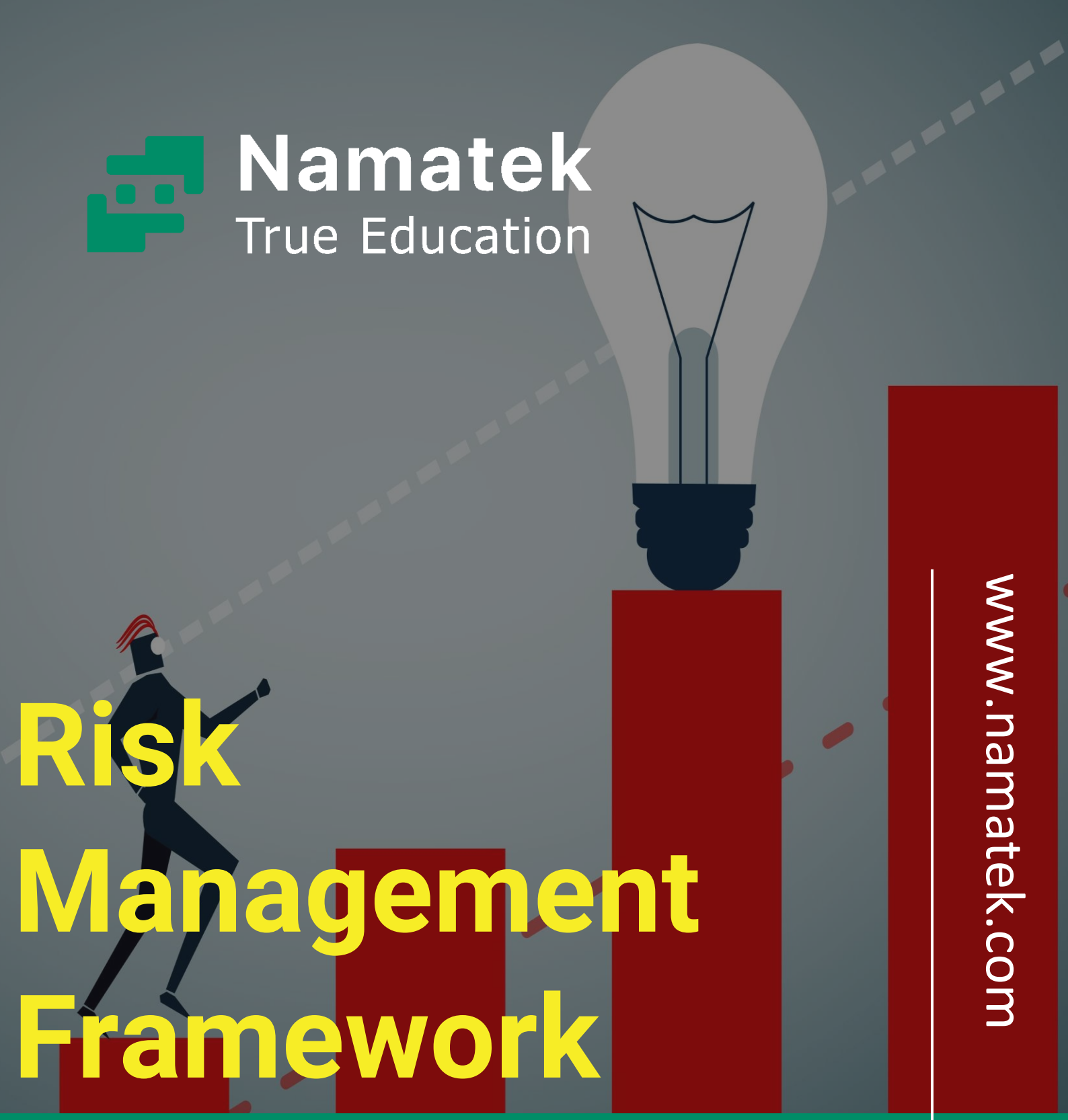
Namatek
True Education



Risk Management Framework

www.namatek.com

rmf چیست؟

فهرست مطالب

مدیریت ریسک به عنوان یکی از مهم‌ترین وظایف سازمان‌ها شناخته می‌شود. با افزایش تهدیدات امنیتی، تغییرات سریع فناوری و پیچیدگی‌های قانونی، سازمان‌ها نیازمند رویکردهای جامع و سیستماتیک برای مدیریت ریسک‌های خود هستند. چارچوب مدیریت ریسک (RMF) به عنوان یک ابزار کارآمد و جامع، به سازمان‌ها کمک می‌کند تا ریسک‌های خود را به طور مؤثر شناسایی، ارزیابی و مدیریت کنند؛ اما rmf چیست؟

