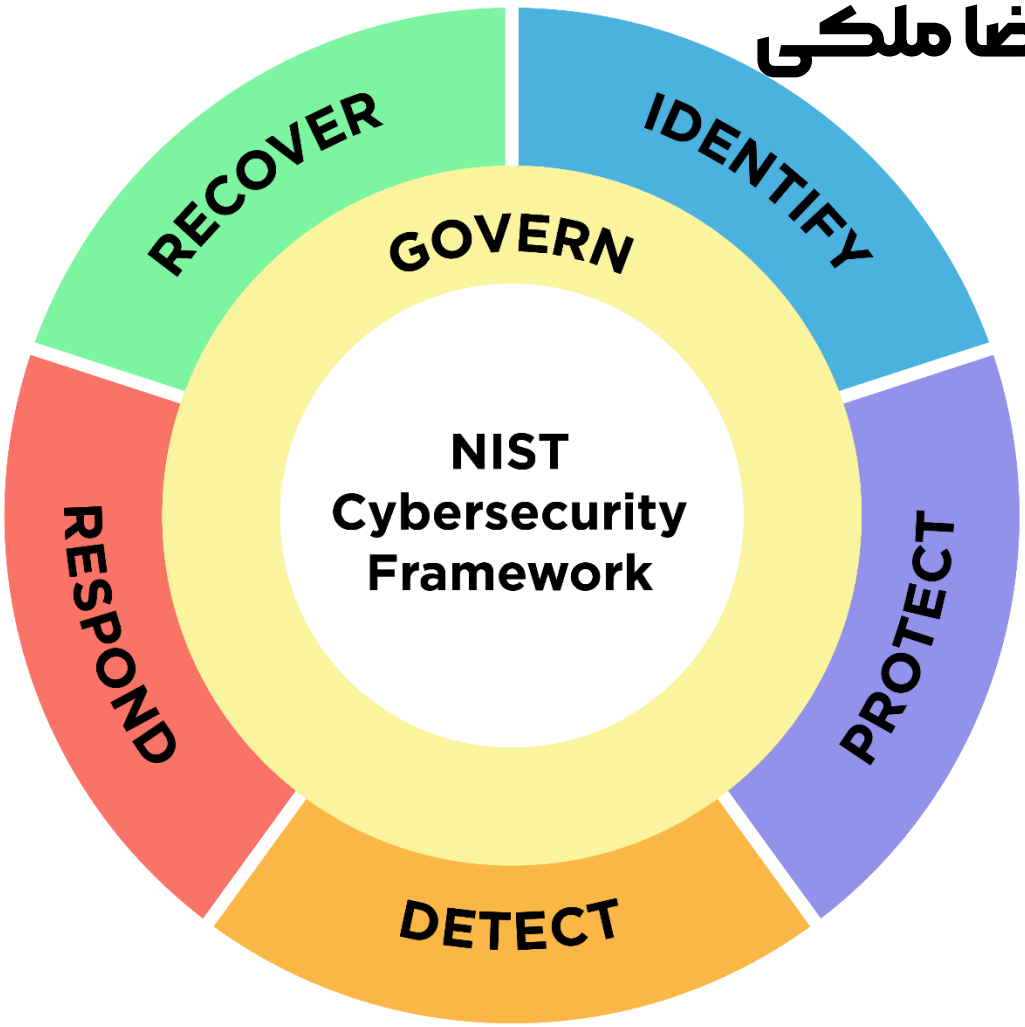
NIST Cybersecurity Framework (CSF) v2.0

نسخه فارسی

علیرضا ملکی



مقدمه

چارچوب امنیت سایبری (CSF) 2.0 به عنوان یک ابزار گسترده‌ای طراحی شده است که به سازمان‌های مختلف در مدیریت و کاهش خطرات امنیت سایبری کمک می‌کند. این چارچوب، بدون توجه به اندازه و صنعت سازمان، مناسب همه است و این امکان را می‌دهد تا خطرات امنیتی منحصر به فرد خود را با در نظر گرفتن مأموریت‌ها و اهداف خود مدیریت کنند. از طریق توصیف نتایج مطلوب، CSF امکان انطباق با نیازهای مختلف سازمان‌ها را فراهم می‌کند و به آن‌ها امکان می‌دهد که کنترل‌های امنیتی خود را برای مقابله با خطرات امنیتی مشخص شده اجرا کنند.

این چارچوب، با تأکید بر اهمیت حاکمیت و زنجیره تأمین، قابلیت‌های جدیدی را ارائه می‌دهد و اطمینان می‌دهد که هم سازمان‌های کوچک و هم بزرگ بتوانند به‌راحتی از آن بهره‌مند شوند. با ارائه نمونه‌های پیاده‌سازی و مراجع اطلاعاتی، CSF به سازمان‌ها کمک می‌کند تا وضعیت فعلی و مطلوب خود را ارزیابی کرده و کنترل‌های امنیتی خود را به‌طور مداوم به‌روزرسانی کنند.

با توجه به گسترش پیوسته خطرات امنیت سایبری، مدیریت این خطرات باید یک فرآیند پیوسته باشد. این موضوع حقیقتی است که بدون توجه به اینکه یک سازمان برای رویارویی با چالش‌های امنیتی سایبری خود آغازگر است یا سال‌ها با یک تیم امنیت سایبری پیشرفته و منابع کافی فعالیت کرده، همچنان اعتبار دارد. CSF طراحی شده است تا برای هر نوع سازمانی ارزشمند باشد و انتظار می‌رود به مدت طولانی مدت، راهنمایی مناسبی فراهم کند.
نسخه اصلی سند در این لینک، موجود است.

امید است تا این ترجمه برایتان مفید واقع شود.

علیرضا ملکی

فروردین ۱۴۰۳

فهرست

1. بررسی اجمالی چارچوب امنیت سایبری (CSF)

این سند، نسخه 2.0 از سند NIST CSF است که شامل موارد زیر می‌باشد:

- **مرکز CSF** ، هسته اصلی CSF می‌باشد، که یک طبقه‌بندی از نتایج امنیت سایبری سطح بالا است که می‌تواند به هر سازمانی در مدیریت ریسک‌های امنیتی خود کمک کند. مؤلفه‌های اصلی CSF سلسله‌مراتبی از توابع، دسته‌ها و زیردسته‌ها هستند که هر نتیجه را جزئیات می‌دهند. این نتایج می‌توانند توسط یک جمع کلی گوناگون شامل مدیران ارشد، مدیران و عوامل اجرایی، بدون در نظر گرفتن تخصص امنیت سایبری، درک شوند. از آنجایی که نتایج بی‌طرف از نظر بخش، کشور و فناوری هستند، این امکان را به یک سازمان می‌دهند تا از انعطاف‌پذیری لازم برای رفع خطرات، فناوری‌ها و ملاحظات ماموریتی خود استفاده کنند.
- **پروفایل‌های سازمانی CSF** ، که یک مکانیزم برای توصیف وضعیت امنیت سایبری فعلی و یا مقصد یک سازمان از نظر نتایج اصلی CSF هستند.
- **لایه‌های CSF** ، که می‌توانند برای پروفایل‌های سازمانی CSF به‌کار گرفته شوند تا شدت حاکمیت و مدیریت ریسک امنیتی یک سازمان را مشخص کنند. لایه‌ها همچنین می‌توانند سازمان‌ها را نشانه‌گذاری کنند که چگونه به خطرات امنیت سایبری نگاه می‌کنند و فرایندهای موجود برای مدیریت آن‌ها.

این سند توصیف می‌کند که یک سازمان چه نتایج مطلوبی را می‌تواند برای دستیابی به آن‌ها هدف قرار دهد. این سند نتایج را مشخص نمی‌کند و نهایتا چگونگی دستیابی به آن‌ها را تعیین نمی‌کند. توصیف‌هایی از اینکه یک سازمان چگونه می‌تواند به این نتایج دست پیدا کند، در یک مجموعه منابع آنلاین ارائه شده است که با فریمورک CSF تطابق دارند و از طریق وب‌سایت NIST CSF در دسترس هستند. این منابع راهنمایی اضافی در مورد روش‌ها و کنترل‌هایی که برای دستیابی به نتایج می‌توانند استفاده شوند ارائه می‌دهند و هدف آن کمک به یک سازمان برای درک، پذیرش و استفاده از CSF است. این منابع شامل موارد زیر هستند:

- مراجع اطلاعاتی که به منابع راهنمایی در مورد هر نتیجه از استانداردها، رهنمودها، فریمورک‌ها، مقررات، سیاست‌ها و غیره از استانداردها، رهنمودها، فریمورک‌ها، مقررات، سیاست‌ها و غیره اشاره می‌کنند.
- نمونه‌های پیاده‌سازی که راه‌های ممکن برای دستیابی به هر نتیجه را نشان می‌دهند
- راهنمای شروع سریع که راهنمایی عملی در مورد استفاده از CSF و منابع آنلاین آن را ارائه می‌دهد، از جمله گذار از نسخه‌های قبلی CSF به نسخه 2.0
- پروفایل‌های انجمن و الگوهای پروفایل سازمانی که به یک سازمان کمک می‌کنند تا CSF را در عمل اجرا کرده و اولویت‌های مدیریت ریسک‌های امنیتی را تعیین کند.

یک سازمان می‌تواند از هسته CSF ، پروفایل‌ها و لایه‌ها به همراه منابع تکمیلی استفاده کند تا ریسک امنیت سایبری را درک، ارزیابی، اولویت‌بندی و ارتباط برقرار کند.

- درک و ارزیابی: توصیف وضعیت فعلی یا مقصد امنیت سایبری یک بخش یا کل سازمان، شناسایی تفاوت‌ها و ارزیابی پیشرفت در رو به رو شدن با آن تفاوت‌ها.
- اولویت‌بندی: شناسایی، سازماندهی و اولویت‌بندی اقدامات برای مدیریت خطرات امنیتی سایبری که با مأموریت، الزامات قانونی و تنظیمات نظارتی و مدیریتی ریسک سازمان همخوانی دارند.
- ارتباط: فراهم کردن یک زبان مشترک برای ارتباط درون و بیرون سازمان در مورد خطرات امنیتی سایبری، توانایی‌ها، نیازها و انتظارات.

CSF به طور طراحی شده است تا توسط سازمان‌های همه اندازه‌ها و بخش‌ها، از جمله صنعت، دولت، دانشگاه و سازمان‌های غیرانتفاعی، بدون در نظر گرفتن سطح بلوغ برنامه‌های امنیتی سایبری آن‌ها، استفاده شود. CSF یک منبع اساسی است که به طور داوطلبانه و از طریق سیاست‌ها و فرمان‌های دولتی قابل پذیرش است. طبقه‌بندی و استانداردها، رهنمودها، و روش‌های ارجاع‌شده توسط CSF کشور مشخصی را هدف ندارند و نسخه‌های قبلی CSF توسط بسیاری از دولت‌ها و سازمان‌های داخلی و خارجی ایالات متحده با موفقیت بهره‌برداری شده‌اند.

