد(های) ضروری تنها زمانی در دستگاه‌های قابل حمل ذخیره می‌شوند که حداقل استاندارد امنیتی این دستگاه ها با خط‌مشی‌های امنیتی فراگیر شما مطابقت داشته باشند. داده های دستگاه های قابل حمل از نظر فنی ایمن هستند.	دستگاه‌های تلفن همراهی که داده های مهم عملکرد(های) ضروری را نگهداری می کنند، فهرست‌بندی می‌شوند، تحت کنترل سازمان شما هستند و بر اساس بهترین روش برای پلتفرم، با سیاست‌های فنی و رویه‌ای مناسب، پیکربندی می‌شوند. سازمان شما می‌تواند از راه دور همه دستگاه‌های قابل حمل را که داده‌های مهمی برای عملکرد(های) ضروری دارند پاک کند. شما این داده ها را در این دستگاه های قابل حمل به حداقل رسانده اید. برخی از داده ها ممکن است پس از یک دوره معین به طور خودکار از دستگاه های قابل حمل حذف شوند.

B3.e پاکسازی رسانه / تجهیزات

قبل از استفاده مجدد و/یا دور انداختن، دستگاه‌ها، تجهیزات و رسانه‌های قابل جابجایی حاوی داده‌های مهم برای عملکرد(های) ضروری خود را به طور مناسب پاکسازی کنید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
برخی یا همه دستگاه‌ها، تجهیزات یا رسانه‌های قابل جابجایی که داده‌های مهم برای عملکرد(های) ضروری را نگه می‌دارند، بدون پاکسازی آن داده‌ها مجدداً مورد استفاده قرار می‌گیرند یا دور ریخته می‌شوند.	داده های مهم برای عملیات عملکرد(های) ضروری قبل از استفاده مجدد و/یا دور ریختن از همه دستگاه ها، تجهیزات و رسانه های قابل جابجایی حذف می شوند.	همه دستگاه‌هایی که حاوی داده‌های مهم برای عملکرد(های) ضروری هستند (خواه یک دستگاه ذخیره‌سازی خاص یا یک دستگاه ذخیره‌سازی یکپارچه) را فهرست‌نویسی و ردیابی می‌کنید. داده‌های مهم برای عملکرد(های) ضروری قبل از استفاده مجدد و/یا با استفاده از محصول یا خدمات مطمئن از همه دستگاه‌ها، تجهیزات و رسانه‌های قابل جابجایی حذف می‌شوند.

اصل B4 امنیت سیستم

شبکه و سیستم های اطلاعاتی و فناوری حیاتی برای عملکردهای ضروری در برابر حملات سایبری محافظت می شوند. درک سازمانی از ریسک برای عملکردهای اساسی، استفاده از اقدامات امنیتی حفاظتی قوی و قابل اعتماد را برای محدود کردن موثر فرصت‌های مهاجمان برای به خطر انداختن شبکه‌ها و سیستم‌ها نشان می‌دهد.

B4.a ایمن با طراحی

شما امنیت را در شبکه و سیستم های اطلاعاتی طراحی می کنید که از عملکرد(های) ضروری شما پشتیبانی می کند. سطح حمله آن‌ها را به حداقل می‌رسانید و اطمینان می‌دهید که عملکرد(های) ضروری شما تحت تأثیر سوءاستفاده از هیچ آسیب‌پذیری قرار نگیرد.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
سیستم های ضروری برای عملکرد(های) ضروری به طور مناسب از سایر سیستم ها جدا نیستند. دسترسی به اینترنت از طریق شبکه و سیستم های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می کنند در دسترس است.	شما از تخصص مناسب برای طراحی شبکه و سیستم های اطلاعاتی استفاده می کنید. شما در جایی که شبکه و سیستم های اطلاعاتی شما با سایر سازمان ها یا جهان به طور کلی	شما از متخصصین مناسب برای طراحی شبکه و سیستم های اطلاعاتی استفاده می کنید. شبکه و سیستم‌های اطلاعاتی شما به مناطق امنیتی مناسب تفکیک شده‌اند (به عنوان مثال سیستم‌هایی که از عملکرد(های) ضروری پشتیبانی

جریان داده‌ها بین شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما و سایر سیستم‌ها پشتیبانی می‌کنند، پیچیده است، و تمایز قائل شدن بین ترافیک مجاز و نامجاز / مخرب را دشوار می‌سازد. دسترسی های از راه دور یا شخص ثالث برخی از کنترل های شبکه را دور می زند تا دسترسی مستقیم بیشتری به شبکه و سیستم های اطلاعاتی که از عملکرد(های) ضروری پشتیبانی می کنند، بدست آورند.	ارتباط برقرار می کنند، دفاع مرزی قوی طراحی می کنید. شما جریان های داده ساده ای را بین شبکه و سیستم های اطلاعاتی خود و هر رابط خارجی طراحی می کنید تا امکان نظارت موثر را فراهم کنید. شما طراحی می کنید تا بازیابی شبکه و سیستم اطلاعاتی را ساده کنید. تمام ورودی‌های شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، در حد امکان در مرز شبکه بررسی و تأیید می‌شوند، یا نظارت اضافی برای حملات مبتنی بر محتوا وجود دارد.	می‌کنند در یک منطقه بسیار قابل اعتماد و امن‌تر تفکیک شده‌اند). شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، به گونه‌ای طراحی شده‌اند که جریان داده‌های ساده‌ای را بین اجزا داشته باشند تا از نظارت مؤثر امنیتی پشتیبانی کنند. شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند به گونه‌ای طراحی شده‌اند که بازیابی آن آسان باشد. حملات مبتنی بر محتوا برای همه ورودی‌های شبکه و سیستم‌های اطلاعاتی که بر عملکرد(های) اساسی تأثیر می‌گذارند (به عنوان مثال از طریق تبدیل و بازرسی) کاهش می‌یابد.