این چارچوب که توسط موسسه ملی استانداردها و فناوری (NIST) توسعه یافته است، به سازمان‌ها امکان می‌دهد تا ریسک‌های مرتبط با امنیت اطلاعات، حریم خصوصی و سایر جنبه‌های کسب‌وکار را به دقت کنترل کنند.

در ادامه با ما همراه باشید.

RMF چیست؟

در پاسخ به سوال rmf چیست می‌توان گفت چارچوب مدیریت ریسک (Risk Management Framework) مجموعه‌ای از فرآیندها و روش‌ها است که به سازمان‌ها کمک می‌کند تا ریسک‌های خود را به طور مؤثر مدیریت کنند. این چارچوب به سازمان‌ها امکان می‌دهد تا ریسک‌های

مرتبط با امنیت اطلاعات، حریم خصوصی و زنجیره تأمین را شناسایی و کنترل کنند.

RMF به عنوان یک راهنمای جامع برای مدیریت ریسک‌های امنیتی و حریم خصوصی در سازمان‌ها طراحی شده است. این چارچوب توسط موسسه ملی استانداردها و فناوری (NIST) توسعه یافته و به سازمان‌ها کمک می‌کند تا فرآیندهای خود را بهبود بخشند و از منابع خود به بهترین شکل استفاده کنند.

اهمیت RMF در مدیریت ریسک چیست؟

چارچوب مدیریت ریسک (RMF) نقش بسیار مهمی در مدیریت ریسک‌های سازمانی ایفا می‌کند. این چارچوب به سازمان‌ها کمک می‌کند تا به طور جامع و سیستماتیک ریسک‌های خود را شناسایی و ارزیابی کنند که در نهایت منجر به بهبود عملکرد بلند مدت می‌شود. همچنین به سازمان‌ها امکان می‌دهد تا تصمیم‌گیری‌های بهتری انجام دهند و از وقوع حوادث ناگوار جلوگیری کنند. RMF به سازمان‌ها کمک می‌کند تا با مقررات و استانداردهای مرتبط تطابق داشته باشند و اعتماد ذینفعان را جلب کنند.

یک RMF موثر به دنبال محافظت از سرمایه و درآمد یک سازمان، بدون ایجاد مانع در رشد خواهد بود. علاوه بر این سرمایه گذاران تمایل بیشتری برای سرمایه گذاری در شرکت‌هایی با شیوه‌های مدیریت ریسک خوب خواهند داشت.

اجزای اصلی RMF چیست؟

چارچوب مدیریت ریسک (RMF) شامل چندین بخش است که هر کدام نقش مهمی در مدیریت ریسک دارند. در ادامه بررسی می‌کنیم که مفهوم هریک از این اجزا در RMF چیست؟

- **شناسایی ریسک‌ها:** سازمان‌ها باید تمامی ریسک‌های ممکن را شناسایی کنند. این مرحله شامل ریسک‌های مرتبط با فناوری اطلاعات، عملیات، مقررات، قانونی، سیاسی و استراتژیک است.
- **ارزیابی و اندازه‌گیری ریسک‌ها:** پس از شناسایی ریسک‌ها، سازمان‌ها باید میزان و احتمال وقوع هر ریسک را ارزیابی کنند. این ارزیابی به سازمان‌ها کمک می‌کند تا تأثیر هر ریسک بر عملکرد کلی سازمان را درک کنند.

- **کاهش ریسک‌ها:** سازمان‌ها باید استراتژی‌هایی برای کاهش ریسک‌ها انتخاب کنند. این استراتژی‌ها می‌توانند شامل پیاده‌سازی کنترل‌های امنیتی، تغییر فرآیندها یا استفاده از بیمه باشند.
- **گزارش‌دهی و نظارت:** سازمان‌ها باید به طور مداوم ریسک‌ها و کنترل‌های مرتبط با آن‌ها را نظارت کنند و گزارش‌های دوره‌ای تهیه کنند. این نظارت به سازمان‌ها کمک می‌کند تا به موقع به تغییرات و تهدیدات جدید پاسخ دهند.
- **حاکمیت:** حاکمیت به سازمان‌ها کمک می‌کند تا اطمینان حاصل کنند که تمامی افراد در سازمان به درستی وظایف خود را انجام می‌دهند و فرآیندهای مدیریت ریسک به درستی اجرا می‌شوند.