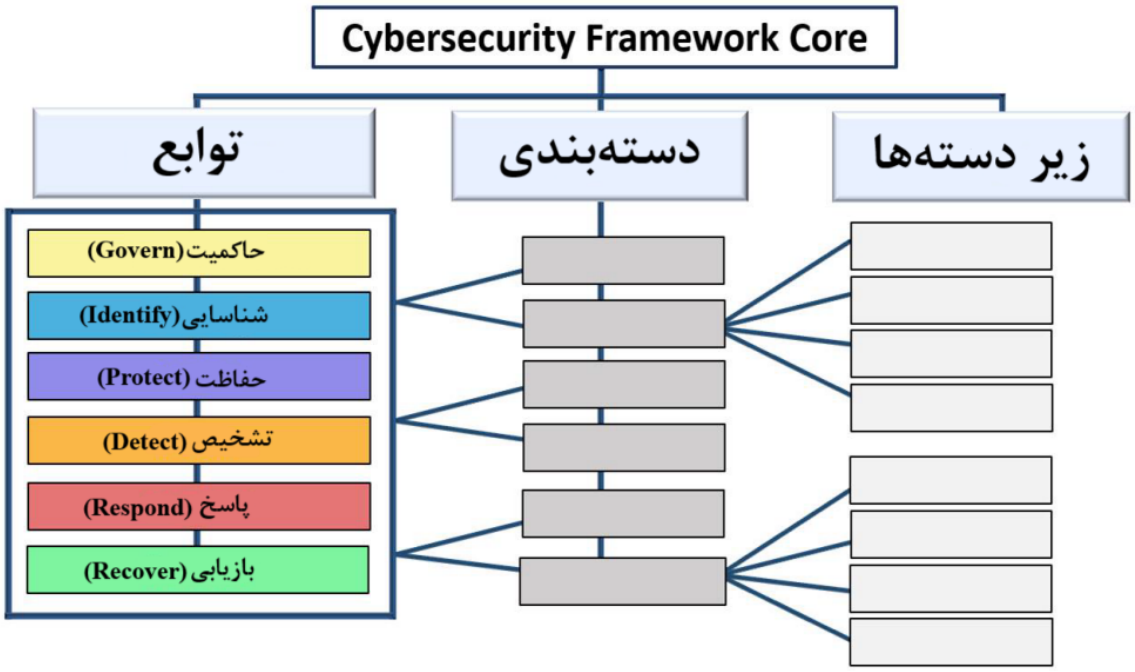
CSF باید به همراه منابع دیگر (مانند فریمورک‌ها، استانداردها، رهنمودها و روش‌های برتر) برای بهتر مدیریت ریسک امنیت سایبری و اطلاع‌رسانی به مدیریت کلی ریسک فناوری اطلاعات و ارتباطات در سطح شرکت استفاده شود. CSF یک فریمورک انعطاف‌پذیر است که قصد دارد برای استفاده توسط همه سازمان‌ها به طور مستقل از اندازه، اختصاص یابد. سازمان‌ها همچنان خطرات منحصر به فردی - از جمله تهدیدات و آسیب‌پذیری‌های مختلف - و تحمل‌های ریسک منحصر به فردی، و همچنین اهداف و الزامات ماموریتی منحصر به فردی خواهند داشت. بنابراین، رویکردها و پیاده‌سازی‌های سازمان‌ها به مدیریت ریسک و پیاده‌سازی CSF متفاوت خواهد بود.

بخش‌های باقی‌مانده این سند به شرح زیر است:

- بخش 2: توضیحات اصولی درباره هسته CSF: توابع، دسته‌ها و زیردسته‌ها.
- بخش 3: تعریف مفاهیم پروفایل‌ها و لایه‌هایCSF.
- بخش 4: مروری بر اجزای انتخاب‌شده از مجموعه منابع آنلاین CSF: مراجع اطلاعاتی، نمونه‌های پیاده‌سازی و راهنمای شروع سریع.
- بخش 5: بحث در مورد چگونگی ادغام CSF با دیگر برنامه‌های مدیریت ریسک.
- پیوست الف: هسته CSF.
- پیوست ب: تصویر نمایشی از لایه‌های CSF.

2. معرفی هسته CSF

پیوست الف هسته CSF است، مجموعه‌ای از نتایج امنیت سایبری که براساس تابع، سپس دسته و در نهایت زیردسته‌ها ترتیب داده شده‌اند، همانطور که در شکل 1 نشان داده شده است. این نتایج یک فهرست از اقدامات برای انجام نیستند؛ اقدامات خاص برای دستیابی به یک نتیجه برای هر سازمان مورد استفاده متفاوت خواهد بود، همچنین شخص مسئول برای این اقدامات نیز متفاوت خواهد بود. علاوه بر این، ترتیب و اندازه توابع، دسته‌ها و زیردسته‌ها در هسته، به ترتیب و اهمیت دستیابی به آنها اشاره نمی‌کند. ساختار هسته برای ارتباط بیشتر با افرادی طراحی شده است که مسئولیت مدیریت ریسک‌ها را در یک سازمان دارند.



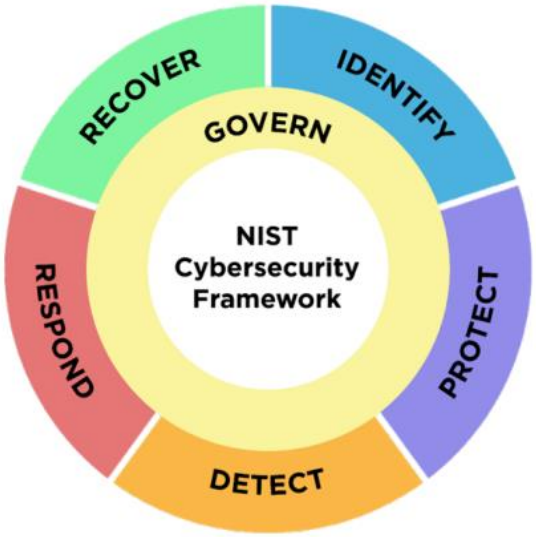
شکل 1. ساختار هسته CSF

توابع اصلی CSF: GOVERN، IDENTIFY، PROTECT، DETECT، RESPOND و RECOVER نتایج امنیت سایبری را در سطح بالاتر خود سازماندهی می‌کنند.

- **Govern(حاکمیت):** استراتژی مدیریت ریسک امنیت سایبری، انتظارات و سیاست سازمان تعیین، ارتباط داده می‌شود و نظارت می‌شود. تابع GOVERN نتایجی را ارائه می‌دهد تا بیانگر این باشد که یک سازمان ممکن است چه کارهایی را برای دستیابی به و اولویت‌بندی نتایج پنج تابع دیگر در زمینه مأموریت و انتظارات ذینفعان خود انجام دهد. فعالیت‌های حاکمیت برای گنجاندن امنیت سایبری در استراتژی مدیریت ریسک شرکتی گسترده‌تر یک سازمان حیاتی است. GOVERN به درک محیط سازمانی، تعیین استراتژی امنیت سایبری و مدیریت ریسک زنجیره تأمین امنیت سایبری، نقش‌ها، مسئولیت‌ها و اختیارات، سیاست و نظارت بر استراتژی امنیت سایبری می‌پردازد.

- **Identify(شناسایی)**: خطرات امنیتی سایبری فعلی سازمان درک می‌شوند. درک دارایی‌های سازمان (مانند داده‌ها، سخت‌افزار، نرم‌افزار، سیستم‌ها، امکانات، خدمات، افراد)، تأمین‌کنندگان و خطرات مرتبط با امنیت سایبری، به یک سازمان امکان می‌دهد تا تلاش‌های خود را با استراتژی مدیریت ریسک خود و نیازهای مأموریتی شناسایی شده زیر GOVERN سازمان و همسان کند. این تابع همچنین شامل شناسایی فرصت‌های بهبود برای سیاست‌ها، برنامه‌ها، فرآیندها، روش‌ها و روش‌های سازمان که از مدیریت خطرات امنیت سایبری حمایت می‌کنند، برای اطلاع‌رسانی تلاش‌ها در تمام شش تابع است.
- **Protect(حفاظت)**: اقدامات محافظتی برای مدیریت ریسک امنیت سایبری سازمان استفاده می‌شود. بعد از شناسایی و اولویت‌بندی دارایی‌ها و خطرات، PROTECT امکان محافظت از این دارایی‌ها را برای جلوگیری یا کاهش احتمال و تأثیر رویدادهای منفی امنیت سایبری فراهم می‌کند، همچنین برای افزایش احتمال و تأثیر بهره‌مندی از فرصت‌ها. نتایجی که توسط این تابع پوشش داده می‌شوند شامل مدیریت هویت، احراز هویت و کنترل دسترسی؛ آگاهی و آموزش؛ امنیت داده؛ امنیت پلتفرم (یعنی امنیت سخت‌افزار، نرم‌افزار و خدمات پلتفرم‌های فیزیکی و مجازی)؛ و انعطاف‌پذیری زیرساخت فناوری می‌باشد.
- **Detect(تشخیص)**: حملات و مخاطرات احتمالی امنیتی شناسایی و تحلیل می‌شوند. DETECT امکان کشف و تحلیل به موقع موارد مشکوک، نشانگرهای نفوذ، و دیگر رویدادهای بالقوه منفی را فراهم می‌کند که ممکن است نشان دهنده وقوع حملات و رویدادهای امنیتی باشند. این تابع فعالیت‌های موفقیت‌آمیز پاسخ به حوادث و بازیابی را پشتیبانی می‌کند.
- **Respond(پاسخ)**: اقدامات مربوط به یک حادثه امنیتی شناسایی شده انجام می‌شود. RESPOND امکان حفظ تأثیرات حوادث امنیتی را فراهم می‌کند. نتایج درون این تابع شامل مدیریت، تجزیه و تحلیل، کاهش، گزارش‌دهی و ارتباط حوادث است.
- **Recover(بازیابی)**: دارایی‌ها و فعالیت‌های تحت تأثیر حادثه امنیتی بازیابی می‌شوند. RECOVER امکان بازیابی به موقع از عملیات عادی را برای کاهش اثرات حوادث امنیتی فراهم می‌کند و امکان ارتباط مناسب در طول تلاش‌های بازیابی را فراهم می‌کند.

شکل 2 توابع CSF را به عنوان یک چرخ نشان می‌دهد زیرا همه توابع با یکدیگر ارتباط دارند. به عنوان مثال، یک سازمان دارایی‌ها را در زیر IDENTIFY دسته‌بندی می‌کند و مراحلی را برای ایمن نگه‌داشتن آن دارایی‌ها در PROTECT انجام می‌دهد. سرمایه‌گذاری‌ها در برنامه‌ریزی و آزمایش در GOVERN و IDENTIFY از تشخیص به موقع رویدادهای غیرمنتظره در DETECT پشتیبانی می‌کنند، همچنین اقدامات پاسخ و بازیابی حادثه برای حوادث امنیتی در RESPOND و RECOVER را فراهم می‌کنند. GOVERN در مرکز چرخ قرار دارد زیرا نحوه پیاده‌سازی سایر پنج تابع را مشخص می‌کند.



شکل 2. توابع CSF

توابع باید به طور همزمان مورد توجه قرار گیرند. اقداماتی که پشتیبانی ازGOVERN ، IDENTIFY، PROTECT و DETECT را دارند، باید به طور مداوم انجام شوند، و اقداماتی که از RESPOND و RECOVER پشتیبانی می‌کنند، باید در همه زمان‌ها آماده و در هنگام وقوع حوادث امنیت سایبری انجام شوند. تمام توابع، نقش‌های حیاتی مرتبط با حوادث امنیتی دارند. نتایج GOVERN، IDENTIFYو PROTECT در جلوگیری و آماده‌سازی برای حوادث کمک می‌کنند، در حالی که نتایجGOVERN ، DETECT، RESPONDو RECOVER در کشف و مدیریت حوادث کمک می‌کنند.