B4.b پیکربندی امن

شما به طور ایمن شبکه و سیستم های اطلاعاتی را که از عملکرد(های) ضروری شما پشتیبانی می کنند، پیکربندی می کنید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
شما دارایی هایی را که برای حفظ امنیت عملکرد(های) ضروری باید به دقت پیکربندی شوند، شناسایی نکرده اید. خط‌مشی‌های مربوط به امنیت ساخت‌ها یا پیکربندی‌های سیستم عامل به طور مداوم در سراسر شبکه و سیستم‌های اطلاعاتی مرتبط با عملکرد(های) ضروری شما اعمال نمی‌شوند. جزئیات پیکربندی ثبت نشده یا فاقد اطلاعات کافی برای بازسازی سیستم یا دستگاه است.	شما دارایی هایی را که برای حفظ امنیت عملکرد(های) ضروری باید به دقت پیکربندی شوند، شناسایی و مستند کرده اید. پلت فرم ها و ساخت دستگاه امن در سراسر دارایی استفاده می شود. پیکربندی سیستم و دستگاه یکسان، ایمن و ساده در انواع محیط های مشابه اعمال می شود.	شما دارایی هایی را که برای حفظ امنیت عملکرد(های) ضروری باید به دقت پیکربندی شوند، شناسایی، مستند کرده و به طور فعال مدیریت کرده اید (مانند حفظ پیکربندی های امنیتی، وصله، به روز رسانی بر اساس روش خوب). همه پلتفرم‌ها با ساختار پایه ایمن و تعریف‌شده شما یا آخرین نسخه پیکربندی خوب شناخته شده برای آن محیط مطابقت دارند. شما از نزدیک و به طور موثر تغییرات را در محیط خود مدیریت می کنید، و

ضبط تغییرات یا تنظیمات امنیتی که بر عملکرد(های) ضروری شما تأثیر می گذارد، وجود ندارد یا متناقض است. حساب‌های عمومی، به اشتراک‌گذاشته شده، با نام پیشفرض و ازقبل ساخته شده حذف یا غیرفعال نشده است.	تغییرات و تنظیمات درپیکربندی امنیتی در مرزهای امنیتی با شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند تأیید و مستند شده‌اند. قبل ازمجاز بودن نصب، نرم افزار را تأیید می کنید. حساب‌های عمومی، به اشتراک‌گذاشته شده، با نام پیشفرض و از قبل ساخته شده حذف یا غیرفعال شده‌اند. در مواردی که این امکان وجود ندارد، دسترسی این حساب ها تغییرکرده است.	مطمئن می شوید که پیکربندی های شبکه و سیستم ایمن و مستند هستند. شما مرتباً بررسی و تأیید می کنید که شبکه و سیستم های اطلاعاتی شما دارای تنظیمات و پیکربندی ایمن و مورد انتظارهستند. فقط نرم افزارهای مجاز قابل نصب هستند. کاربران استاندارد قادر به تغییر تنظیماتی نیستند که بر امنیت یا عملیات تجاری تأثیربگذارد. اگر از فناوری‌های تصمیم‌گیری خودکار استفاده شود، عملکرد آنها به خوبی درک می‌شود و می‌توان تصمیم‌ها را برگرداند. حساب‌های عمومی، به اشتراک‌گذاشته شده، با نام پیشفرض و از قبل ساخته شده حذف یا غیرفعال شده‌اند. در مواردی که این امکان وجود ندارد، دسترسی این حساب ها تغییر کرده است

B4.cمدیریت امن

شما شبکه و سیستم های اطلاعاتی سازمان خود که ازعملکرد(های) ضروری شما پشتیبانی می کنند را مدیریت می کنید تا امنیت را فعال و حفظ کنید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است	تمام عبارات زیردرست است
سیستم‌ها و دستگاه‌های شما که از عملکرد(های) ضروری پشتیبانی می‌کنند، توسط دستگاه‌هایی که مالکیت و مدیریت شرکتی ندارند، مدیریت یا نگهداری می‌شوند. شما مستندات فنی خوب یا فعلی از شبکه و سیستم های اطلاعاتی خود ندارید.	سیستم‌ها و دستگاه‌های شما که از عملکردهای ضروری پشتیبانی می‌کنند، فقط توسط کاربران مجاز از دستگاه‌هایی که به اندازه کافی با استفاده از رویکرد مبتنی بر ریسک، از فعالیت‌های کاربران استاندارد، جدا شده‌اند، مدیریت یا نگهداری می‌شوند.	سیستم‌ها و دستگاه‌های شما که از عملکرد(های) ضروری پشتیبانی می‌کنند، فقط توسط کاربران مجاز مجاز از دستگاه‌های بسیارقابل اعتماد، مانند ایستگاه‌های کاری دسترسی ممتاز، که صرفاً به آن عملیات اختصاص داده شده است، مدیریت یا نگهداری می‌شوند.

	دانش فنی در مورد شبکه و سیستم های اطلاعاتی، مانند اسناد و نمودارهای شبکه، به طور مرتب بررسی و به روز می شود. شما از بدافزارها و نرم افزارهای غیرمجاز جلوگیری، و آن‌ها را شناسایی و حذف می کنید. در صورت لزوم از اقدامات فنی، رویه ای و فیزیکی استفاده می کنید.	شما به طور منظم دانش فنی در مورد شبکه و سیستم های اطلاعاتی مانند اسناد و نمودارهای شبکه را بررسی و به روز می کنید و از ذخیره ایمن آنها اطمینان می دهید. شما از بدافزارها و نرم افزارهای غیرمجاز جلوگیری، و آنها را شناسایی و حذف می کنید. در صورت لزوم از اقدامات فنی، رویه ای و فیزیکی استفاده می کنید.

B4.d. مدیریت آسیب پذیری

شما آسیب پذیری های شناخته شده را در شبکه و سیستم های اطلاعاتی خود مدیریت می کنید تا از تأثیر نامطلوب بر عملکرد(های) ضروری خود جلوگیری کنید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
شما میزان قرار گرفتن عملکرد(های) ضروری خود را در معرض آسیب پذیری های شناخته شده عمومی درک نمی کنید. شما آسیب‌پذیری‌های خارجی را به‌سرعت کاهش نمی‌دهید. شما اخیراً برای تأیید درک خود از آسیب‌پذیری‌های شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، آزمایش نکرده‌اید. سیستم‌ها یا نرم‌افزارهایی که دیگر پشتیبانی نمی‌شوند را به‌طور مناسب کاهش نداده‌اید. شما به دنبال جایگزینی برای سیستم ها یا نرم افزارهای پشتیبانی نشده نیستید	شما درک فعلی از قرار گرفتن عملکرد(های) ضروری خود در معرض آسیب پذیری های شناخته شده عمومی را حفظ می کنید. آسیب‌پذیری‌های اعلام‌شده برای همه بسته‌های نرم‌افزاری، شبکه و سیستم‌های اطلاعاتی که برای پشتیبانی از عملکرد(های) ضروری شما استفاده می‌شوند، ردیابی می‌شوند، اولویت‌بندی می‌شوند و آسیب‌پذیری‌های آشکار شده با راه حل قطعی خارجی به‌سرعت کاهش می‌یابند (مثلاً با وصله‌سازی). برخی از آسیب‌پذیری‌ها که آشکار شده با راه حل قطعی خارجی نیستند، کاهش‌های موقتی برای مدت طولانی دارند. در حین پیگیری مهاجرت به فناوری پشتیبانی شده، اقدامات کاهش موقتی برای سیستم ها و نرم افزارهای پشتیبانی نشده دارید. شما به طور منظم آزمایش می کنید تا آسیب پذیری های شبکه و سیستم های اطلاعاتی را که از عملکرد(های) ضروری شما پشتیبانی می کنند، به طور کامل درک کنید.	شما درک فعلی از قرار گرفتن عملکرد(های) ضروری خود در معرض آسیب پذیری های شناخته شده عمومی را حفظ می کنید. آسیب‌پذیری‌های اعلام‌شده برای همه بسته‌های نرم‌افزاری، شبکه و سیستم‌های اطلاعاتی که برای پشتیبانی از عملکرد(های) ضروری شما استفاده می‌شوند، به سرعت ردیابی، اولویت‌بندی و کاهش می‌یابند (مثلاً با وصله‌سازی). شما مرتباً آزمایش می‌کنید تا آسیب‌پذیری‌های شبکه و سیستم‌های اطلاعاتی را که از عملکرد(های) ضروری شما پشتیبانی می‌کنند کاملاً درک کنید و این درک را با آزمایش شخص ثالث تأیید کنید. شما استفاده از نرم افزار، سیستم عامل و سخت افزار پشتیبانی شده را در شبکه و سیستم های اطلاعاتی خود که از عملکرد(های) ضروری شما پشتیبانی می کنند، به حداکثر می رسانید.