تا به اینجا متوجه شدیم که مفهوم RMF چیست و از چه اجزایی تشکیل شده است. برای استفاده از این چهارچوب نیاز به انجام مراحلی است که در ادامه این مقاله هریک از این مراحل را بررسی می‌کنیم.

مرحله آماده‌سازی

مراحل آماده سازی rmf چیست؟ این مرحله شامل فعالیت‌های ضروری است که باید در سطح سازمان، فرآیندهای کسب‌وکار و سیستم‌های اطلاعاتی انجام شود.

- **تعیین نقش‌ها و مسئولیت‌ها:** سازمان‌ها باید نقش‌ها و مسئولیت‌های کلیدی در مدیریت ریسک را تعیین کنند. این شامل تعیین مسئولیت‌های مدیران ارشد، مدیران امنیت اطلاعات و سایر افراد مرتبط با مدیریت ریسک است.
- **تدوین استراتژی مدیریت ریسک:** سازمان‌ها باید یک استراتژی جامع برای مدیریت ریسک‌های خود تدوین کنند. این استراتژی باید شامل تعیین تحمل ریسک، اهداف مدیریت ریسک و روش‌های ارزیابی ریسک و کاهش آن باشد.
- **ارزیابی ریسک سازمانی:** سازمان‌ها باید یک ارزیابی جامع از ریسک‌های خود انجام دهند. این ارزیابی شامل شناسایی ریسک‌های مرتبط با امنیت اطلاعات، حریم خصوصی و سایر جنبه‌های کسب‌وکار است.
- **توسعه و پیاده‌سازی استراتژی نظارت مداوم:** سازمان‌ها باید یک استراتژی برای نظارت مداوم بر ریسک‌ها و کنترل‌های امنیتی خود توسعه دهند و پیاده‌سازی کنند. این استراتژی به سازمان‌ها کمک می‌کند تا به موقع به تغییرات و تهدیدات جدید پاسخ دهند.
- **شناسایی کنترل‌های مشترک:** سازمان‌ها باید کنترل‌های امنیتی مشترک را شناسایی کنند که می‌توانند در سراسر سازمان استفاده

شوند. این کنترل‌ها به سازمان‌ها کمک می‌کنند تا به طور مؤثرتر ریسک‌های خود را مدیریت کنند.

مرحله دسته‌بندی

این مرحله به سازمان‌ها امکان می‌دهد تا ریسک‌های مرتبط با هر سیستم را شناسایی و مدیریت کنند.

- **شناسایی انواع اطلاعات:** سازمان‌ها باید انواع اطلاعاتی که سیستم‌ها پردازش، ذخیره و منتقل می‌کنند را شناسایی کنند. این اطلاعات می‌تواند شامل داده‌های حساس، اطلاعات شخصی و اطلاعات مالی باشد.
- **انتخاب سطح تأثیر موقت:** سازمان‌ها باید سطح تأثیر موقت برای هر نوع اطلاعات را انتخاب کنند. این سطح تأثیر بر اساس تحلیل تأثیرات احتمالی از دست دادن محرمانگی، یکپارچگی و دسترسی‌پذیری اطلاعات تعیین می‌شود.
- **بازبینی و نهایی‌سازی سطح تأثیر:** سازمان‌ها باید سطح تأثیر موقت را بازبینی و نهایی‌سازی کنند. این بازبینی به سازمان‌ها کمک می‌کند تا

اطمینان حاصل کنند که سطح تأثیر به درستی تعیین شده است و تمامی جنبه‌های مرتبط با ریسک‌ها در نظر گرفته شده‌اند.