هر تابع با یک فعلی نامگذاری شده است که محتوای آن را خلاصه می‌کند. هر تابع به دسته‌ها تقسیم شده است، که نتایج امنیت سایبری مرتبطی هستند که به طور کلی تابع را تشکیل می‌دهند. زیردسته‌ها هر دسته را به نتایج مشخص‌تری از فعالیت‌های فنی و مدیریتی تقسیم می‌کنند. زیردسته‌ها کامل نیستند، اما نتایج جزئی را که پشتیبانی از هر دسته را انجام می‌دهند، توصیف می‌کنند.

توابع، دسته‌ها و زیردسته‌ها برای تمام فناوری‌های اطلاعات و ارتباطاتی که یک سازمان استفاده می‌کند، اعمال می‌شوند، از جمله فناوری اطلاعات (IT)، اینترنت اشیاء (IoT) و فناوری عملیاتی (OT). همچنین برای همه انواع محیط‌های فناوری، از جمله ابر، موبایل و سیستم‌های هوش مصنوعی مورد استفاده قرار می‌گیرند. هسته CSF پیش بینی کننده است و قرار است در تغییرات آینده فناوری‌ها و محیط‌ها به کار رود.

3. معرفی پروفایل‌ها و سطوح CSF

در این بخش، به مفاهیم پروفایل‌ها و سطوح CSF می‌پردازیم.

3.1 پروفایل‌های CSF

یک پروفایل سازمانیCSF ، وضعیت فعلی و یا مطلوب امنیت سایبری یک سازمان را به ازای نتایج اصلی هسته شرح می‌دهد. پروفایل‌های سازمانی برای درک، سفارشی‌سازی، ارزیابی، اولویت‌بندی و ارتباط نتایج اصلی با در نظر گرفتن اهداف مأموریتی، انتظارات ذینفعان، منظریه تهدید و نیازهای یک سازمان استفاده می‌شوند. سپس سازمان می‌تواند اقدامات خود را برای دستیابی به نتایج خاص اولویت بندی کند و این اطلاعات را به ذینفعان ارتباط دهد.

هر پروفایل سازمانی شامل یک یا هر دوی موارد زیر می‌شود:

1. پروفایل فعلی مشخص می‌کند که یک سازمان در حال حاضر (یا تلاش برای دستیابی به) نتایج اصلی هسته را دارد و نحوه یا میزان دستیابی به هر نتیجه را مشخص می‌کند.
2. پروفایل هدف نتایج مطلوبی را که یک سازمان برای دستیابی به اهداف مدیریت ریسک امنیت سایبری خود انتخاب و اولویت بندی کرده است مشخص می‌کند. یک پروفایل هدف تغییرات پیش‌بینی شده در وضعیت امنیت سایبری سازمان را مطرح می‌کند، مانند نیازهای جدید، پذیرش فناوری جدید و روندهای اطلاعات تهدیدات

یک پروفایل اجتماعی، یک پایگاه از نتایج CSF است که برای برآورده کردن اهداف و منافع مشترک بین چند سازمان ایجاد و منتشر می‌شود. یک پروفایل اجتماعی معمولاً برای یک بخش خاص، زیربخش، فناوری، نوع تهدید یا دیگر موارد مصرفی توسعه داده می‌شود. یک سازمان می‌تواند از یک پروفایل اجتماعی به عنوان پایه برای پروفایل هدف خود استفاده کند. مثال‌هایی از پروفایل‌های اجتماعی می‌توان در وب‌سایت CSF NIST پیدا کرد.

مراحل نشان داده شده در شکل ۳ به طور خلاصه ، یک روش نشان دهنده است که یک سازمان می‌تواند از یک پروفایل سازمانی برای کمک به اطلاع رسانی بهبود مداوم امنیت سایبری خود استفاده کند.

شکل ۳. مراحل ایجاد و استفاده از یک پروفایل سازمانیCSF

1. **تعیین حوزه‌ی پروفایل سازمانی.** اسنادی راجع به واقعیت‌ها و فرضیات سطح بالا تهیه کنید که بر اساس آن‌ها پروفایل تعریف خواهد شد تا حوزه‌اش را تعیین کنید. یک سازمان می‌تواند تعداد دلخواهی پروفایل سازمانی داشته باشد، هر کدام با یک حوزه متفاوت. به عنوان مثال، یک پروفایل می‌تواند به کل یک سازمان مرتبط باشد یا محدود به سیستم‌های مالی یک سازمان یا به مقابله با تهدیدات ransomware و مدیریت حوادث ransomware مربوط به آن سیستم‌های مالی باشد.
2. **جمع‌آوری اطلاعات مورد نیاز برای آماده‌سازی پروفایل سازمانی.** مثال‌هایی از اطلاعات ممکن شامل سیاست‌های سازمانی، اولویت‌ها و منابع مدیریت ریسک، پروفایل‌های ریسک سازمانی، ثبت‌های تجزیه و تحلیل تأثیر کسب و کار(BIA) ، الزامات و استانداردهای امنیت سایبری که سازمان پیروی می‌کند، روش‌ها و ابزارها و نقش‌های کاری است.
3. **ایجاد پروفایل سازمانی.** تعیین کنید چه نوع اطلاعاتی برای نتایج انتخاب شده CSF در پروفایل باید شامل شود، و اطلاعات مورد نیاز را مستند کنید. ارزیابی اثرات ریسک پروفایل فعلی برای اطلاعاتی که برای برنامه‌ریزی و اولویت‌بندی پروفایل هدف لازم است در نظر گرفته شود. همچنین، در نظر بگیرید که از یک پروفایل جامعی به عنوان پایه برای پروفایل هدف استفاده کنید.
4. **تحلیل نقاط ضعف بین پروفایل فعلی و هدف، و ایجاد یک برنامه عمل.** یک تحلیل نقطه ضعف (gap analysis) برای شناسایی و تجزیه و تحلیل تفاوت‌ها بین پروفایل فعلی و هدف انجام دهید، و یک برنامه عمل با اولویت‌بندی (مانند ثبت ریسک، گزارش جزئیات ریسک، برنامه عمل و گام‌های نیاز به طی شدن) برای رفع این تفاوت‌ها تهیه کنید.

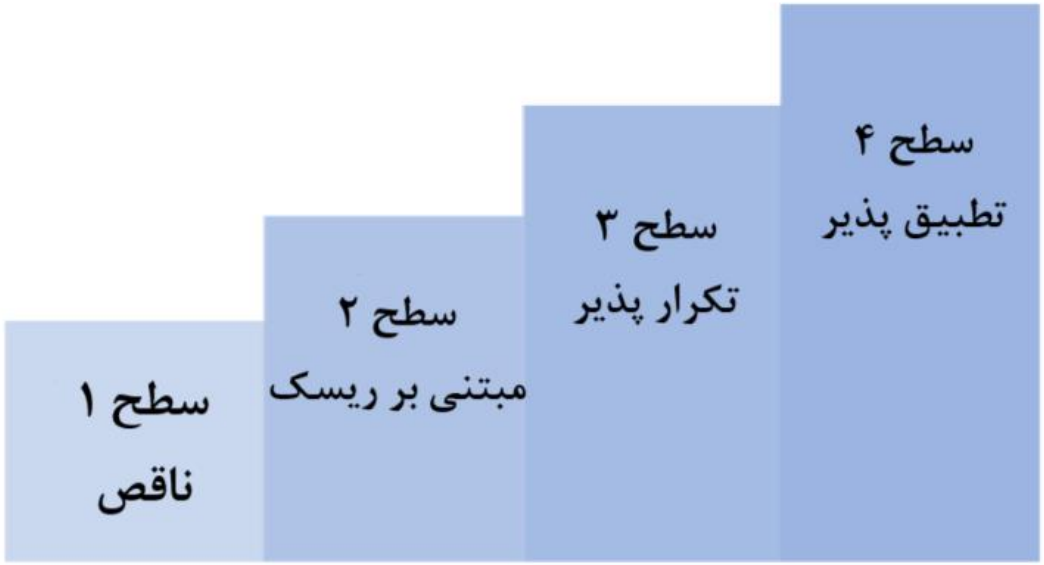
5. **اجرای برنامه عمل و به‌روزرسانی پروفایل سازمانی**. برنامه عمل را دنبال کرده و برای حل نقاط ضعف و انتقال سازمان به سمت پروفایل هدف، عمل کنید. یک برنامه عمل ممکن است یک مهلت کلی داشته باشد یا به طور مداوم باشد.

با توجه به اهمیت بهبود مداوم، یک سازمان می‌تواند این مراحل را تا زمانی که نیاز باشد تکرار کند.

برای پروفایل‌های سازمانی کاربردهای دیگری وجود دارد. به عنوان مثال، یک پروفایل فعلی می‌تواند برای مستند کردن و ارتباط برقرار کردن با توانمندی‌های امنیت سایبری و فرصت‌های شناخته شده سازمان با ذینفعان خارجی مانند شرکای تجاری یا مشتریان آتی استفاده شود. همچنین، یک پروفایل هدف می‌تواند به سازمان کمک کند نیازها و انتظارات مدیریت ریسک امنیت سایبری را به تأمین‌کنندگان، شرکای تجاری و دیگر شخصیت‌های ثالث به عنوان یک هدف برای دستیابی به آن نشان دهد.

3.2 سطوح CSF

یک سازمان می‌تواند از سطوح برای اطلاع‌رسانی به پروفایل‌های فعلی و هدف خود استفاده کند. سطوح مراتب از دقت و تدبیر مدیریت ریسک امنیت سایبری یک سازمان را تعریف می‌کنند، و متناسب با اینکه یک سازمان چگونه ریسک‌های امنیتی را می‌بیند و فرآیندهای موجود برای مدیریت این ریسک‌ها چیست. این سطوح، همانطور که در شکل ۴ و به طور مفهومی در پیوست ب نشان داده شده است، تمایلات یک سازمان را برای مدیریت ریسک‌های امنیتی را از سطح جزئی (سطح ۱)، مطابق با ریسک (سطح ۲)، تکرارپذیر (سطح ۳) و تطبیقی (سطح ۴) توصیف می‌کنند. این سطوح، یک پیشرفت از پاسخ‌های غیر رسمی و به صورت دلخواه به روش‌های سریع، مطلع از ریسک و بهبود مداوم را نشان می‌دهند. انتخاب سطوح به کمک تنظیم کلیات کاربردی برای مدیریت ریسک‌های امنیتی یک سازمان است.



شکل ۴. سطوح CSF برای مدیریت ریسک امنیت سایبری

سطوح باید به روش مدیریت ریسک امنیت سایبری سازمان تکمیل کنند، نه جایگزین آن باشند. به عنوان مثال، یک سازمان می‌تواند از سطوح برای ارتباط داخلی به عنوان یک معیار برای یک رویکرد سازمانی کلی برای مدیریت ریسک‌های امنیت سایبری استفاده کند. پیشرفت به سطوح بالاتر تشویق می‌شود زمانی که ریسک‌ها یا فرمان‌ها بیشتر باشند یا زمانی که یک تجزیه و تحلیل فایده و هزینه نشان دهنده کاهش قابل قبول و موثر هزینه ریسک‌های منفی امنیت سایبری است.

وب‌سایت NIST CSF اطلاعات اضافی در مورد استفاده از پروفایل‌ها و سطوح را فراهم می‌کند. این شامل اشاره‌گرها به الگوهای پروفایل سازمانی میزبان شده توسط NIST و یک مخزن از پروفایل‌های انجمن به صورت متناوب و قابل استفاده انسانی و قابل خواندن توسط ماشین است.

4. معرفی منابع آنلاین که CSF را تکمیل می‌کنند.