اصل B5 شبکه ها و سیستم های انعطاف پذیر

سازمان در برابر حملات سایبری و شکست سیستم در طراحی، پیاده‌سازی، بهره‌برداری و مدیریت سیستم‌هایی که از عملکرد عملکردهای ضروری پشتیبانی می‌کنند، انعطاف‌پذیری ایجاد می‌کند.

B5.a آماده سازی انعطاف پذیری

شما آماده هستید تا عملکرد(های) ضروری خود را پس از تاثیر نامطلوب بازیابی کنید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
شما از تمام عناصر ضروری برای بازیابی عملکرد(ها) درک محدودی دارید. شما برنامه های تداوم کسب و کار و پوشش فاجعه را برای سیستم های شبکه و اطلاعات که از عملکرد(های) ضروری پشتیبانی می کند، از جمله وابستگی های آنها، تکمیل نکرده اید. شما اجرای عملی تداوم کسب و کار و طرح های بازیابی فاجعه را به طور کامل ارزیابی نکرده اید	شما تمام سیستم‌های شبکه و اطلاعات و فناوری‌های زیربنایی که برای بازگرداندن عملکرد(ها) ضروری است را می‌شناسید و وابستگی متقابل آنها را درک می کنید. شما می دانید که سیستم ها به چه ترتیبی باید بازیابی شوند تا به طور موثر و موثر عملکرد(های) ضروری را بازیابی کنند.	شما برنامه های تداوم کسب و کار و بازیابی فاجعه دارید که از نظر عملی بودن، اثربخشی و کامل بودن آزمایش شده اند. استفاده مناسب از روش های مختلف آزمون (مثلاً تیم قرمز) انجام می شود. شما از آگاهی امنیتی و منابع اطلاعاتی تهدید استفاده می کنید تا سطوح جدید یا افزایش یافته خطر را شناسایی کنید، که منجر به اقدامات امنیتی فوری و بالقوه موقت برای افزایش امنیت شبکه و سیستم های اطلاعاتی شما می شود (به عنوان مثال در پاسخ به شیوع گسترده بدافزار بسیار مخرب)..

B5.b طرحی برای انعطاف پذیری

شما شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند را طوری طراحی می‌کنید تا در برابر حوادث امنیت سایبری انعطاف پذیر باشند. سیستم ها به طور مناسب تفکیک شده و محدودیت های منابع کاهش می یابد.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
شبکه و سیستم‌های اطلاعاتی که از عملکرد (عملکردهای) ضروری شما پشتیبانی می‌کنند، به‌طور مناسبی تفکیک نشده‌اند. خدمات اینترنتی، مانند وب گردی و ایمیل، از طریق شبکه و سیستم های اطلاعاتی که از عملکرد(های) ضروری پشتیبانی می کنند، قابل دسترسی هستند. شما در مورد کاهش همه محدودیت های منابعی که می تواند بر عملکرد(های) ضروری شما تاثیر منفی داشته باشد بی اطلاع هستید یا برای آن برنامه ای ندارید	شبکه و سیستم های اطلاعاتی که از عملکرد (های) ضروری شما پشتیبانی می کنند، به طور منطقی از کسب و کار شما جدا هستند سیستم ها (به عنوان مثال، آنها درهمان شبکه با بقیه سازمان اما در یک DMZ قرار دارند). خدمات اینترنتی از طریق شبکه و سیستم های اطلاعاتی که از عملکرد(های) ضروری پشتیبانی می کنند، قابل دسترسی نیستند. محدودیت های منابع (به عنوان مثال پهنای باند شبکه، مسیرهای تک شبکه) شناسایی شده اند اما به طورکامل کاهش نیافته اند.	شبکه‌ها و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند با ابزارهای فنی و فیزیکی مناسب (به عنوان مثال جداسازی زیرساخت سیستم و شبکه با مدیریت کاربر مستقل)، از دیگر سیستم های تجاری و خارجی جدا می‌شوند. خدمات اینترنتی از طریق شبکه و سیستم های اطلاعاتی که از عملکرد(های) ضروری پشتیبانی می کنند، قابل دسترسی نیستند. شما تمام محدودیت های منابع (مانند محدودیت های پهنای باند و مسیرهای تک شبکه) را شناسایی و کاهش داده اید. شما هر گونه محدودیت یا ضعف جغرافیایی را شناسایی و کاهش داده اید. (به عنوان مثال سیستم هایی که عملکرد(های) ضروری شما به آنها وابسته است در مکان دیگری تکرار می شوند، اتصال شبکه مهم دارای مسیرهای فیزیکی و ارائه دهندگان خدمات جایگزین است). ارزیابی‌های وابستگی‌ها، محدودیت‌های منابع و جغرافیایی و کاهش‌ها را در صورت لزوم بررسی و به‌روزرسانی می‌کنید.

B5.c پشتیبان گیری

شما نسخه‌های پشتیبان فعلی قابل دسترسی و ایمن از داده‌ها و اطلاعات مورد نیاز برای بازیابی عملکرد(های) ضروری خود را نگهداری می‌کنید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
پوشش پشتیبان‌گیری ناقص است و شامل تمام داده‌ها و اطلاعات مرتبط مورد نیاز برای بازیابی عملکرد(های) ضروری شما نمی‌شود. پشتیبان گیری به اندازه کافی تکرار نمی شود تا عملکرد(های) ضروری شما به طور موثر بازیابی شود. فرآیند بازیابی شما عملکرد(های) ضروری شما را در یک بازه زمانی مناسب بازیابی نمی کند	شما از پشتیبان‌گیری (شامل داده‌ها، اطلاعات پیکربندی، نرم‌افزار، تجهیزات، فرآیندها و دانش) به نحوی مناسب محافظت کرده‌اید. این پشتیبان‌ها برای بازیابی از یک رویداد شدید قابل دسترسی خواهند بود. شما به طور معمول نسخه‌های پشتیبان را آزمایش می‌کنید تا مطمئن شوید که عملکرد(های) فرآیند پشتیبان‌گیری صحیح و پشتیبان‌گیری‌ها قابل استفاده هستند.	پشتیبان‌گیری‌های فنی و رویه‌ای جامع، خودکار و آزمایش‌شده شما در سایت‌های قابل دسترسی مرکزی یا ثانویه برای بازیابی از یک رویداد شدید ایمن می‌شوند. پشتیبان گیری از تمام داده ها و اطلاعات مهم مورد نیاز برای بازیابی عملکرد(های) ضروری ساخته، آزمایش، مستند شده و به طور معمول بررسی می شود.