- **تعیین دسته‌بندی امنیتی سیستم:** سازمان‌ها باید دسته‌بندی امنیتی سیستم را تعیین کنند. این دسته‌بندی شامل تعیین سطح تأثیر کلی سیستم بر اساس تحلیل تأثیرات احتمالی از دست دادن محرمانگی، یکپارچگی و دسترسی‌پذیری اطلاعات است.
- **مستندسازی دسته‌بندی:** سازمان‌ها باید دسته‌بندی امنیتی سیستم و سطح تأثیر کلی را مستندسازی کنند. این مستندسازی به سازمان‌ها کمک می‌کند تا اطلاعات مربوط به دسته‌بندی را به طور دقیق و جامع ثبت کنند و در صورت نیاز به آن‌ها دسترسی داشته باشند.

مرحله انتخاب

این مرحله به سازمان‌ها امکان می‌دهد تا از اطلاعات و سیستم‌های خود محافظت کنند.

- **انتخاب کنترل‌های امنیتی:** سازمان‌ها باید مجموعه‌ای از کنترل‌های امنیتی را بر اساس ارزیابی ریسک انتخاب کنند. این کنترل‌ها

می‌توانند شامل کنترل‌های فنی، مدیریتی و فیزیکی باشند که به کاهش ریسک‌های شناسایی شده کمک می‌کنند.

- **تنظیم و تطبیق کنترل‌ها:** سازمان‌ها باید این کنترل‌ها را تنظیم کنند و تطبیق دهند تا با نیازها و شرایط خاص سازمان هماهنگ شوند. این تنظیم و تطبیق به سازمان‌ها کمک می‌کند تا کنترل‌ها به طور مؤثرتر اجرا شوند.
- **مستندسازی کنترل‌ها:** سازمان‌ها باید کنترل‌های انتخاب شده را مستندسازی کنند. این مستندسازی شامل توضیح نحوه اجرای کنترل‌ها، مسئولیت‌ها و فرآیندهای مرتبط با آن‌ها است.
- **توسعه استراتژی نظارت مداوم:** سازمان‌ها باید یک استراتژی برای نظارت مداوم بر اجرای کنترل‌های امنیتی توسعه دهند. این استراتژی به سازمان‌ها کمک می‌کند تا به موقع به تغییرات و تهدیدات جدید پاسخ دهند و اطمینان حاصل کنند که کنترل‌ها به درستی اجرا می‌شوند.
- **ارزیابی و بازبینی کنترل‌ها:** سازمان‌ها باید به طور دوره‌ای کنترل‌های امنیتی را ارزیابی و بازبینی کنند. این ارزیابی به سازمان‌ها کمک می‌کند تا نقاط ضعف را شناسایی و اصلاح کنند و اطمینان حاصل کنند که کنترل‌ها به درستی عمل می‌کنند.

مرحله پیاده‌سازی

این مرحله به سازمان‌ها امکان می‌دهد تا اطمینان حاصل کنند که کنترل‌ها به درستی پیاده‌سازی شده‌اند و به اهداف مورد نظر دست یافته‌اند.

- **اجرای کنترل‌های امنیتی :**در این مرحله، سازمان‌ها باید کنترل‌های امنیتی انتخاب شده را به طور کامل اجرا کنند. این کنترل‌ها می‌توانند شامل کنترل‌های فنی، مدیریتی و فیزیکی باشند که به کاهش ریسک‌های شناسایی شده کمک می‌کنند.
- **مستندسازی پیاده‌سازی:** سازمان‌ها باید نحوه اجرای کنترل‌های امنیتی را مستندسازی کنند. این مستندسازی شامل توضیح دقیق فرآیندهای پیاده‌سازی، مسئولیت‌ها و نتایج حاصل از اجرای کنترل‌هاست.
- **آموزش و آگاهی‌بخشی:** در این مرحله، سازمان‌ها باید کارکنان خود را در مورد کنترل‌های امنیتی و نحوه اجرای آن‌ها آموزش دهند. این

آموزش‌ها به کارکنان کمک می‌کند تا با فرآیندهای جدید آشنا شوند و به درستی از آن‌ها استفاده کنند.