NIST و سازمان‌های دیگر مجموعه‌ای از منابع آنلاین تولید کرده‌اند که به سازمان‌ها کمک می‌کنند تا CSF را درک کنند، به آن اعتماد کنند و از آن استفاده کنند. از آنجا که این منابع اضافی به صورت آنلاین میزبانی می‌شوند، امکان به‌روزرسانی آنها از این سند که به ندرت به‌روزرسانی می‌شود تا استقرار استقرار به کاربران خود استقرار به کاربران خود استقرار امکان پذیر است و در فرمت‌های قابل خواندن توسط ماشین در دسترس است. این بخش شرحی از سه نوع منابع آنلاین ارائه می‌دهد: مراجع اطلاعاتی، نمونه‌های اجرایی و راهنمای شروع سریع.

مراجع اطلاعاتی نقش‌هایی است که ارتباطات بین هسته و استانداردها، رهنمودها، مقررات و محتوای دیگر را نشان می‌دهند. مراجع اطلاعاتی کمک می‌کنند تا چگونگی دستیابی به نتایج هسته را اطلاع‌رسانی کنند. مراجع اطلاعاتی ممکن است به صورت خاص برای بخش‌های خاصی از صنعت یا فناوری باشند. آنها ممکن است توسط NIST یا سازمان دیگری تولید شوند. برخی از مراجع اطلاعاتی دامنه‌ای باریک‌تر از یک زیردسته هستند. به عنوان مثال، یک کنترل خاص از SP 800-53 ، کنترل‌های امنیتی و حریم خصوصی برای سیستم‌ها و سازمان‌ها، یکی از مراجع مورد نیاز برای دستیابی به نتایج توصیف شده در یک زیردسته می‌تواند باشد. مراجع اطلاعاتی دیگر ممکن است بیشتر سطحی باشند، مانند یک الزام از یک سیاست که به طور جزئی به بسیاری از زیردسته‌ها پاسخ می‌دهد. در استفاده از CSF، یک سازمان می‌تواند مراجع اطلاعاتی مهم‌ترین را شناسایی کند. نمونه‌های اجرایی مثال‌های ذاتی، جذاب و عملی را برای کمک به دستیابی به نتایج زیردسته‌ها ارائه می‌دهند. افعال استفاده شده برای بیان مثال‌ها شامل به اشتراک گذاری، اسناد، توسعه، اجرا، نظارت، تجزیه و تحلیل، ارزیابی و تمرین هستند. این مثال‌ها فهرست جامعی از همه اقداماتی نیستند که یک سازمان می‌تواند انجام دهد تا به نتیجه برسد، و یا نشان‌دهنده یک سطح ضروری از اقدامات مورد نیاز برای مدیریت ریسک‌های امنیت سایبری نیستند.

راهنمای شروع سریع (QSG) اسناد مختصر در مورد موضوعات خاص مربوط به CSF هستند و اغلب به زیرمجموعه‌های خاصی اختصاص داده شده‌اند. راهنمای‌های شروع سریع می‌توانند به یک سازمان کمک کنند تا CSF را پیاده‌سازی کنند زیرا آنها بخش‌های خاصی از CSF را به "اولین قدم‌های" قابل انجام تبدیل می‌کنند که یک سازمان می‌تواند روی آنها در مسیر بهبودی امنیت سایبری خود و مدیریت ریسک‌های مرتبط با آن تأمل کند. این راهنماها با فراهم کردن اطلاعاتی زمان‌بندی شده خودشان به روزرسانی می‌شوند، و راهنماهای جدید زمانی که نیاز باشد اضافه می‌شوند.

پیشنهادات برای مراجع اطلاعاتی جدید برای CSF 2.0 همیشه می‌تواند با NIST به آدرس olir@nist.gov به اشتراک گذاشته شود. پیشنهادات برای منابع دیگری که ممکن است بر روی وب‌سایت NIST CSF ارجاع شود، از جمله موضوعات QSG اضافی، باید به ایمیل cyberframework@nist.gov ارسال شود.

5. بهبود ارتباط و ادغام ریسک‌های سایبری

استفاده از CSF بر اساس مأموریت و ریسک‌های منحصر به فرد یک سازمان متفاوت خواهد بود. با درک انتظارات سایر ذی‌نفعان و تاب‌آوری و سربارهای ریسک (همانطور که در GOVERN ذکر شده است)، یک سازمان می‌تواند فعالیت‌های امنیت سایبری را اولویت بندی کرده و تصمیمات آگاهانه‌تری در مورد هزینه‌ها و اقدامات امنیت سایبری بگیرد. یک سازمان ممکن است بسته به تأثیرات و احتمالات احتمالی، ریسک را به یک یا چند روش - از جمله کاهش، انتقال، اجتناب، یا پذیرش ریسک‌های منفی و درک، به اشتراک گذاشتن، افزایش یا پذیرش ریسک‌های مثبت انتخاب کند. نکته مهم این است که یک سازمان می تواند از CSF هم به صورت داخلی برای مدیریت قابلیت های امنیت سایبری خود و هم به صورت خارجی برای نظارت یا ارتباط با شرکای سوم استفاده کند.

به هر حال، با استفاده از CSF به عنوان راهنما برای کمک به درک، ارزیابی، اولویت‌بندی و ارتباط ریسک‌های سایبری و اقداماتی که مدیریت خواهد کرد، یک سازمان می‌تواند بهره‌مندی داشته باشد. نتایج انتخاب شده می‌توانند برای تمرکز و اجرای تصمیمات استراتژیک جهت بهبود امنیت سایبری و حفظ پیوستگی عملکردهای مهم مأموریتی در نظر گرفته شوند همچنین اولویت‌ها و منابع موجود را در نظر بگیرند.

5.1 بهبود ارتباط مدیریت ریسک

CSF اساسی برای بهبود ارتباط در مورد انتظارات، برنامه‌ریزی و منابع امنیت سایبری فراهم می‌کند. CSF جریان اطلاعات دوطرفه را بین مدیران اجرایی که بر اولویت‌ها و جهت‌گیری‌های استراتژیک سازمان تمرکز می‌کنند و مدیرانی که ریسک‌های امنیتی خاصی را که ممکن است بر دستیابی به این اولویت‌ها تأثیر بگذارد مدیریت می‌کنند، ترویج می‌کند. CSF همچنین جریان مشابهی را (همانطور که در نیمه پایین تصویر ۵ نشان داده شده است) بین مدیران و افرادی که فناوری‌ها را اجرا و اداره می‌کنند، پشتیبانی می‌کند. نیمه چپ تصویر نشان می‌دهد که اهمیت افراد ارتباطی اطلاعات، بینش‌ها و مشکلات خود را با مدیران و مدیران اجرایی به اشتراک بگذارند.

برای آماده‌سازی برای ایجاد و استفاده از پروفایل‌های سازمانی، اطلاعات مربوط به اولویت‌ها، منابع و جهت‌گیری ریسک سازمان از اجرایی‌ها جمع‌آوری می‌شود. سپس مدیران با افراد فنی به همکاری برای ارتباط با نیازهای تجاری و ایجاد پروفایل‌های سازمانی مبتنی بر ریسک مشغول می‌شوند. اقداماتی برای پوشاندن هر گونه اختلاف مشاهده شده بین پروفایل‌های فعلی و هدفی اجرا شده و مدیران و افراد فنی وارد عمل شده و اطلاعات کلیدی را به طرح‌های سطح سیستم ارائه می‌دهند. هنگامی که حالت هدف در سراسر سازمان، شامل کنترل‌ها و نظارتی که در سطح سیستم اعمال می‌شوند، نتایج به‌روزرسانی شده می‌توانند از طریق ثبت ریسک و گزارش‌های پیشرفت به اشتراک گذاشته شوند. به عنوان یک بخش از ارزیابی مداوم، مدیران درک‌هایی برای ایجاد تغییراتی که بهبود آسیب‌های ممکن را افزایش دهند و منافع ممکن را افزایش دهند کسب می‌کنند.

تابع GOVERN ارتباطات سازمانی ریسک را با اجرایی‌ها پشتیبانی می‌کند. بحث‌های اجرایی به استراتژی، به‌ویژه چگونگی تأثیر عدم اطمینان مرتبط با امور امنیت سایبری بر دستیابی به اهداف سازمان می‌پردازد. این گفتگوهای حاکمیتی درباره استراتژی‌های مدیریت ریسک (شامل ریسک زنجیره تأمین سایبری)؛ نقش‌ها، مسئولیت‌ها و اختیارات؛ سیاست‌ها؛ و نظارت حمایت می‌کند. همچنین به عنوان اجرایی‌ها اولویت‌ها و اهداف امنیت سایبری را بر اساس آن

نیازها تعیین می‌کنند، انتظارات خود را در مورد تاب‌آوری ریسک، مسئولیت پذیری و منابع ارتباط می‌دهند. اجرایی‌ها همچنین مسئول ادغام مدیریت ریسک سایبری با برنامه‌های مدیریت ریسک ERM و برنامه‌های مدیریت ریسک سطح پایین‌تر هستند (راهنمای ۵.۲ را ببینید). ارتباطاتی که در نیمه بالای تصویر ۵ نمایان است می‌تواند شامل ملاحظاتی برای ERM و برنامه‌های سطح پایین‌تر باشد و بنابراین اطلاعاتی را برای مدیران و افراد فنی فراهم کند.
اهداف امنیت سایبری کلی توسط اجرایی‌ها آگاهانه و به مدیران منتقل می‌شوند. در یک شرکت تجاری، این‌ها ممکن است به یک خط تجاری یا بخش عملیاتی اعمال شوند. برای نهادهای دولتی، این‌ها ممکن است ملاحظات سطح بخش یا شاخه باشند. هنگام اجرایCSF ، مدیران بر روی این تمرکز خواهند کرد که چگونه از طریق خدمات مشترک، کنترل‌ها و همکاری به تحقق اهداف ریسک می‌رسند، همانطور که در پروفایل هدف و بهبود از طریق اقداماتی که در برنامه اقدامات ردیابی می‌شوند (مانند ثبت ریسک، گزارش جزئیات ریسک، POA&M بیان شده است).
افراد فنی بر روی اجرای حالت هدف و اندازه‌گیری تغییرات در ریسک‌های عملیاتی تمرکز می‌کنند تا به برنامه‌ریزی، اجرا و نظارت بر فعالیت‌های خاص امنیت سایبری کمک کنند. هنگامی که کنترل‌ها برای مدیریت ریسک به سطح قابل قبولی اعمال می‌شوند، افراد عملی اطلاعاتی (مانند شاخص‌های عملکرد اصلی، شاخص‌های ریسک اصلی) که مدیران و اجرایی‌ها برای درک وضعیت امنیت سایبری سازمان نیاز دارند را ارائه می‌دهند تا تصمیمات آگاهانه اتخاذ کنند و استراتژی ریسک را به‌طور مناسب حفظ یا تغییر دهند. اجرایی‌ها همچنین می‌توانند این داده‌های ریسک امنیت سایبری را با اطلاعات مربوط به سایر انواع ریسک از سراسر سازمان ترکیب کنند. به‌روزرسانی‌های انتظارات و اولویت‌ها در پروفایل‌های سازمانی به‌روز شده به‌عنوان یک چرخه تکرار می‌شود.