اصل B6 آگاهی و آموزش کارکنان

کارکنان از آگاهی، دانش و مهارت های مناسبی برخوردارند تا نقش های سازمانی خود را به طور موثر در رابطه با امنیت شبکه و سیستم های اطلاعاتی که از عملکرد عملکردهای اساسی پشتیبانی می کنند، انجام دهند.

B6.a فرهنگ امنیت سایبری

شما یک فرهنگ امنیت سایبری مثبت را توسعه داده و حفظ می کنید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
افراد در سازمان شما نمی دانند که چه چیزی به امنیت سایبری عملکرد(های) ضروری کمک می کنند. افراد در سازمان شما نمی دانند که چگونه در مورد امنیت سایبری شما به طور معمول نسخه‌های پشتیبان را آزمایش می‌کنید تا مطمئن شوید که عملکرد(های) فرآیند پشتیبان‌گیری صحیح و پشتیبان‌گیری‌ها قابل استفاده هستند.کنند. مردم بر این باورند که مشکلات گزارش ممکن است آنها را با مشکل مواجه کند. رویکرد سازمان شما به امنیت سایبری توسط کارکنان به عنوان مانع کسب و کار سازمان تلقی می شود.	مدیریت اجرایی شما اهمیت فرهنگ امنیت سایبری مثبت را درک کرده و به طور گسترده ای با آنها ارتباط برقرار می کند. نگرش ها، رفتارها و انتظارات مثبت برای سازمان شما شرح داده شده است. همه افراد در سازمان شما مشارکت در عملکرد(های) ضروری امنیت سایبری را درک می کنند. همه افراد در سازمان شما می دانند که با چه کسی تماس بگیرند و از کجا به اطلاعات بیشتر در مورد امنیت سایبری دسترسی داشته باشند. آنها می دانند که چگونه یک مسئله امنیت سایبری را مطرح کنند.	مدیریت اجرایی شما به طور واضح و موثر اولویت ها و اهداف امنیت سایبری سازمان را به همه کارکنان منتقل می کند. سازمان شما نگرش ها، رفتارها و انتظارات امنیت سایبری مثبتی را نشان می دهد. با افرادی که در سازمان شما حوادث و مسائل احتمالی امنیت سایبری را مطرح می کنند، برخورد مثبتی صورت می گیرد. افراد در تمام سطوح سازمان شما به طور معمول نگرانی‌ها یا مسائل مربوط به امنیت سایبری را گزارش می‌کنند و به دلیل مشارکت در حفظ امنیت سازمان شناخته می‌شوند. دیده می شود که مدیریت شما متعهد به امنیت سایبری است و فعالانه در آن مشارکت دارد. سازمان شما آشکارا در مورد امنیت سایبری ارتباط برقرار می کند و هر گونه نگرانی جدی گرفته می شود. افراد در سراسر سازمان شما در فعالیت‌ها و بهبودهای امنیت سایبری شرکت می‌کنند، مالکیت مشترک ایجاد می‌کنند و دانش حوزه تخصصی خود را ارائه می دهند.

B6.b آموزش امنیت سایبری

افرادی که از عملکرد(های) ضروری شما پشتیبانی می کنند، به طور مناسب در زمینه امنیت سایبری آموزش دیده اند.
طیف وسیعی از رویکردها برای آموزش امنیت سایبری، آگاهی و ارتباطات به کار گرفته شده است.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
تیم هایی که عملکرد(های) ضروری شما را اداره و پشتیبانی می کنند فاقد هرگونه آموزش امنیت سایبری هستند. آموزش امنیت سایبری به نقش های خاصی در سازمان شما محدود می شود. سوابق آموزشی امنیت سایبری برای سازمان شما وجود ندارد یا ناقص است	شما آموزش و فعالیت‌های آگاهی‌بخشی امنیت سایبری را برای همه نقش‌ها در سازمانتان، از مدیران اجرایی گرفته تا جوان‌ترین نقش‌ها، تعریف کرده‌اید. شما از طیف وسیعی از تکنیک های آموزشی و ارتباطی برای آموزش و فعالیت‌های آگاهی‌بخشی امنیت سایبری استفاده می کنید تا به طور موثر به گسترده ترین مخاطبان دسترسی پیدا کنید. اطلاعات امنیت سایبری به راحتی در دسترس است.	همه افراد در سازمان شما، از مسن ترین تا جوان ترین، مسیرهای آموزش امنیت سایبری مناسب را دنبال می کنند. آموزش امنیت سایبری هر فرد در فواصل زمانی مناسب ردیابی و به روز می شود. شما به طور معمول فعالیت‌های آموزش و فعالیت‌های آگاهی‌بخشی امنیت سایبری خود را ارزیابی می‌کنید تا اطمینان حاصل کنید که آنها به وسیع‌ترین مخاطبان دسترسی دارند و مؤثر هستند. در سازمان شما طلاعات امنیت سایبری و راهنمایی‌های عملکرد خوب به راحتی در دسترس و به طور گسترده قابل استفاده بوده و می‌دانید که مورد استفاده قرار می گیرند.

CAF - هدف C - تشخیص رویدادهای امنیت سایبری

قابلیت‌هایی برای اطمینان از مؤثر ماندن دفاع‌های امنیتی و شناسایی تاثیرگذاری یا تاثیر بالقوه رویدادهای امنیت سایبری بر عملکرد(های) ضروری وجود دارد.

اصل C1 نظارت بر امنیت

سازمان وضعیت امنیتی شبکه و سیستم‌های اطلاعاتی را که از عملکردهای ضروری پشتیبانی می‌کنند، نظارت می‌کند تا مشکلات امنیتی احتمالی را شناسایی کند و اثربخشی مداوم اقدامات امنیتی حفاظتی را پیگیری کند.