- **ارزیابی اولیه:** پس از پیاده‌سازی کنترل‌ها، سازمان‌ها باید یک ارزیابی اولیه انجام دهند تا اطمینان حاصل کنند که کنترل‌ها به درستی اجرا شده‌اند و به اهداف مورد نظر دست یافته‌اند. این ارزیابی به سازمان‌ها کمک می‌کند تا نقاط ضعف را شناسایی و اصلاح کنند.
- **بهبود مستمر:** مرحله پیاده‌سازی باید به عنوان یک فرآیند پویا و مداوم در نظر گرفته شود. سازمان‌ها باید به طور مداوم کنترل‌های امنیتی را ارزیابی و بهبود دهند تا اطمینان حاصل کنند که این کنترل‌ها به درستی عمل می‌کنند و به تغییرات و تهدیدات جدید پاسخ می‌دهند.

مرحله ارزیابی

مرحله ارزیابی به سازمان‌ها امکان می‌دهد تا نقاط ضعف را شناسایی و اصلاح کنند. در ادامه مقاله rmf چیست به بررسی پیاده سازی مرحله ارزیابی می‌پردازیم.

- **آماده‌سازی برای ارزیابی:** سازمان‌ها باید تمامی مستندات و اطلاعات مربوط به کنترل‌های امنیتی را جمع‌آوری و آماده کنند. این شامل مستندات پیاده‌سازی، گزارش‌های نظارت و سایر اطلاعات مرتبط است.
- **انجام ارزیابی:** سازمان‌ها باید ارزیابی‌های دقیقی از کنترل‌های امنیتی انجام دهند تا اطمینان حاصل کنند که این کنترل‌ها به درستی اجرا شده‌اند و به اهداف مورد نظر دست یافته‌اند. این ارزیابی‌ها می‌توانند شامل تست‌های نفوذ، ارزیابی‌های امنیتی و بررسی‌های فنی باشند.
- **تحلیل نتایج ارزیابی:** سازمان‌ها باید نتایج را تحلیل کنند تا نقاط ضعف و مشکلات موجود را شناسایی کنند. این تحلیل به سازمان‌ها کمک می‌کند تا بفهمند که کدام کنترل‌ها به درستی عمل نمی‌کنند و نیاز به بهبود دارند.
- **مستندسازی نتایج:** سازمان‌ها باید نتایج ارزیابی را مستندسازی کنند. این مستندسازی شامل توضیح نقاط ضعف شناسایی شده، توصیه‌های بهبود و برنامه‌های اصلاحی است.
- **اجرای اقدامات اصلاحی:** سازمان‌ها باید اقدامات اصلاحی لازم را برای بهبود کنترل‌های امنیتی انجام دهند. این اقدامات می‌توانند شامل به‌روزرسانی کنترل‌ها، آموزش کارکنان و تغییر فرآیندها باشند.
- **ارزیابی مجدد:** سازمان‌ها باید ارزیابی‌های مجددی انجام دهند تا اطمینان حاصل کنند که مشکلات شناسایی شده به طور کامل برطرف شده‌اند و کنترل‌ها به درستی عمل می‌کنند.

مرحله مجوزدهی

این مرحله به سازمان‌ها امکان می‌دهد تا تصمیم‌گیری‌های نهایی در مورد مجوزدهی سیستم‌ها را انجام دهند.

- **آماده‌سازی بسته مجوزدهی:** سازمان‌ها باید تمامی مستندات و اطلاعات مربوط به ارزیابی‌های امنیتی و کنترل‌های پیاده‌سازی شده را جمع‌آوری و در قالب یک بسته مجوزدهی تهیه کنند. این بسته شامل گزارش‌های ارزیابی، مستندات پیاده‌سازی و نتایج ارزیابی‌ها است.
- **تحلیل ریسک و تعیین سطح پذیرش:** سازمان‌ها باید تحلیل دقیقی از ریسک‌های شناسایی شده انجام دهند و تعیین کنند که آیا این ریسک‌ها در سطح قابل قبولی قرار دارند یا خیر. این تحلیل به سازمان‌ها کمک می‌کند تا تصمیم‌گیری‌های نهایی در مورد مجوزدهی سیستم‌ها را انجام دهند.