5.2 بهبود ادغام با برنامه‌های مدیریت ریسک دیگر

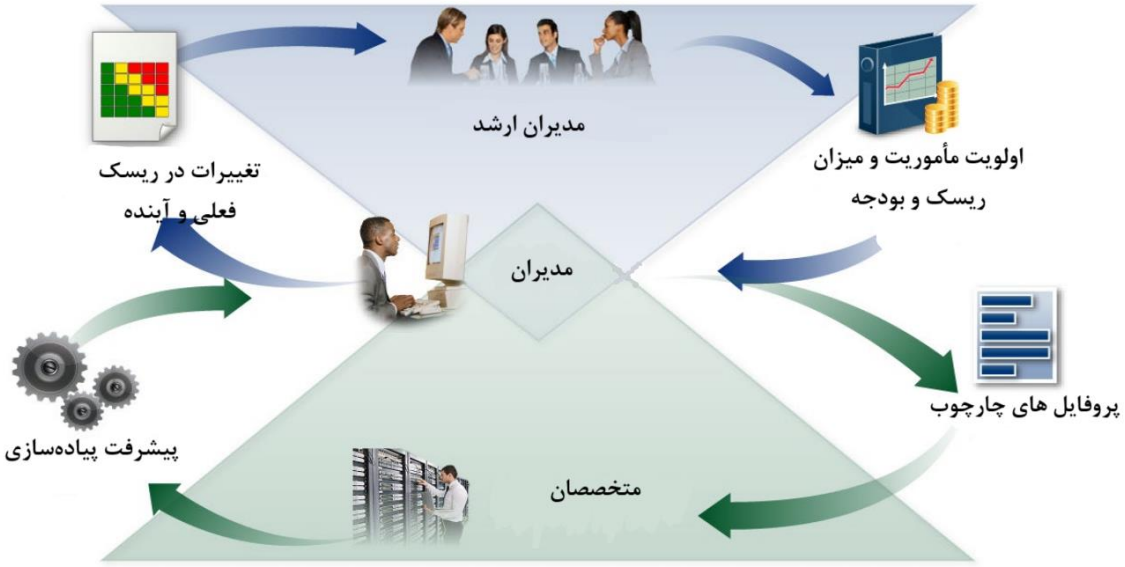
هر سازمان با چندین نوع ریسک فناوری اطلاعات (مانند حریم خصوصی، زنجیره تأمین، هوش مصنوعی) روبرو می‌شود و ممکن است از چارچوب‌ها و ابزارهای مدیریت مختص به هر ریسک استفاده کند. برخی از سازمان‌ها فناوری اطلاعات و همه تلاش‌های مدیریت ریسک دیگر را در سطح بالا با استفاده از ERM ادغام می‌کنند، در حالی که دیگران تلاش‌ها را جدا نگه می‌دارند تا توجه کافی به هرکدام را اطمینان دهند. سازمان‌های کوچک به طبیعت خود ممکن است ریسک را در سطح سازمانی نظارت کنند، در حالی که شرکت‌های بزرگ ممکن است تلاش‌های مدیریت ریسک را جداگانه حفظ کرده و آنها را به ERM ادغام کنند .سازمان‌ها می‌توانند از یک رویکرد ERM استفاده کنند تا یک نمایه‌ی ترکیبی از موارد مرتبط با ریسک را، از جمله امنیت سایبری، به‌طور آگاهانه تعادل دهند و تصمیمات آگاهانه‌ای بگیرند. اجرایی‌ها ورودی‌های قابل توجهی درباره فعالیت‌های ریسک فعلی و برنامه‌ریزی‌شده را دریافت می‌کنند زمانی که ادغام حاکمیت و استراتژی‌های ریسک با نتایج استفاده‌های قبلی از CSF را انجام می‌دهند CSF .به سازمان‌ها کمک می‌کند تا اصطلاحات خود را برای امنیت سایبری و مدیریت ریسک سایبری خود به زبان عمومی مدیریت ریسک ترجمه کنند .منابع NIST که رابطه متقابل بین مدیریت ریسک سایبری و ERM را توصیف می‌کنند عبارتند از:

- NIST CSF 2.0: شروع سریع مدیریت ریسک
- NIST IR 8286: ادغام امنیت سایبری و مدیریت ریسک سازمانی
- IR 8286A: شناسایی و تخمین ریسک امنیتی سایبری برای مدیریت ریسک سازمانی
- IR 8286B: اولویت‌بندی ریسک امنیتی سایبری برای مدیریت ریسک سازمانی

- IR 8286C: مراحل بندی ریسک‌های امنیتی سایبری برای مدیریت ریسک سازمانی و نظارت بر حاکمیت
- IR 8286D: استفاده از تجزیه و تحلیل تأثیر کسب‌وکار برای اطلاع رسانی اولویت‌بندی و پاسخ ریسک
- SP 800-221: تأثیر سازمانی ریسک فناوری اطلاعات و ارتباطات: حاکمیت و مدیریت برنامه‌های ریسک فناوری اطلاعات و ارتباطات داخل یک پرتفوی ریسک سازمانی
- SP 800-221A: نتایج ریسک فناوری اطلاعات و ارتباطات :(ICT) ادغام برنامه‌های مدیریت ریسک ICT با پرتفوی ریسک سازمانی

یک سازمان همچنین ممکن است از NIST CSF برای ادغام مدیریت ریسک امنیت سایبری با برنامه‌های مدیریت ریسک فناوری اطلاعات و ارتباطات (ICT) استفاده کند، مانند:

- **مدیریت و ارزیابی ریسک امنیت سایبری:** چارچوب مدیریت ریسک برای سیستم‌ها و سازمان‌ها (RMF) SP 800-37و راهنمای انجام ارزیابی‌های ریسک SP 800-30 از چارچوب مدیریت ریسک NIST (RMF) برای انتخاب و اولویت‌بندی کنترل‌ها از SP 800-53 ، کنترل‌های امنیتی و حریم خصوصی برای سیستم‌ها و سازمان‌ها استفاده می‌شود. برای یک سازمانی که از چارچوب RMF NIST و مجموعه انتشارات آن استفاده می‌کند، می‌توان از چارچوب CSF به عنوان مکملی برای رویکرد RMF به انتخاب و اولویت‌بندی کنترل‌ها از SP 800-53 استفاده کرد.
- **ریسک‌های حریم خصوصی:** در حالی که امنیت سایبری و حریم خصوصی حوزه‌های مستقلی هستند، اهداف آن‌ها در شرایط خاصی با هم تداخل دارند، همانطور که در شکل ۶ نشان داده شده است.



شکل ۶. رابطه بین ریسک‌های امنیت سایبری و حریم خصوصی

مدیریت ریسک امنیت سایبری برای برخورد با ریسک‌های حریم خصوصی مرتبط با از دست دادن محرمانگی، یکپارچگی و دسترسی به داده‌های افراد ضروری است. به عنوان مثال، نقض داده‌ها می‌تواند به سرقت هویت منجر شود. با این حال، ریسک‌های حریم خصوصی همچنین ممکن است از طریق وسایلی که با حوادث امنیت سایبری مرتبط نیستند، به‌وجود بیایند.

یک سازمان داده‌ها را برای دستیابی به اهداف ماموریتی یا تجاری پردازش می‌کند، که گاهاً می‌تواند باعث بروز رویدادهای حریم خصوصی شود که افراد ممکن است به دلیل پردازش داده‌ها مشکلاتی را تجربه کنند. این مشکلات می‌توانند به انواع مختلفی بیان شوند، اما NIST آن‌ها را از اثرات نوع کرامت (مانند شرم‌آوری یا افتخار) تا آسیب‌های قابل لمس (مانند تبعیض، از دست دادن اقتصادی یا آسیب جسمانی) توصیف می‌کند. چارچوب حریم خصوصی و چارچوب امنیت سایبری NIST می‌توانند به همراه استفاده از منابع دیگر مانند چارچوب ارزیابی ریسک حریم خصوصی NIST به عنوانPRAM ، در جهت برخورد با جنبه‌های مختلف ریسک‌های امنیت سایبری و حریم خصوصی مورد استفاده قرار گیرند.

- **ریسک‌های زنجیره تأمین:** یک سازمان می‌تواند از چارچوب CSF برای تقویت نظارت بر ریسک‌های امنیت سایبری و ارتباط با دست‌اندرکاران در سراسر زنجیره‌های تأمین استفاده کند. تمام انواع فناوری بر یک اکوسیستم زنجیره‌ی تأمین پیچیده، توزیع شده به صورت جهانی، گسترده و پیوندی با سطوح مختلف out sourcing وابسته است. این اکوسیستم از شرکت‌های دولتی و خصوصی (مانند خریداران، تامین‌کنندگان، توسعه‌دهندگان، ادغام‌کنندگان سیستم، ارائه‌دهندگان خدمات سیستم خارجی و سایر ارائه‌دهندگان خدمات مرتبط با فناوری) تشکیل شده است که برای تحقیق، توسعه، طراحی، تولید، تهیه، ادغام، عملیات، نگهداری، دفع و استفاده یا مدیریت محصولات و خدمات فناوری تعامل می‌کنند. این تعاملات توسط فناوری‌ها، قوانین، سیاست‌ها، رویه‌ها و روش‌ها شکل گرفته و تحت تأثیر آن‌ها قرار می‌گیرد. با توجه به ارتباطات پیچیده و پیوندهای متقابل در این اکوسیستم، مدیریت ریسک زنجیره تأمین (SCRM) برای سازمان‌ها اساسی است. مدیریت ریسک امنیت سایبری در زنجیره تأمین (C-SCRM) یک فرآیند سیستماتیک برای مدیریت بروزرسانی ریسک امنیت سایبری در سراسر زنجیره‌های تأمین و توسعه استراتژی‌ها، سیاست‌ها، رویه‌ها و روش‌های پاسخگویی مناسب است. زیرشاخه‌ها در دسته بندی C-SCRM چارچوب CSF اتصالی بین نتایجی که تنها بر روی امنیت سایبری تمرکز دارند و کسانی که بر روی C-SCRM تمرکز دارند، فراهم می‌کنند . SP 800-161r1(بازبینی 1) ، شیوه‌های مدیریت ریسک زنجیره تأمین امنیت سایبری برای سیستم‌ها و سازمان‌ها، اطلاعات عمیقی را در مورد C-SCRM ارائه می‌دهد.
- **ریسک‌های ناشی از فناوری‌های نوظهور:** هرگاه فناوری‌های جدید و کاربردهای جدید فناوری در دسترس قرار گیرند، ریسک‌های جدید مشخص می‌شوند. یک مثال معاصر، هوش مصنوعی (AI) است که ریسک‌های امنیت سایبری و حریم خصوصی دارد، همچنین انواع مختلف ریسک دیگر. چارچوب مدیریت ریسک هوش مصنوعی NIST (AI RMF) به منظور کمک به برخورد با این ریسک‌ها توسعه یافته است. برخورد با ریسک‌های AI در کنار سایر ریسک‌های سازمانی (مانند مالی، امنیت سایبری، شهرت و حریم خصوصی) به نتیجه یکپارچه‌تر و بهره‌وری‌های سازمانی منجر خواهد شد. در نظر گرفتن مدیریت ریسک امنیت سایبری و حریم خصوصی و رویکردهای آنها قابل اجرا برای طراحی، توسعه، استقرار، ارزیابی و استفاده از سیستم‌های هوش مصنوعی قابل استفاده است. هسته چارچوب AI RMF از توابع، دسته‌بندی‌ها و زیرشاخه‌ها برای توصیف نتایج AI استفاده می‌کند و کمک به مدیریت ریسک‌های مرتبط با AI می‌کند.