C1.a پوشش نظارتی

منابع داده ای که در نظارت خود لحاظ می کنید، امکان شناسایی به موقع رویدادهای امنیتی که ممکن است بر عملکرد(های) ضروری شما تأثیر بگذارد را فراهم می کند.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
داده های مربوط به امنیت و اداره عملکرد(های) ضروری شما جمع آوری نمی شود. شما با اطمینان وجود یا عدم وجود شاخص های تهدید (IoC) را در عملکرد(های) ضروری خود، مانند امضاهای مخرب فرمان و کنترل شناخته شده شناسایی نمی کنید (زیرا استفاده از نشانگر مشکل است یا داده های گزارش شما به اندازه کافی دقیق نیست). شما نمی توانید فعالیت های کاربران را در رابطه با عملکرد(های) ضروری خود ممیزی کنید. شما هیچ ترافیکی را که از مرز شبکه خود عبور می کند، از جمله حداقل اتصالات IP، ضبط نمی کنید	داده‌های مربوط به امنیت و عملکرد برخی از بخش های عملکرد(های) ضروری شما جمع‌آوری شده است، اما پوشش جامع نیست. شما به راحتی وجود یا عدم وجود IoCها را در عملکرد(های) ضروری خود، مانند امضای فرمان و کنترل مخرب شناخته شده، تشخیص می دهید. برخی از نظارت های کاربر انجام شده است، اما همه موارد رفتار مشکوک یا نامطلوب را پوشش نمی دهد. شما ترافیک عبوری از مرز شبکه خود را (از جمله اتصالات آدرس IP به عنوان حداقل) نظارت می کنید.	مانیتورینگ مبتنی است بر درک شبکه های شما، روش های رایج حمله سایبری و آنچه شما نیاز به آگاهی دارید تا حوادث امنیتی احتمالی که می توانند بر عملکرد(های) اساسی ما تأثیر بگذارند شناسایی شوند (مانند وجود بدافزار، ایمیل های مخرب، نقض خط مشی کاربر) داده‌های نظارت شما جزئیات کافی را برای شناسایی مطمئن حوادث امنیتی که می‌تواند بر عملکرد(های) ضروری شما تأثیر بگذارد، ارائه می‌کند. شما به راحتی وجود یا عدم وجود IoCها را در عملکرد(های) ضروری خود، مانند امضای فرمان و کنترل مخرب شناخته شده، تشخیص می دهید. نظارت گسترده بر فعالیت کاربر در رابطه با عملکرد(های) ضروری شما به شما امکان می دهد نقض خط مشی ها و لیست توافق شده ای از رفتارهای مشکوک یا نامطلوب را شناسایی کنید. شما پوشش نظارتی گسترده ای دارید که شامل مانیتورینگ مبتنی برمیزبان و دروازه های شبکه می باشد. تمام سیستم های جدید به عنوان منابع داده نظارتی بالقوه برای حفظ قابلیت نظارت جامع در نظر گرفته می شوند

C1.b امن سازی لاگ ها

شما داده‌های گزارش را ایمن نگه می‌دارید و فقط به حساب‌هایی که نیازکاری دارند، دسترسی مناسب می‌دهید. هیچ سیستم یا کاربری نباید نیازبه تغییریا حذف نسخه های اصلی داده های گزارش دریک دوره نگهداری توافق شده داشته باشد و پس ازآن باید حذف شود.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است	تمام عبارات زیردرست است
این امکان وجود دارد که داده های گزارش به راحتی توسط کاربران غیرمجاز یا مهاجمان مخرب ویرایش یا حذف شوند هیچ لیست کنترل شده ای از کاربران و سیستم هایی که می توانند داده های گزارش را مشاهده و جستجو کنند وجود ندارد. هیچ نظارتی بر دسترسی به داده های گزارش وجود ندارد. هیچ سیاستی برای دسترسی به داده های گزارش وجود ندارد. داده‌های گزارش با استفاده از یک منبع زمانی مشترک دقیق، همگام‌سازی نمی‌شوند	فقط کارکنان مجاز می توانند داده های گزارش را برای بررسی مشاهده کنند. کاربران و سیستم های مجاز می توانند به طور مناسب به داده های گزارش دسترسی داشته باشند. برخی نظارت بردسترسی به داده های گزارش وجود دارد (مانند کپی، حذف، تغییریا مشاهده).	یکپارچگی داده های گزارش محافظت می شود، یا هرگونه تغییری شناسایی و نشان داده می شود. معماری لاگ دارای مکانیسم‌ها، سیاست‌ها، فرآیندها و رویه‌هایی است تا اطمینان حاصل کند که می‌تواند خود را در برابر تهدیدهایی که می‌خواهد شناسایی کند، محافظت کند. این شامل محافظت از خود عملکرد(های) ضروری و داده های درون آن می شود. تجزیه و تحلیل و عادی سازی داده های گزارش فقط روی کپی هایی از داده ها انجام می شود که نسخه اصلی را بدون تغییرنگه می دارد. داده‌های گزارش با استفاده از یک منبع زمانی مشترک دقیق همگام‌سازی می‌شوند، به طوری که مجموعه داده‌های جداگانه را می‌توان به روش‌های مختلف مرتبط کرد. دسترسی به داده‌های گزارش به کسانی که نیاز کاری دارند محدود است و نه دیگران. همه اقدامات مربوط به تمام داده های گزارش (مانند کپی، حذف، اصلاح یا مشاهده) را می توان برای یک کاربر منحصربه فرد ردیابی کرد. دلایل قانونی برای دسترسی به داده های گزارش درخط مشی های استفاده ذکرشده است.

C1.c ایجاد هشدارها

شواهد مربوط به حوادث امنیتی بالقوه موجود در داده های نظارتی شما به طور معتبر شناسایی شده و هشدارها را راه اندازی می کند.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
هشدارهای نرم افزارهای امنیتی شخص ثالث بررسی نمی شوند (مثلاً ارائه دهندگان آنتی ویروس (AV)). گزارش‌ها در بین دستگاه‌ها توزیع می‌شوند و هیچ راه آسانی برای دسترسی به آنها غیر از ورود به سیستم به صورت دستی یا اقدام فیزیکی وجود ندارد. اقدامی جهت تحلیل هشدارهای دارایی یا سیستم شبکه انجام نمی شود. هشدارهای امنیتی مربوط به عملکرد(های) ضروری در اولویت قرار ندارند. گزارش ها به ندرت بررسی می شوند	هشدارهای نرم افزارهای امنیتی شخص ثالث بررسی می شوند و اقدامات لازم انجام می شود. برخی، اما نه همه، داده های گزارش را می توان به راحتی با ابزارهای جستجو برای کمک به تحقیقات جستجو کرد. تحلیل هشدارهای دارایی یا سیستم شبکه به طور منظم انجام می شود. هشدارهای امنیتی مربوط به برخی عملکرد(های) ضروری در اولویت قرار دارند. گزارش‌ها در فواصل منظم بررسی می‌شوند	هنگام بررسی فعالیت‌ها یا هشدارهای مشکوک، داده‌های گزارش با دیگر دانش و داده‌های شبکه غنی می‌شوند. طیف گسترده ای از امضاها و شاخص های تهدید برای بررسی فعالیت های مشکوک و هشدارها استفاده می شود. هشدارهای دارای های شبکه را می توان به راحتی با استفاده از دانش شبکه ها و سیستم ها رفع کرد. رفع این هشدارها تقریباً در لحظه انجام می شود. هشدارهای امنیتی مربوط به همه عملکرد(های) ضروری اولویت بندی می شوند و این اطلاعات برای پشتیبانی از مدیریت حادثه استفاده می شود. گزارش‌ها تقریباً به طور مداوم و در زمان واقعی بررسی می‌شوند. هشدارها برای اطمینان از اینکه به طور قابل اعتماد تولید می شوند و امکان تشخیص حوادث امنیتی واقعی از هشدارهای کاذب وجود دارد آزمایش می شوند.