- **تصمیم‌گیری مجوزدهی:** یک مقام ارشد سازمان باید تصمیم بگیرد که آیا سیستم مجاز به فعالیت است یا خیر. این تصمیم بر اساس ارزیابی ریسک و نتایج ارزیابی کنترل‌ها اتخاذ می‌شود. مقام ارشد باید اطمینان حاصل کند که تمامی ریسک‌ها به درستی مدیریت شده‌اند و سیستم آماده بهره‌برداری است.
- **صدور مجوز:** سازمان باید مجوز رسمی برای بهره‌برداری از سیستم صادر کند. این مجوز به سیستم اجازه می‌دهد تا به طور رسمی و قانونی فعالیت کند و از منابع سازمان استفاده کند.
- **مستندسازی تصمیمات:** سازمان‌ها باید تمامی تصمیمات و فرآیندهای مرتبط با مجوزدهی را مستندسازی کنند. این مستندسازی شامل توضیح دلایل تصمیم‌گیری، تحلیل ریسک و نتایج ارزیابی‌ها است.
- **نظارت مداوم:** سازمان‌ها باید به طور مداوم اجرای کنترل‌ها و ریسک‌های مرتبط با سیستم را نظارت کنند. این نظارت به سازمان‌ها کمک می‌کند تا به موقع به تغییرات و تهدیدات جدید پاسخ دهند و اطمینان حاصل کنند که سیستم همچنان در سطح قابل قبولی از ریسک قرار دارد.

مرحله نظارت

این مرحله به سازمان‌ها امکان می‌دهد تا به موقع به تغییرات و تهدیدات جدید پاسخ دهند و اطمینان حاصل کنند که کنترل‌ها به درستی عمل می‌کنند.

- **پایش مداوم کنترل‌ها:** سازمان‌ها باید به طور مداوم اجرای کنترل‌های امنیتی را پایش کنند. این پایش شامل بررسی عملکرد کنترل‌ها، شناسایی نقاط ضعف و ارزیابی تأثیرات آن‌ها بر ریسک‌های سازمان است.
- **ارزیابی دوره‌ای ریسک‌ها:** سازمان‌ها باید به طور دوره‌ای ریسک‌های مرتبط با سیستم‌های خود را ارزیابی کنند. این ارزیابی‌ها به سازمان‌ها کمک می‌کند تا تغییرات در محیط ریسک را شناسایی کنند و به موقع به آن‌ها پاسخ دهند.
- **به‌روزرسانی مستندات:** سازمان‌ها باید مستندات مرتبط با کنترل‌های امنیتی و ریسک‌ها را به‌روزرسانی کنند. این به‌روزرسانی شامل مستندسازی تغییرات در کنترل‌ها، نتایج ارزیابی‌ها و اقدامات اصلاحی است.

- **گزارش‌دهی:** سازمان‌ها باید گزارش‌های دوره‌ای از وضعیت کنترل‌های امنیتی و ریسک‌ها تهیه کنند. این گزارش‌ها به مدیران ارشد و سایر ذینفعان کمک می‌کند تا از وضعیت امنیتی سازمان آگاه شوند و تصمیمات لازم را اتخاذ کنند.
- **پاسخ به حوادث:** سازمان‌ها باید برنامه‌های پاسخ به حوادث را اجرا کنند. این برنامه‌ها شامل شناسایی، تحلیل و پاسخ به حوادث امنیتی است که ممکن است بر سیستم‌ها و اطلاعات سازمان تأثیر بگذارد.
- **بهبود مستمر:** مرحله نظارت باید به عنوان یک فرآیند پویا و مداوم در نظر گرفته شود. سازمان‌ها باید به طور مداوم کنترل‌های امنیتی و فرآیندهای مدیریت ریسک را ارزیابی کنند و بهبود دهند تا اطمینان حاصل کنند که این کنترل‌ها به درستی عمل می‌کنند و به تغییرات و تهدیدات جدید پاسخ می‌دهند.