پیوست الف: هسته CSF

این پیوست وظایف، دسته‌ها و زیردسته‌های هسته CSF را توضیح می‌دهد. جدول ۱ نام‌ها و شناسه‌های الفبایی منحصربه‌فرد وظیفه و دسته‌های هسته CSF 2.0 را فهرست می‌کند. هر نام وظیفه در جدول به قسمت مربوطه از پیوست پیوند دارد. ترتیب وظایف، دسته‌ها و زیردسته‌های هسته به ترتیب الفبایی نیست؛ این امر برای بازتاب بهتر با کسانی که مسئول عملیاتی کردن مدیریت ریسک در یک سازمان هستند، طراحی شده است. شماره‌گذاری زیردسته‌ها با هدف متعمد عدم پیاپی بوده است؛ در اینجا، شکاف‌هایی در شماره‌گذاری نشان می‌دهد که زیردسته‌های CSF 1.1 که به CSF 2.0 منتقل شده‌اند.

جدول ۱. نام‌ها و شناسه‌های الفبایی منحصربه‌فرد وظیفه و دسته‌های هسته CSF 2.0

تابع	دسته	شناسه دسته
حاکمیت(GV)	زمینه سازمانی	GV.OC
	استراتژی مدیریت ریسک	GV.RM
	نقش‌ها، مسئولیت‌ها و اختیارات	GV.RR
	سیاست	GV.PO
	نظارت	GV.OV
	مدیریت ریسک زنجیره تامین سایبری	GV.SC
شناسایی(ID)	مدیریت دارایی	ID.AM
	ارزیابی ریسک	ID.RA
	بهبود	ID.IM
حفاظت(PR)	مدیریت هویت، احراز هویت و کنترل دسترسی	PR.AA
	آگاهی و آموزش	PR.AT
	امنیت داده	PR.DS
	امنیت پلتفرم	PR.PS
	استحکام زیرساخت فناوری	PR.IR
تشخیص(DE)	مانیتورینگ پیوسته	DE.CM
	تجزیه و تحلیل رویدادهای مخرب	DE.AE
پاسخ(RS)	مدیریت حوادث	RS.MA
	تجزیه و تحلیل حوادث	RS.AN
	گزارش‌دهی و ارتباطات پاسخ به حوادث	RS.CO

	کاهش اثرات حوادث	RS.MI
بازیابی(RC)	اجرای برنامه بازیابی حوادث	RC.PR
	ارتباطات بازیابی حوادث	RC.CO

هسته CSF، ارجاعات اطلاعاتی و مثال‌های اجرایی در وب‌سایت CSF 2.0 و از طریق ابزار مرجع CSF 2.0 قابل دسترسی هستند که به کاربران امکان مشاهده و خروجی‌گیری از آن‌ها در فرمت‌های قابل فهم برای انسان و ماشین را می‌دهد. همچنین، هسته CSF 2.0 در فرمت excel مشابه CSF 1.1 نیز قابل دسترسی است.

حاکمیت(GV): استراتژی، انتظارات و سیاست مدیریت ریسک امنیت سایبری سازمان تعیین، ارتباط داده شده و نظارت شده‌اند.

- **زمینه سازمانی(GV.OC)** : شرایط، ماموریت، انتظارات سهامداران، وابستگی‌ها، و الزامات قانونی، نظارتی و قراردادی، اطراف تصمیمات مدیریت ریسک امنیت سایبری سازمان درک شده‌اند.
  - **GV.OC-01:** ماموریت سازمان درک شده و در مدیریت ریسک امنیت سایبری تأثیرگذار است.
  - **GV.OC-02:** سهامداران داخلی و خارجی درک شده، و نیازها و انتظارات آن‌ها در مورد مدیریت ریسک امنیت سایبری درک شده و در نظر گرفته می‌شوند.
  - **GV.OC-03:** الزامات قانونی، نظارتی و قراردادی در مورد امنیت سایبری، شامل الزامات حریم خصوصی و آزادی‌های مدنی، درک و مدیریت می‌شوند.
  - **GV.OC-04:** اهداف، توانمندی‌ها و خدمات بحرانی که سهامداران خارجی به آن‌ها وابسته‌اند یا از سازمان انتظار دارند، درک شده و ارتباط داده شده‌اند.
  - **GV.OC-05:** نتایج، توانمندی‌ها و خدماتی که سازمان به آن‌ها وابسته است درک شده و ارتباط داده شده‌اند.
- **استراتژی مدیریت ریسک(GV.RM):** اولویت‌ها، محدودیت‌ها، اظهارات تحمل ریسک و انتهاپذیری، و فرضیات سازمان تعیین، ارتباط داده شده و برای پشتیبانی از تصمیم‌گیری‌های عملیاتی ریسک استفاده شده‌اند.
  - **GV.RM-01:** اهداف مدیریت ریسک توسط سهامداران سازمان تعیین و توافق شده‌اند.
  - **GV.RM-02:** بیانیه‌های تحمل ریسک و تحمل ریسک تعیین، ارتباط داده شده‌اند و حفظ می‌شوند.
  - **GV.RM-03:** فعالیت‌ها و نتایج مدیریت ریسک امنیت سایبری در فرآیندهای مدیریت ریسک سازمانی در نظر گرفته می‌شوند.
  - **GV.RM-04:** جهت‌گیری استراتژیک که گزینه‌های مناسب پاسخ به ریسک را توصیف می‌کند، تعیین و ارتباط داده شده‌اند.
  - **GV.RM-05:** خطوط ارتباطی در سراسر سازمان برای ریسک‌های امنیت سایبری، از جمله ریسک‌های از تأمین‌کنندگان و سومین اطراف دیگر، تعیین شده‌اند.

- **GV.RM-06:** روش استاندارد برای محاسبه، مستندسازی، طبقه‌بندی و اولویت‌بندی ریسک‌های امنیت سایبری تعیین و ارتباط داده شده‌اند.
- **GV.RM-07:** فرصت‌های استراتژیک (به عبارتی، ریسک‌های مثبت) تعیین شده و در گفتگوهای ریسک امنیت سایبری سازمانی شامل شده‌اند.

- **نقش‌ها، مسئولیت‌ها و اختیارات(GV.RR):** نقش‌ها، مسئولیت‌ها و اختیارات امنیت سایبری برای تقویت امتیاز، ارزیابی عملکرد و بهبود مستمر تعیین و ارتباط داده شده‌اند.
  - **GV.RR-01:** رهبر سازمان در قبال خطرات امنیت سایبری مسئول و پاسخگو است و فرهنگی را پرورش می دهد که آگاه به ریسک، اخلاقی و به طور مستمر در حال بهبود است.
  - **GV.RR-02:** نقش‌ها، مسئولیت‌ها و اختیارات مربوط به مدیریت ریسک امنیت سایبری تعیین، ارتباط داده شده، درک شده و اجرا می‌شوند.
  - **GV.RR-03:** منابع کافی بر اساس استراتژی ریسک امنیت سایبری، نقش‌ها، مسئولیت‌ها و سیاست‌های مدیریت شده‌اند.
  - **GV.RR-04:** امنیت سایبری در رویه‌های منابع انسانی شامل شده است.
- **سیاست(GV.PO):** سیاست سازمانی امنیت سایبری تعیین، ارتباط داده شده و اجرا می‌شود.
  - **GV.PO-01:** سیاست مدیریت ریسک‌های امنیت سایبری بر اساس سیاق سازمانی، استراتژی امنیت سایبری و اولویت‌ها تعیین و ارتباط داده شده و اجرا می‌شود.
  - **GV.PO-02:** سیاست مدیریت ریسک‌های امنیت سایبری بررسی، به‌روزرسانی، ارتباط داده شده و اجرا می‌شود تا تغییرات در الزامات، تهدیدها، فناوری و ماموریت سازمانی را منعکس کند.
- **نظارت(GV.OV):** نتایج فعالیت‌های مدیریت ریسک امنیت سایبری سراسر سازمان و عملکرد برای اطلاع‌رسانی، بهبود و تنظیم استراتژی مدیریت ریسک استفاده می‌شود.
  - **GV.OV-01:** نتایج استراتژی مدیریت ریسک امنیت سایبری بررسی شده و برای اطلاع‌رسانی و تنظیم استراتژی و جهت‌گیری مورد استفاده قرار می‌گیرد.
  - **GV.OV-02:** استراتژی مدیریت ریسک امنیت سایبری بررسی و تنظیم می‌شود تا اطمینان از پوشش الزامات و ریسک‌های سازمانی حاصل شود.
  - **GV.OV-03:** عملکرد مدیریت ریسک امنیت سایبری سازمانی برای ارزیابی و بررسی تنظیمات مورد نیاز به بررسی می‌شود.
- **مدیریت ریسک زنجیره تأمین امنیت سایبری(GV.SC):** فرآیندهای مدیریت ریسک زنجیره تأمین سایبری توسط ذینفعان سازمانی شناسایی، تعیین، مدیریت، نظارت و بهبود می‌شوند.
  - **GV.SC-01:** یک برنامه، استراتژی، اهداف، سیاست‌ها و فرآیندهای مدیریت ریسک زنجیره تأمین سایبری توسط ذینفعان سازمانی تعیین و توافق شده‌اند.

- **GV.SC-02**: نقش‌ها و مسئولیت‌های امنیت سایبری برای تامین‌کنندگان، مشتریان و شرکا درونی و خارجی تعیین، ارتباط داده شده و هماهنگ شده‌اند.
- **GV.SC-03**: مدیریت ریسک زنجیره تأمین سایبری در فرآیندهای مدیریت ریسک امنیت سایبری و ریسک مدیریت نرم‌افزاری و بهبود یکپارچه می‌شود.
- **GV.SC-04**: تامین‌کنندگان به عنوان مهم و اولویت‌بندی شده شناخته می‌شوند
- **GV.SC-05**: الزامات برای مدیریت ریسک‌های امنیت سایبری در زنجیره‌های تأمین تعیین، اولویت‌بندی و در توافقات و سایر انواع قراردادها با تامین‌کنندگان و سایر اشخاص ثالث مرتبط دیگر یکپارچه می‌شوند
- **GV.SC-06**: برنامه‌ریزی و دقت کار انجام می‌شود تا خطرات پیش از ورود به ارتباط رسمی با تامین‌کنندگان یا سایر اشخاص ثالث کاهش یابد.
- **GV.SC-07**: خطرات ایجاد شده توسط تامین‌کننده، محصولات و خدمات آنها و سایر اشخاص ثالث در طول ارتباط درک، ثبت، اولویت‌بندی، ارزیابی، پاسخگویی و نظارت مورد استفاده قرار می‌گیرند.
- **GV.SC-08**: تامین‌کنندگان مربوطه و سایر اشخاص ثالث در برنامه‌های برنامه‌ریزی، پاسخگویی و بازیابی حادثه مشمول می‌شوند.
- **GV.SC-09**: شیوه‌های امنیتی زنجیره تأمین در برنامه‌های مدیریت ریسک امنیتی و مدیریت ریسک نرم‌افزاری یکپارچه شده‌اند و عملکرد آنها در طول چرخه عمر محصول و خدمات فناوری نظارت می‌شود.
- **GV.SC-10**: برنامه‌های مدیریت ریسک زنجیره تأمین امنیت سایبری شامل اقداماتی برای فعالیت‌هایی که پس از پایان توافق یا توافق خدمات رخ می‌دهد، مطالعه می‌شود.

شناسایی(ID): ریسک‌های امنیتی فعلی سازمان درک شده‌اند.