C1.d شناسایی حوادث امنیتی

شما هشدارها را با آگاهی از تهدید و سیستم های خود، برای شناسایی حوادث امنیتی که نیاز به نوعی واکنش دارند، می سازید.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
سازمان شما هیچ منبع اطلاعاتی تهدید ندارد. شما پس از دریافت به‌روزرسانی‌ها را به‌موقع اعمال نمی‌کنید (مثلاً به‌روزرسانی‌های امضای AV، سایر امضاهای تهدید یا شاخص‌های تهدید (IoC)). شما به‌روزرسانی‌های امضایی را برای همه فناوری‌های حفاظتی مانند AV و IDS یا سایر نرم‌افزارهای در حال استفاده دریافت نمی‌کنید. شما قابلیت استفاده از اطلاعات تهدید خود را ارزیابی نمی کنید یا بازخورد خود را با ارائه دهندگان یا سایر کاربران به اشتراک نمی گذارید.	سازمان شما از برخی از سرویس‌های اطلاعاتی تهدید استفاده می‌کند، اما شما لزوماً منابع یا ارائه‌دهندگان را به‌خاطر نیازهای تجاری خود یا تهدیدهای خاص در بخش خود انتخاب نمی‌کنید (مانند اشتراک‌گذاری اطلاعات مبتنی بر بخش، فروشندگان نرم‌افزار ICS، ارائه‌دهندگان ضد ویروس، اطلاعات تهدید تخصصی شرکت ها، گروه های ذینفع خاص). شما به‌روزرسانی‌هایی را برای همه فناوری‌های حفاظتی مبتنی بر امضا (مانند AV، IDS) دریافت می‌کنید. شما برخی به روز رسانی ها، امضاها و IoC ها را به موقع اعمال می کنید. شما می دانید که اطلاعات تهدید شما چقدر موثر است (به عنوان مثال با ردیابی اینکه چگونه اطلاعات تهدید به شما در شناسایی مشکلات امنیتی کمک می کند).	شما منابع یا سرویس‌های اطلاعاتی تهدید را با استفاده از تصمیم‌های مبتنی بر ریسک و مبتنی بر تهدید بر اساس نیازهای تجاری و بخش خود انتخاب کرده‌اید (مثلاً گزارش‌دهی و وصله‌سازی فروشنده، ارائه‌دهندگان قوی ضد ویروس، اشتراک‌گذاری اطلاعات مبتنی بر بخش و جامعه، گروه‌های ذینفع خاص). شما همه امضاها و IoCهای جدید را در یک زمان معقول (مبتنی برریسک) پس از دریافت آنها اعمال می کنید. شما به‌روزرسانی‌های امضا را برای همه فناوری‌های محافظتی خود (مانند AV، IDS) دریافت می‌کنید. شما کارآمدی فیدهای اطلاعاتی خود را دنبال می کنید و بازخوردهای مفیدی از IoC و هر شاخص دیگری را با جامعه تهدید (به عنوان مثال شرکای بخش، ارائه دهندگان اطلاعات تهدید، سازمان های دولتی) به اشتراک می گذارید.

C1.e ابزارها و مهارت های نظارتی

نظارت بر مهارت‌ها، ابزارها و نقش‌های کارکنان، از جمله مواردی که برون‌سپاری می‌شوند، باید منعکس‌کننده الزامات حاکمیتی و گزارش‌دهی، تهدیدات مورد انتظار و پیچیدگی‌های شبکه یا داده‌های سیستمی باشد که آنها باید استفاده کنند. کارکنان ناظر از عملکرد(های) اساسی که باید محافظت کنند، آگاهی دارند.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
هیچ کارمندی وجود ندارد که وظیفه نظارت را انجام دهد. کارکنان مانیتورینگ مهارت های تخصصی درستی ندارند. کارکنان ناظر قادر به گزارش در برابر الزامات حاکمیتی نیستند. کارکنان مانیتورینگ فاقد مهارت لازم برای اجرای موفقیت آمیز بخش های مهم جریان کار تعریف شده هستند. ابزارهای مانیتورینگ فقط می توانند از کسری از داده های گزارش جمع آوری شده استفاده کنند. ابزارهای مانیتورینگ را نمی توان برای استفاده از جریان های گزارش جدید پیکربندی کرد، زیرا آنها آنلاین هستند. کارکنان ناظر از عملکرد(های) اساسی که سازمان ارائه می دهد، دارایی های مربوط به آن کارکردها و ازاین رو اهمیت داده های گزارش و رویدادهای امنیتی آگاهی ندارند.	کارکنان مانیتورینگ دارای برخی مهارت‌های تحقیقی و درک اولیه از داده‌هایی هستند که باید با آنها کار کنند. کارکنان نظارت می توانند به سایر بخش های سازمان (به عنوان مثال مدیران امنیتی، مدیران تاب آوری) گزارش دهند. کارکنان مانیتورینگ قادر به پیروی از اکثر جریان های کاری مورد نیاز هستند. ابزارهای نظارتی شما می‌توانند از گزارش‌گیری استفاده کنند که می‌تواند انواع حملات غیرپیچیده و غیرهدفمند را به تصویر بکشد. ابزارهای نظارتی شما با انجام برخی تنظیمات با اکثر داده‌های گزارش کار می‌کنند. کارکنان نظارت از برخی عملکرد(های) ضروری آگاه هستند و می توانند هشدارهای مربوط به آنها را مدیریت کنند.	شما کارکنان نظارتی دارید که مسئول تجزیه و تحلیل، بررسی و گزارش هشدارهای نظارتی هستند که هم امنیت و هم عملکرد را پوشش می دهند. کارکنان نظارت، نقش ها و مهارت هایی را تعریف کرده اند که تمام بخش های فرآیند نظارت و تحقیق را پوشش می دهد. کارکنان ناظر از سیاست ها، فرآیندها و رویه هایی پیروی می کنند که تمامی الزامات گزارش دهی حاکمیتی، داخلی و خارجی را مورد توجه قرار می دهد. کارکنان ناظر این اختیار را دارند که با توسعه تکنیک‌های تحقیقی خود و استفاده جدید از داده‌ها، فراتر از فرآیند ثابت برای بررسی و درک تهدیدات غیر استاندارد نگاه کنند. ابزارهای نظارتی شما از تمام داده‌های گزارش جمع‌آوری‌شده برای مشخص کردن دقیق فعالیت در یک حادثه استفاده می‌کنند. کارکنان و ابزارهای نظارتی مجموعه داده های گزارش جدید را هدایت و شکل می دهند و می توانند از آن استفاده گسترده ای کنند. کارکنان ناظر از عملکرد (های) ضروری و دارایی های مرتبط آگاه هستند و می توانند هشدارها با تحقیقات مربوط به آنها را شناسایی و اولویت بندی کنند.