مزایای استفاده از RMF چیست؟

در ادامه بررسی می‌کنیم که مزایای اصلی استفاده از RMF چیست؟

- **شناسایی و ارزیابی دقیق ریسک‌ها:** RMF به سازمان‌ها کمک می‌کند تا ریسک‌های مرتبط با فعالیت‌های خود را به طور دقیق شناسایی و ارزیابی کنند. این فرآیند شامل تحلیل تأثیرات احتمالی و تعیین اولویت‌های ریسک‌ها است.
- **بهبود تصمیم‌گیری:** سازمان‌ها می‌توانند تصمیمات استراتژیک بهتری بگیرند و از منابع خود به بهترین شکل استفاده کنند.
- **افزایش اعتماد ذینفعان:** سازمان‌هایی که از RMF استفاده می‌کنند، اعتماد بیشتری از سوی ذینفعان خود جلب می‌کنند. این اعتماد به دلیل شفافیت و دقت در مدیریت ریسک‌ها به وجود می‌آید.
- **کاهش هزینه‌ها:** با شناسایی و کنترل ریسک‌ها، سازمان‌ها می‌توانند از وقوع حوادث پرهزینه جلوگیری کنند.
- **بهبود عملکرد سازمانی:** با مدیریت مؤثر ریسک‌ها، سازمان‌ها می‌توانند فرآیندهای خود را بهینه کنند و به اهداف خود دست یابند.
- **تطابق با مقررات و استانداردها:** این تطابق به سازمان‌ها امکان می‌دهد تا از جریمه‌ها و مشکلات قانونی جلوگیری کنند.
- **حفاظت از دارایی‌ها:** استفاده از RMF به سازمان‌ها کمک می‌کند تا دارایی‌های خود را از تهدیدات مختلف محافظت کنند. این دارایی‌ها می‌تواند شامل اطلاعات حساس، تجهیزات و منابع مالی باشد.
- **بهبود فرآیندهای داخلی:** RMF به سازمان‌ها کمک می‌کند تا فرآیندهای داخلی خود را بهبود بخشند و کارایی بیشتری داشته باشند. این بهبود فرآیندها می‌تواند به افزایش بهره‌وری و کاهش خطاها منجر شود.

چالش‌های پیاده‌سازی RMF چیست؟

استفاده از این چهارچوب هم مانند تمامی روش‌های دیگر علی‌رغم مزایای قابل‌توجهی که دارد، چالش‌ها و سختی‌هایی نیز به همراه دارد. در این بخش بررسی می‌کنیم که مهم‌ترین این چالش‌ها در RFM چیست؟

- **نیاز به منابع مالی و انسانی:** سازمان‌ها باید بودجه کافی برای اجرای کنترل‌های امنیتی، ارزیابی‌ها و نظارت مداوم فراهم کنند. همچنین، نیاز به کارکنان متخصص و آموزش دیده برای مدیریت ریسک‌ها وجود دارد.
- **پیچیدگی فرآیندها:** فرآیندهای مرتبط با RMF ممکن است پیچیده و زمان‌بر باشند. این پیچیدگی می‌تواند شامل تحلیل‌های دقیق ریسک، انتخاب و پیاده‌سازی کنترل‌های امنیتی و ارزیابی‌های مداوم باشد.
- **نیاز به آموزش کارکنان:** یکی از چالش‌های اصلی پیاده‌سازی RMF، نیاز به آموزش کارکنان است. کارکنان باید با مفاهیم و فرآیندهای

مدیریت ریسک آشنا شوند و توانایی اجرای کنترل‌های امنیتی را داشته باشند. این آموزش‌ها می‌تواند زمان‌بر و هزینه‌بر باشد.

- **نیاز به هماهنگی بین بخش‌ها:** پیاده‌سازی RMF نیازمند هماهنگی بین بخش‌های مختلف سازمان است. این هماهنگی می‌تواند شامل همکاری بین بخش‌های فناوری اطلاعات، امنیت، مدیریت ریسک و مدیریت ارشد باشد.

نتیجه‌گیری

چارچوب مدیریت ریسک (RMF) ابزاری قدرتمند برای مدیریت ریسک‌های سازمانی است. مدیریت ریسک اجازه می‌دهد تا تعادلی بین پذیرش ریسک و کاهش آنها ایجاد شود. این چارچوب به سازمان‌ها کمک می‌کند تا ریسک‌های خود را شناسایی، ارزیابی و مدیریت کنند و از وقوع حوادث ناگوار جلوگیری کنند. با استفاده از RMF، سازمان‌ها می‌توانند فرآیندهای خود را بهبود بخشند و از منابع خود به بهترین شکل استفاده کنند.

استفاده از RMF به سازمان‌ها امکان می‌دهد تا تصمیم‌گیری‌های بهتری انجام دهند، اعتماد ذینفعان را جلب کنند و هزینه‌های ناشی از وقوع حوادث را کاهش دهند. همچنین، این چارچوب به سازمان‌ها کمک می‌کند تا با مقررات و استانداردهای مرتبط تطابق داشته باشند و دارایی‌های خود را از تهدیدات مختلف محافظت کنند.