- **مدیریت دارایی‌ها(ID.AM)**: دارایی‌ها (مانند داده‌ها، سخت‌افزار، نرم‌افزار، سیستم‌ها، امکانات، خدمات، افراد) به سازمان کمک می‌کنند تا اهداف کسب و کار خود را دست‌یابی کنند، شناسایی و مدیریت می‌شوند که با اهمیت نسبی خود به اهداف سازمانی و استراتژی ریسک سازمان هماهنگ باشند.
  - **ID.AM-01**: موجودی سخت‌افزار توسط سازمان حفظ می‌شود.
  - **ID.AM-02**: موجودی نرم‌افزارها، خدمات و سیستم‌های توسط سازمان حفظ می‌شود.
  - **ID.AM-03**: نمایندگی از ارتباطات شبکه مجاز و داده‌های داخلی و خارجی شبکه سازمان حفظ می‌شود.
  - **ID.AM-04**: موجودی خدمات ارائه شده توسط تامین‌کنندگان حفظ می‌شود.
  - **ID.AM-05**: دارایی‌ها بر اساس طبقه‌بندی، اهمیت، منابع و تأثیر بر ماموریت اولویت‌بندی می‌شوند.

- **ID.AM-07**: موجودی داده‌ها و metadataهای متناظر برای انواع داده‌های تعیین شده حفظ می‌شود.
- **ID.AM-08**: سیستم‌ها، سخت‌افزار، نرم‌افزارها، خدمات و داده‌ها در طول چرخه عمر آنها مدیریت می‌شوند.

- **ارزیابی ریسک(ID.RA)**: ریسک امنیتی برای سازمان، دارایی‌ها و افراد توسط سازمان درک می‌شود.
  - **ID.RA-01**: آسیب‌پذیری‌های دارایی‌ها شناسایی، تأیید و ثبت می‌شوند.
  - **ID.RA-02**: Threat Intelligence از انجمن‌ها و منابع به اشتراک‌گذاری اطلاعات دریافت می‌شود.
  - **ID.RA-03**: تهدیدات داخلی و خارجی به سازمان شناسایی و ثبت می‌شوند.
  - **ID.RA-04**: اثرات و احتمالات Exploit آسیب‌پذیری‌ها توسط تهدیدات، شناسایی و ثبت می‌شوند.
  - **ID.RA-05**: تهدیدات، آسیب‌پذیری‌ها، احتمالات و اثرات برای درک ریسک ذاتی استفاده می‌شوند و اولویت‌بندی پاسخ ریسک را مطلع می‌کنند.
  - **ID.RA-06**: پاسخ‌های ریسک انتخاب شده، اولویت‌بندی شده، برنامه‌ریزی شده، پیگیری شده و ارتباط داده می‌شوند.
  - **ID.RA-07**: تغییرات و استثناها مدیریت می‌شوند، برای اثرات ریسک ارزیابی می‌شوند، ثبت می‌شوند و پیگیری می‌شوند.
  - **ID.RA-08**: فرآیندهای دریافت، تجزیه و تحلیل و پاسخ به افشاس آسیب‌پذیری تعیین شده‌اند.
  - **ID.RA-09**: اعتبار و صحت سخت‌افزار و نرم‌افزار قبل از تهیه و استفاده ارزیابی می‌شود.
  - **ID.RA-10**: تأمین‌کنندگان حیاتی قبل از تهیه ارزیابی می‌شوند.
- **بهبود(ID.IM)**: بهبودهایی در فرآیندها، روش‌ها و فعالیت‌های مدیریت ریسک امنیت سایبری سازمان در تمامی توابع CSF شناسایی می‌شوند.
  - **ID.IM-01**: بهبودها از ارزیابی‌ها شناسایی می‌شوند.
  - **ID.IM-02**: بهبودها از آزمون‌ها و تمرین‌های امنیتی شناسایی می‌شوند، از جمله آن‌هایی که همراه با تامین‌کنندگان و سومین‌های مرتبط انجام می‌شوند.
  - **ID.IM-03**: بهبودها از اجرای فرآیندها، روش‌ها و فعالیت‌های عملیاتی شناسایی می‌شوند.
  - **ID.IM-04**: برنامه‌های پاسخ به حوادث و سایر برنامه‌های امنیتی که بر عملکرد تأثیر می‌گذارند، تعیین، ارتباط داده، حفظ و بهبود می‌شوند.

حفاظت(PR): تدابیری که برای مدیریت ریسک‌های امنیت سازمان استفاده می‌شوند.

- **مدیریت هویت، احراز هویت و کنترل دسترسی(PR.AA)**: دسترسی به دارایی‌های فیزیکی و منطقی محدود به کاربران، خدمات و سخت‌افزارهای مجاز است و مدیریت می‌شود که با ریسک دسترسی غیرمجاز ارزیابی شده متناسب باشد.

- **PR.AA-01:** هویت و اعتبارهای کاربران، خدمات و سخت‌افزارهای مجاز توسط سازمان مدیریت می‌شوند.
- **PR.AA-02:** هویت‌ها بر اساس زمینه تعاملات اثبات و به اعتبار می‌آیند.
- **PR.AA-03:** کاربران، خدمات و سخت‌افزارها تأیید احراز هویت می‌شوند.
- **PR.AA-04:** ادعاهای هویت حفظ، انتقال و اعتبارسنجی می‌شوند.
- **PR.AA-05:** مجوزهای دسترسی، اختیارات و اجازه‌ها در یک سیاست تعریف شده، مدیریت، اجرا و بازبینی می‌شوند و اصول کمترین اختیار و جداسازی وظایف را دربرمی‌گیرند.
- **PR.AA-06:** دسترسی فیزیکی به دارایی‌ها مطابق با ریسک، مدیریت، نظارت و اجرا می‌شود.

- **آگاهی و آموزش(PR.AT):** کارکنان سازمان با آگاهی و آموزش امنیت سایبری فراهم می‌شوند تا بتوانند وظایف مرتبط با امنیت سایبری خود را انجام دهند.
  - **PR.AT-01:** کارکنان با آگاهی و آموزش فراهم شده، دانش و مهارت‌های لازم را برای انجام وظایف عمومی با ریسک‌های امنیتی در ذهن داشته باشند.
  - **PR.AT-02:** افراد در نقش‌های ویژه با آگاهی و آموزش فراهم شده، دانش و مهارت‌های لازم را برای انجام وظایف مرتبط با ریسک‌های امنیتی در ذهن داشته باشند.
- **امنیت داده‌ها (PR.DS)** داده‌ها به‌طور سازمانی با استراتژی ریسک سازمان مدیریت می‌شوند تا محرمانگی، صحت و دسترسی آن‌ها تضمین شود.
  - **PR.DS-01:** محرمانگی، صحت و دسترسی داده‌های در استراحت حفاظت می‌شوند.
  - **PR.DS-02:** محرمانگی، صحت و دسترسی داده‌های در حال انتقال حفاظت می‌شوند.
  - **PR.DS-10:** محرمانگی، صحت و دسترسی داده‌های در حال استفاده حفاظت می‌شوند.
  - **PR.DS-11:** پشتیبان‌های داده ایجاد، حفاظت، حفظ و آزمایش می‌شوند.
- **امنیت پلتفرم(PR.PS):** سخت‌افزارها، نرم‌افزارها (مانند نرم‌افزار ریزبرنامه، سیستم‌های عامل، برنامه‌ها) و خدمات پلتفرم‌های فیزیکی و مجازی مطابق با استراتژی ریسک سازمان مدیریت می‌شوند تا محرمانگی، صحت و دسترسی آن‌ها تضمین شود.
  - **PR.PS-01:** روش‌های مدیریت پیکربندی تعیین و اعمال می‌شوند.
  - **PR.PS-02:** نرم‌افزارها با ریسک تعمیر، تعویض و حذف می‌شوند.
  - **PR.PS-03:** سخت‌افزارها با ریسک تعمیر، تعویض و حذف می‌شوند.
  - **PR.PS-04:** رکوردهای ورودی ایجاد و برای نظارت مداوم در دسترس قرار می‌گیرند.
  - **PR.PS-05:** نصب و اجرای نرم‌افزارهای غیرمجاز جلوگیری می‌شود.
  - **PR.PS-06:** روش‌های توسعه نرم‌افزار امن به روش‌های توسعه نرم‌افزار ترکیب می‌شوند و عملکرد آن‌ها در طول چرخه عمر توسعه نرم‌افزار نظارت می‌شود.

- **انعطاف‌پذیری زیرساخت فناوری(PR.IR)**: معماری‌های امنیتی با استراتژی ریسک سازمان مدیریت می‌شوند تا محرمانگی، صحت و دسترسی دارایی‌ها و انعطاف‌پذیری سازمانی تضمین شود.
  - **PR.IR-01**: شبکه‌ها و محیط‌ها از دسترسی منطقی و استفاده غیرمجاز حفاظت می‌شوند.
  - **PR.IR-02**: دارایی‌های فناوری سازمان از تهدیدات محیطی حفاظت می‌شوند.
  - **PR.IR-03**: مکانیزم‌ها برای دستیابی به الزامات انعطاف‌پذیری در شرایط عادی و نامطلوب اجرا می‌شوند.
  - **PR.IR-04**: ظرفیت منابع کافی برای اطمینان از دسترسی به حفظ شده است.

تشخیص(DE): حملات و تخلفات امنیتی احتمالی شناسایی و تجزیه و تحلیل می‌شوند.

- **مانیتورینگ پیوسته(DE.CM)**: دارایی‌ها برای یافتن ناهنجاری‌ها، نشانه های نفوذ و سایر رویدادهای مخرب احتمالی نظارت می‌شوند.
  - **DE.CM-01**: شبکه‌ها و سرویس‌های شبکه برای یافتن رویدادهای احتمالاً مخرب نظارت می‌شوند.
  - **DE.CM-02**: محیط فیزیکی برای یافتن رویدادهای احتمالاً مخرب نظارت می‌شود.
  - **DE.CM-03**: فعالیت‌های پرسنل و استفاده از فناوری برای یافتن رویدادهای احتمالاً مخرب نظارت می‌شوند.
  - **DE.CM-06**: فعالیت‌ها و خدمات ارائه دهندگان خدمات خارجی برای یافتن رویدادهای احتمالاً مخرب نظارت می‌شوند.
  - **DE.CM-09**: سخت‌افزار و نرم‌افزارهای محاسباتی، محیط‌های اجرا و داده‌های آنها برای یافتن رویدادهای احتمالاً مخرب نظارت می‌شوند.
- **تجزیه و تحلیل رویدادهای مخرب(DE.AE)**: ناهنجاری‌ها، نشانگرهای تخلف و سایر رویدادهای احتمالاً مخرب برای شناسایی رویدادهای امنیتی تجزیه و تحلیل می‌شوند.
  - **DE.AE-02**: رویدادهای احتمالاً مخرب برای بهتر فهمیدن فعالیت‌های مرتبط با آن‌ها تجزیه و تحلیل می‌شوند.
  - **DE.AE-03**: اطلاعات از منابع متعدد همزمان متناظر می‌شوند.
  - **DE.AE-04**: تأثیر و محدوده احتمالی رویدادهای مخرب درک می‌شوند.
  - **DE.AE-06**: اطلاعات مربوط به رویدادهای مخرب به کارکنان مجاز و ابزارها ارائه می‌شوند.
  - **DE.AE-07**: Threat Intelligence و سایر اطلاعات زمینه‌ای در تجزیه و تحلیل یکپارچه می‌شوند.
  - **DE.AE-08**: حوادث زمانی اعلام می‌شوند که رویدادهای مخرب با معیارهای تعریف شده برای وقوع حادثه تطابق دارند.

پاسخ(RS): اقدامات مربوط به یک حادثه امنیت سایبری شناسایی شده، انجام می‌شود.