اصل C2 کشف رویداد امنیتی پیشگیرانه

سازمان، در داخل شبکه و سیستم‌های اطلاعاتی، فعالیت مخربی را شناسایی می‌کند که بر عملکردهای اساسی تأثیر می‌گذارد یا بالقوه برآن تأثیر می‌گذارد، حتی زمانی که فعالیت با راه‌حل‌های پیشگیری/تشخیص امنیت مبتنی برامضای استاندارد مطابقت ندارد (یا زمانی که راه‌حل‌های استاندارد قابل اجرا نیستند).

C2.a اختلالات سیستم برای تشخیص حمله

شما نمونه‌هایی از ناهنجاری‌ها را دررفتارسیستم تعریف می‌کنید که راه‌های عملی برای شناسایی فعالیت‌های مخرب را ارائه می‌دهند که شناسایی آن‌ها درغیراین صورت دشواراست.

محقق نشده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است
رفتارعادی سیستم به اندازه کافی درک نشده است تا بتوان از ناهنجاری های سیستم برای شناسایی فعالیت های مخرب استفاده کرد. شما هیچ درک ثابتی از اینکه به دنبال چه ناهنجاری هایی باشید که ممکن است به معنای فعالیت های مخرب باشد، ندارید.	رفتارعادی سیستم تا حدی کاملاً درک شده است که جستجوی ناهنجاری‌های سیستم یک راه بالقوه مؤثر برای شناسایی فعالیت‌های مخرب است (به عنوان مثال، شما کاملاً می‌دانید که چه سیستم‌هایی باید و چه زمانی نباید ارتباط برقرارکنند). توصیف ناهنجاری های سیستم از حملات گذشته و اطلاعات تهدید، در شبکه های شما و سایر شبکه ها، برای نشان دادن فعالیت های مخرب استفاده می شود. ناهنجاری‌های سیستمی که جستجو می‌کنید، ماهیت حملاتی را در نظر می‌گیرند که احتمالاً بر شبکه و سیستم‌های اطلاعاتی که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، تأثیر می‌گذارند. توصیف‌های غیرعادی سیستمی که استفاده می‌کنید به‌روزرسانی می‌شوند تا تغییرات شبکه و سیستم‌های اطلاعاتی شما و اطلاعات تهدید فعلی را منعکس کنند

C2.b کشف حمله پیشگیرانه

شما از یک درک آگاهانه از روش های حمله پیچیده تر و رفتار عادی سیستم برای نظارت پیشگیرانه برای فعالیت های مخرب استفاده می کنید.

محقق نشده	محقق شده
حداقل یکی ازعبارات زیردرست است	تمام عبارات زیردرست است
شما به طور معمول برای ناهنجاری های سیستمی که نشان دهنده فعالیت های مخرب هستند جستجو نمی کنید.	شما به طور معمول ناهنجاری‌های سیستمی را جستجو می‌کنید که نشان‌دهنده فعالیت مخرب در شبکه و سیستم‌های اطلاعاتی است که از عملکرد(های) ضروری شما پشتیبانی می‌کنند، و براساس نتایج این جستجوها هشدارهایی ایجاد می‌کنید. شما نسبت به اثربخشی جستجوهای خود برای ناهنجاری‌های سیستمی که نشان‌دهنده فعالیت مخرب هستند، اطمینان موجهی دارید.

CAF – هدف D – به حداقل رساندن تأثیر حوادث امنیت سایبری

قابلیت‌هایی برای به حداقل رساندن تأثیر نامطلوب یک حادثه امنیت سایبری بر عملکردهای ضروری، از جمله بازگرداندن آن عملکرد(ها) درصورت لزوم وجود دارد.

اصل D1 برنامه ریزی پاسخگویی و بازیابی

فرآیندهای مدیریت حادثه به خوبی تعریف شده و آزمایش شده وجود دارد که هدف آن تضمین تداوم عملکرد(های) ضروری درصورت خرابی سیستم یا سرویس است. فعالیت‌های کاهشی که برای مهار یا محدود کردن تأثیر تهدید طراحی شده‌اند نیز وجود دارند.

D1.a طرح پاسخ

شما یک طرح واکنش به حادثه به روز دارید که مبتنی بر ارزیابی ریسک کامل است که عملکرد(های) ضروری شما را در نظر می گیرد و طیف وسیعی از سناریوهای حادثه را پوشش می دهد.

محقق نشده	تا حدی محقق شده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است	تمام عبارات زیر درست است
طرح واکنش به حادثه شما مستند نیست. طرح واکنش به حادثه شما شامل عملکرد(های) ضروری شناسایی شده سازمان شما نمی شود. طرح واکنش به حادثه شما توسط کارکنان مربوطه به خوبی درک نشده است.	طرح واکنش به حادثه شما عملکرد(های) ضروری شما را پوشش می دهد. طرح پاسخ به حادثه شما به طور جامع سناریوهایی را پوشش می دهد که فقط بر تأثیرات احتمالی حملات شناخته شده و کاملاً درک شده متمرکز هستند. طرح واکنش به حادثه شما توسط همه کارکنانی که با عملکرد واکنش سازمان شما درگیر هستند درک می شود. طرح واکنش به حادثه شما مستند شده و با همه ذینفعان مرتبط به اشتراک گذاشته شده است.	طرح پاسخ به حادثه شما بر اساس درک روشنی از خطرات امنیتی شبکه و سیستم های اطلاعاتی است که از عملکرد(های) ضروری شما پشتیبانی می کند. طرح پاسخ به حادثه شما جامع است (یعنی چرخه کامل یک حادثه، نقش ها و مسئولیت ها و گزارش را پوشش می دهد) و اثرات احتمالی هر دو الگوی حمله شناخته شده و حملات احتمالی را که قبلاً دیده نشده اند، پوشش می دهد. طرح واکنش به حادثه شما مستند شده و با طرح‌های تجاری سازمانی گسترده‌تر و طرح‌های واکنش زنجیره تامین، و همچنین وابستگی‌ها به زیرساخت‌های پشتیبانی (مانند برق، سرمایش و غیره) یکپارچه شده است. طرح واکنش به حادثه شما توسط حوزه‌های تجاری مرتبط با عملکرد(های) ضروری شما اطلاع رسانی و درک می‌شود.