- **مدیریت حوادث(RS.MA):** پاسخ‌ها به حوادث امنیت سایبری شناسایی شده مدیریت می‌شود.
  - **RS.MA-01:** برنامه واکنش به حادثه در هماهنگی با نهادهای مربوط شروع به اجرا می‌کند یکبار یک حادثه اعلام شود.
  - **RS.MA-02:** گزارش‌های حادثه تریاژ و تأیید می‌شوند.
  - **RS.MA-03:** حوادث دسته‌بندی و اولویت‌بندی می‌شوند.
  - **RS.MA-04:** حوادث در صورت نیاز افزایش یا افزایش می‌یابند.
  - **RS.MA-05:** معیارهای شروع بازیابی حادثه اعمال می‌شود.
- **تجزیه و تحلیل حوادث(RS.AN):** برای اطمینان از پاسخ مؤثر و پشتیبانی از فانرزیک و فعالیت‌های بازیابی، تحقیقات انجام می‌شود.
  - **RS.AN-03:** تجزیه و تحلیلی انجام می‌شود تا بفهمیم چه اتفاقی در طول یک حادثه رخ داده است و علت اصلی حادثه چیست.
  - **RS.AN-06:** اقدامات انجام شده در طول یک تحقیق ثبت می‌شوند و صحت و اصالت سوابق حفظ می‌شود.
  - **RS.AN-07:** داده‌ها و metadata حادثه جمع‌آوری می‌شوند و صحت و اصالت آنها حفظ می‌شود.
  - **RS.AN-08:** بزرگی یک حادثه تخمین زده شده و تأیید می‌شود.
- **گزارش و ارتباطات پاسخ به حوادث(RS.CO):** فعالیت‌های پاسخ به عنوان درخواست شده توسط قوانین، مقررات یا سیاست‌ها با نهادهای داخلی و خارجی هماهنگ می‌شود.
  - **RS.CO-02:** نهادهای داخلی و خارجی از حوادث مطلع می‌شوند.
  - **RS.CO-03:** اطلاعات با نهادهای داخلی و خارجی مشخص به اشتراک گذاشته می‌شود.
- **کاهش حوادث(RS.MI):** فعالیت‌ها برای جلوگیری از گسترش یک رویداد و کاهش اثرات آن انجام می‌شود.
  - **RS.MI-01:** حوادث محدود می‌شوند.
  - **RS.MI-02:** حوادث از بین می‌روند.

بازیابی(RC): دارایی‌ها و عملیات تحت تأثیر حادثه امنیت سایبری بازیابی می‌شوند.

- **اجرای برنامه بازیابی حوادث(RC.RP):** فعالیت‌های بازیابی انجام می‌شود تا اطمینان از دسترسی عملیاتی سیستم‌ها و خدمات تحت تأثیر حوادث امنیت سایبری حاصل شود.
  - **RC.RP-01:** بخش بازیابی برنامه واکنش به حادثه اجرا می‌شود یکبار از فرآیند واکنش به حادثه شروع شود.

- **RC.RP-02**: اقدامات بازیابی انتخاب می‌شوند، محدوده‌بندی، اولویت‌بندی و انجام می‌شوند.
- **RC.RP-03**: صحت پشتیبان‌ها و سایر دارایی‌های بازیابی قبل از استفاده از آنها برای بازیابی تأیید می‌شود.
- **RC.RP-04**: عملکردهای مهم مأموریتی و مدیریت ریسک امنیت سایبری برای تأسیس نرمال‌های عملیاتی پس از حادثه موردنظر قرار می‌گیرند.
- **RC.RP-05**: صحت دارایی‌های بازیابی تأیید شده، سیستم‌ها و خدمات بازیابی می‌شوند و وضعیت عملیاتی نرمال تأیید می‌شود.
- **RC.RP-06**: پایان بازیابی حادثه براساس معیارها اعلام می‌شود، و مستندات مربوط به حادثه کامل می‌شوند.

- **ارتباط بازیابی حوادث(RC.CO)**: فعالیت‌های بازیابی با ارکان داخلی و خارجی هماهنگ می‌شود.
  - **RC.CO-03**: فعالیت‌های بازیابی و پیشرفت در بازیابی قابلیت‌های عملیاتی به نهادهای مشخص داخلی و خارجی اطلاع داده می‌شود.
  - **RC.CO-04**: به‌روزرسانی‌های عمومی درباره بازیابی حادثه با استفاده از روش‌ها و پیام‌رسانی‌های تأیید شده به اشتراک گذاشته می‌شود.

پیوست ب: سطوح CSF

جدول 2 تصویر مفهومی از سطوح CSF می‌باشد که در بخش 3 بحث شده است. این سطوح، میزان شدت شیوه‌های حاکمیت ریسک امنیت سایبری (GOVERN) و شیوه‌های مدیریت ریسک امنیت سایبری (IDENTIFY، PROTECT، DETECT، RESPOND و RECOVER) یک سازمان را مشخص می‌کنند.

سطح	حاکمیت ریسک امنیت سایبری	مدیریت ریسک امنیت سایبری
سطح 1	تدبیر اجرای استراتژی ریسک امنیت سایبری سازمان به صورت نامنظم مدیریت می‌شود. اولویت‌بندی به صورت نامنظم انجام می‌شود و بر اساس هدف‌ها یا محیط تهدید به طور رسمی مبتنی نمی‌شود.	در سطح سازمانی آگاهی محدودی از خطرات امنیت سایبری وجود دارد. سازمان مدیریت ریسک امنیت سایبری را به صورت نامنظم و موردی اجرا می‌کند. ممکن است در سازمان فرآیندهایی برای به اشتراک گذاری اطلاعات امنیت سایبری در داخل سازمان وجود نداشته باشد. سازمان به طور کلی از خطرات امنیت سایبری مرتبط با تأمین کنندگان خود و محصولات و خدماتی که تأمین و استفاده می‌کند، آگاه نیست.
سطح 2	روش‌های مدیریت ریسک توسط مدیریت تأیید می‌شوند اما ممکن است به عنوان یک سیاست سازمانی به طور کلی تعیین نشده باشند. اولویت‌بندی فعالیت‌ها و نیازهای مربوط به امنیت سایبری مستقیماً توسط اهداف ریسک سازمانی، محیط تهدید یا الزامات تجاری/ماموریتی مطلع می‌شود.	در سطح سازمانی، آگاهی از ریسک‌های سایبری وجود دارد، اما یک رویکرد سازمانی جامع برای مدیریت این ریسک‌ها تأسیس نشده است. در نظر گرفتن امنیت سایبری در اهداف و برنامه‌های سازمان ممکن است در برخی از سطوح سازمان رخ دهد، اما در همه سطوح سازمانی اتفاق نمی‌افتد. ارزیابی ریسک سایبری برای دارایی‌های داخلی و خارجی سازمان انجام می‌شود، اما به طور معمول قابل تکرار یا دوره‌ای نیست. اطلاعات سایبری در سازمان به صورت غیررسمی به اشتراک گذاشته می‌شود. سازمان از ریسک‌های سایبری مرتبط با تامین‌کنندگان و محصولات و خدماتی که تهیه و استفاده می‌کند، آگاه است، اما به طور مداوم یا رسمی برای مقابله با این ریسک‌ها عمل نمی‌کند.
سطح 3	روش‌های مدیریت ریسک سازمان به صورت رسمی تأیید و به عنوان سیاست بیان می‌شوند. سیاست‌ها، فرآیندها و رویه‌های براساس ریسک تعریف شده، به عنوان انتظار و بررسی، اجرا می‌شوند. روش‌های سایبری سازمان به طور منظم بر اساس اعمال فرآیندهای مدیریت ریسک به تغییرات در الزامات تجاری/ماموریتی، تهدیدات و منظر فناورانه به‌روزرسانی می‌شوند.	یک رویکرد سازمانی جامع برای مدیریت ریسک‌های سایبری وجود دارد. اطلاعات سایبری به طور مداوم در سراسر سازمان به اشتراک گذاشته می‌شود. روش‌های مداومی برای پاسخگویی به تغییرات در ریسک وجود دارد. کارکنان دانش و مهارت‌های لازم برای انجام نقش‌ها و مسئولیت‌های خود را دارند. سازمان به طور مداوم و دقیق ریسک‌های سایبری دارایی‌ها را نظارت می‌کند. مدیران ارشد سایبری و غیر سایبری به طور منظم درباره ریسک‌های سایبری ارتباط برقرار می‌کنند. مدیران اطمینان حاصل می‌کنند که در نظر گرفتن سایبری در تمامی خطوط عملیاتی سازمان در نظر گرفته شده است. استراتژی ریسک سازمان با ریسک‌های سایبری مرتبط با تأمین‌کنندگان

		و محصولات و خدماتی که تهیه و استفاده می‌شود، اطلاع‌رسانی می‌شود. کارکنان به طور رسمی بر ریسک‌های مربوطه عمل می‌کنند از طریق مکانیسم‌هایی مانند توافق‌نامه‌های کتبی برای ارتباط پایه، ساختارهای حاکمیتی (مانند شورای ریسک)، و اجرا و نظارت بر سیاست‌ها. این اقدامات به صورت مداوم و به طور معمول اجرا و نظارت می‌شوند و بررسی می‌شوند.
سطح 4	یک رویکرد سازمانی جامع برای مدیریت ریسک‌های سایبری وجود دارد که از سیاست‌ها، فرآیندها و رویه‌های مبتنی بر ریسک برای پرداختن به رویدادهای سایبری پیش بینی‌شده استفاده می‌کند. ارتباط بین ریسک‌های سایبری و اهداف سازمان به طور واضح درک شده و در هنگام تصمیم‌گیری‌ها در نظر گرفته می‌شود. مدیران، ریسک‌های سایبری را در همان سیاقی که ریسک‌های مالی و دیگر ریسک‌های سازمانی را نظارت می‌کنند. بودجه سازمان بر اساس درک محیط و ریسک فعلی و پیش‌بینی‌شده و تحمل ریسک تعیین می‌شود. واحدهای تجاری اجرایی، دیدگاه مدیران را پیاده‌سازی می‌کنند و ریسک‌های سیستمی را با توجه به تحمل ریسک‌های سازمانی تجزیه و تحلیل می‌کنند. مدیریت ریسک سایبری بخشی از فرهنگ سازمان است. این از آگاهی از فعالیت‌های قبلی و آگاهی مداوم از فعالیت‌هایی در سیستم‌ها و شبکه‌های سازمان بوجود می‌آید. سازمان قادر است با سرعت و کارآمدی تغییرات در اهداف تجاری/ماموریتی را در نحوه پیش‌گیری و ارتباط‌دهی به ریسک مد نظر درآورد.	سازمان نیازمند بهینه‌سازی مداوم نگرش‌های سایبری خود بر اساس فعالیت‌های سایبری گذشته و کنونی، از جمله درس‌هایی که یادگرفته‌اند و شاخص‌های پیش‌بینی. از طریق یک فرآیند بهبود مداوم که فناوری‌ها و روش‌های پیشرو در حوزه سایبری را در بر می‌گیرد، سازمان به طور فعال در برابر چشم‌انداز فناوری‌ای که در حال تغییر است و به صورت به موقع و مؤثر در برابر تهدیدهای پیشرفته و پیچیده واکنش نشان می‌دهد. سازمان از اطلاعات به صورت زمان واقعی یا نزدیک به زمان واقعی استفاده می‌کند تا از ریسک‌های سایبری مرتبط با تأمین‌کنندگان و محصولات و خدماتی که تهیه و استفاده می‌شود، درک کند و به طور مداوم بر این اساس عمل کند. اطلاعات سایبری به طور مداوم در سراسر سازمان و با شرکای مجاز به اشتراک گذاشته می‌شود.