D1.b قابلیت پاسخ و بازیابی

شما قادر به استفاده از طرح واکنش به حادثه ای هستید که شامل محدودیت قابل اجرا روی تاثیر بر عملکرد(های) ضروری می باشد. در طول یک حادثه، شما به اطلاعات به موقع دسترسی دارید که بر اساس آن تصمیمات خود را در مورد پاسخ اتخاذ می کنید.

محقق نشده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است
ترتیبات ناکافی برای در دسترس قرار دادن منابع مناسب برای اجرای طرح پاسخ شما انجام شده است. اعضای تیم پاسخگویی شما برای اتخاذ تصمیمات پاسخگویی مناسب و اجرای آنها مجهز نیستند. مکانیسم‌های پشتیبان نامناسبی برای ادامه عملکرد(های) ضروری شما را در طول یک حادثه وجود دارد.	شما منابعی را که احتمالاً برای انجام هر گونه فعالیت پاسخگویی ضروری نیاز خواهد بود، درک می کنید و ترتیباتی برای در دسترس قرار دادن این منابع در نظر گرفته شده است. شما متوجه انواع اطلاعاتی هستید که احتمالاً برای اطلاع رسانی در مورد تصمیمات پاسخگویی مورد نیاز است و ترتیبات لازم برای در دسترس قرار دادن این اطلاعات وجود دارد. اعضای تیم پاسخ شما مهارت ها و دانش لازم برای تصمیم گیری در مورد اقدامات پاسخ لازم برای محدود کردن آسیب، و اختیار انجام آنها را دارند. نقش‌های کلیدی تکراری هستند و دانش تحویل عملیاتی با تمام افرادی که در عملیات و بازیابی عملکرد(های) ضروری مشارکت دارند به اشتراک گذاشته می‌شود. مکانیزم‌های پشتیبان‌گیری در دسترس هستند که می‌توانند به آسانی فعال شوند تا در صورت خرابی یا در دسترس نبودن شبکه اولیه و سیستم‌های اطلاعاتی، امکان ادامه عملکرد(های) ضروری شما، هرچند احتمالاً در سطح کاهش‌یافته، فراهم شود. تمهیداتی وجود دارد که در صورت لزوم، قابلیت‌های پاسخگویی به حوادث سازمان شما را با پشتیبانی خارجی افزایش می‌دهد (مثلاً پاسخگویان متخصص حوادث سایبری).

D1.c تست و تمرین

سازمان شما تمرین‌هایی را برای آزمایش طرح‌های واکنش انجام می‌دهد، با استفاده از حوادث گذشته که بر سازمان شما (و سایرین) تأثیر گذاشته است، و سناریوهایی که بر اطلاعات تهدید و ارزیابی ریسک شما مبتنی است.

محقق نشده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است
تمرین‌ها فقط بخش مجزایی از فرآیند را آزمایش می‌کنند (مثلاً پشتیبان‌گیری‌ها کار می‌کنند)، اما همه بخش‌ها را در نظر نمی‌گیرند. تمرین‌های واکنش به حادثه به‌طور معمول انجام نمی‌شوند یا به‌صورت موقتی انجام می‌شوند. خروجی‌های تمرین‌ها به فرآیند درس‌های آموخته‌شده سازمان وارد نمی‌شوند. تمرین ها همه بخش های چرخه پاسخ را آزمایش نمی کنند.	سناریوهای تمرین بر اساس حوادثی هستند که توسط شما و سایر سازمان‌ها تجربه شده‌اند یا با استفاده از تجربه یا اطلاعات تهدید ساخته شده‌اند. سناریوهای تمرین مستند، مرتباً بررسی و تأیید می شوند. تمرین‌ها به‌طور معمول اجرا می‌شوند و یافته‌ها مستند شده و برای اصلاح طرح‌های واکنش به حادثه و امنیت حفاظتی، مطابق با درس‌های آموخته شده استفاده می‌شوند. تمرین‌ها تمام بخش‌های چرخه پاسخ شما را که به عملکرد(های) ضروری شما مربوط می‌شود (به عنوان مثال بازگرداندن سطوح عملکرد(های) طبیعی) آزمایش می‌کنند.

اصل D2 درس‌های آموخته شده

هنگامی که یک حادثه رخ می دهد، اقدامات لازم برای درک علل اصلی آن و اطمینان از انجام اقدامات اصلاحی مناسب برای محافظت در برابر حوادث آینده انجام می شود.

D2.a تجزیه و تحلیل علت اصلی حادثه

هنگامی که یک حادثه رخ می دهد، باید اقدامات لازم برای درک علل اصلی آن و اطمینان از انجام اقدامات اصلاحی مناسب انجام شود.

محقق نشده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است
شما معمولا قادر به حل و فصل حوادث به صورت ریشه ای نیستید. شما یک فرآیند رسمی برای بررسی علل ندارید.	تجزیه و تحلیل علت ریشه ای به عنوان بخشی کلیدی از فعالیت های آموخته شده شما پس از یک حادثه به طور معمول انجام می شود. تجزیه و تحلیل علت اصلی شما جامع است و مسائل فرآیند سازمانی و همچنین آسیب پذیری های شبکه، سیستم یا نرم افزار شما را پوشش می دهد. تمام داده های مربوط به حادثه برای انجام تجزیه و تحلیل علت اصلی در اختیار تیم تجزیه و تحلیل قرار می گیرد.

D2.b استفاده از حوادث برای ایجاد بهبود

سازمان شما از درس های آموخته شده از حوادث برای بهبود اقدامات امنیتی شما استفاده می کند.

محقق نشده	محقق شده
حداقل یکی از عبارات زیر درست است	تمام عبارات زیر درست است
پس از حوادث، درس‌های آموخته شده به دست نمی‌آیند یا دامنه آن محدود است. بهبودهای ناشی از درس های آموخته شده پس از یک حادثه اجرا نمی شوند یا اولویت سازمانی کافی داده نمی شود.	شما یک فرآیند/خط مشی بررسی حادثه مستند دارید که تضمین می کند درس های آموخته شده از هر حادثه شناسایی، ضبط و براساس آن عمل می شود. درس های آموخته شده مسائل مربوط به گزارش، نقش ها، حکمرانی، مهارت ها و فرآیندهای سازمانی و همچنین جنبه های فنی شبکه و سیستم های اطلاعاتی را پوشش می دهد. شما از درس های آموخته شده برای بهبود اقدامات امنیتی، از جمله به روز رسانی و آزمایش مجدد طرح های پاسخ درصورت لزوم استفاده می کنید. پیشرفت‌های امنیتی شناسایی‌شده در نتیجه درس‌های آموخته شده، اولویت‌بندی می‌شوند، با بالاترین اولویت‌ها به سرعت تکمیل می‌شوند. تجزیه و تحلیل به مدیریت ارشد داده می شود و در مدیریت ریسک و بهبود مستمرگنجانده می شود.