راهنمای 10 مرحله‌ای
سیستم مدیریت امنیت
اطلاعاتISO 27001

راهنمای 10 مرحله‌ای سیستم مدیریت امنیت اطلاعات ISO 27001

مقدمه

گواهینامه ISO 27001

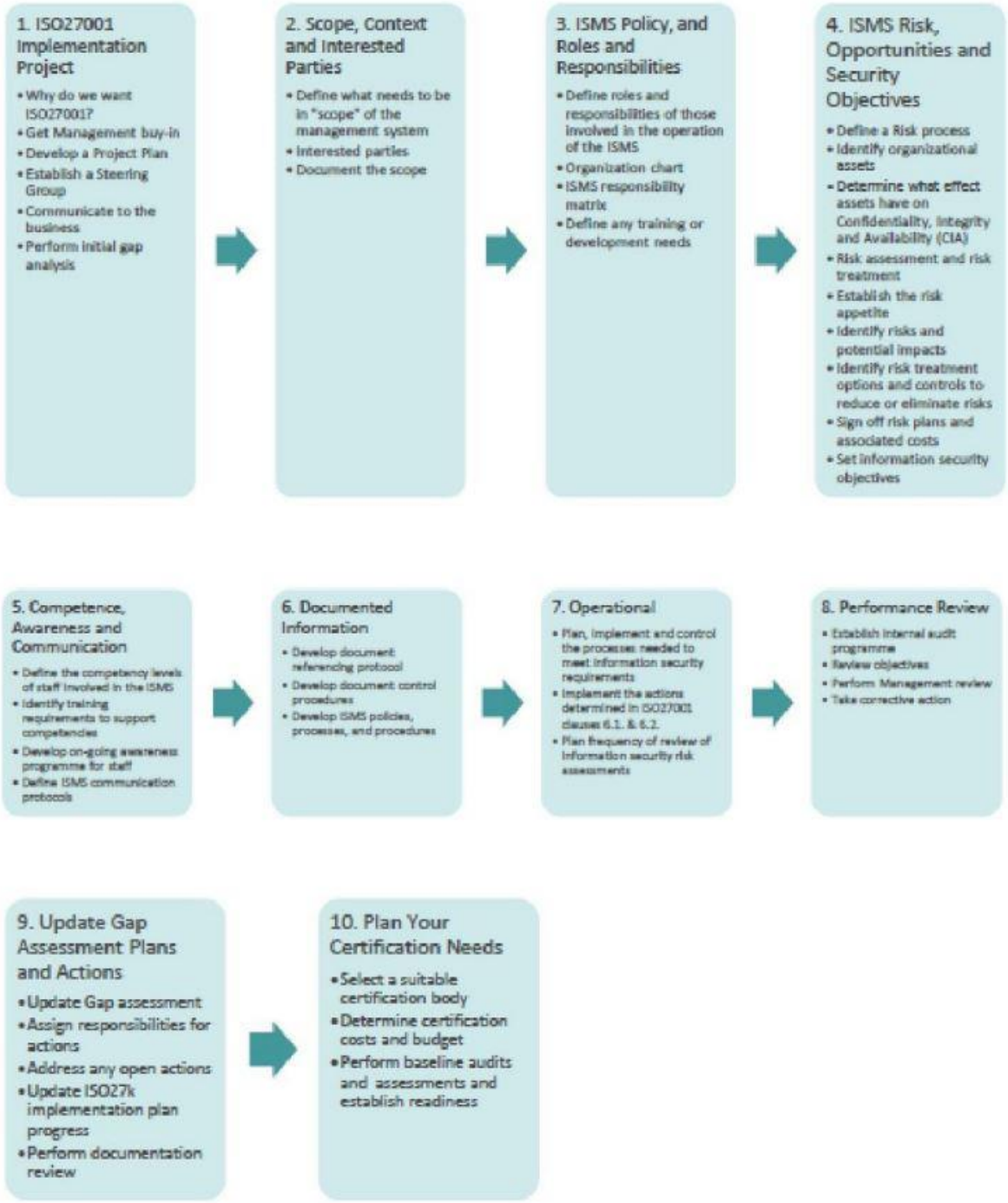
استاندارد **ISO 27001** در سراسر جهان به عنوان یکی از مهم‌ترین چارچوب‌های امنیت اطلاعات شناخته می‌شود. این استاندارد توسط سازمان‌های کوچک و بزرگ در صنایع مختلف پذیرفته شده است و دریافت گواهینامه ISO 27001 به طور فزاینده‌ای به عنوان یک نیاز ضروری در شرایط رقابتی مناقصه‌ها و همچنین به عنوان تضمینی برای ذینفعان که امنیت سایبری جدی گرفته می‌شود، شناخته می‌شود.

گاهی اوقات مشتریان این استاندارد را به عنوان یک الزام مطرح کرده‌اند. بنابراین، برای ادامه فعالیت تجاری، این گواهینامه ضروری است.

این راهنما شما را در مسیر دریافت گواهینامه ISO 27001 همراهی کرده و مراحل اصلی این فرآیند را مشخص می‌کند. توجه داشته باشید که این راهنما قابل استفاده برای دریافت گواهینامه نسخه‌های 17/2013 یا 2022 این استاندارد است.

صدور گواهینامه

شکل 1 سفر صدور گواهینامه به مرحله 1



مرحله اول

اجرای پروژه

چرا گواهینامه ISO 27001 بگیریم؟

دریافت گواهینامه برای هر استاندارد سیستم مدیریت، نیازمند تلاش و منابع است. این شامل راه‌اندازی، استقرار سیاست‌ها و فعالیت‌های مرتبط، و همچنین حفظ و نگهداری سیستم در طولانی‌مدت می‌شود. اولین پرسش اساسی این است :

چرا می‌خواهیم به طور رسمی استاندارد ISO 27001 را بگیریم؟

نیازهای داخلی

ممکن است نیازهای داخلی شما را به دریافت گواهینامه سوق دهند :

-افزایش کارایی یا بهبود روش‌های کاری

-کاهش ریسک‌های تجاری

-کاهش نقایص یا حوادثی که شهرت کسب‌وکار را تحت تأثیر قرار می‌دهند

-ایجاد شناسایی داخلی برای بهبود فرآیندها

نیازهای خارجی

یا شاید دلایل خارجی نیاز به گواهینامه را ایجاد کنند :

-**الزامات مشتری**: قراردادها اغلب یکی از دلایل اصلی نیاز به گواهینامه استاندارد ISO هستند. با این حال، اگر استاندارد را به درستی اجرا کنید، کسب‌وکار شما از مزایای زیادی مانند افزایش اعتماد مشتری و بهبود عملیات بهره‌مند می‌شود.

- **جرایم سایبری**: ممکن است شرکت شما هدف حملات سایبری قرار گرفته باشد. با افزایش پیچیدگی حملات سایبری و تهدیدات علیه اطلاعات محرمانه، حفاظت از داده‌های مشتریان و کارکنان ضروری‌تر از همیشه است.

اگرچه می‌توان فرآیندها و عملیات کسب‌وکار را بدون دریافت گواهینامه رسمی با استاندارد تطبیق داد، اما این کار شما را از دریافت تأییدیه رسمی و توانایی اثبات تطابق به مشتریان، به خصوص در مناقصات، محروم می‌کند .

تعهد مدیریت را به دست آورید

یکی از مهم‌ترین گام‌ها این است که تعهد مدیریت ارشد را به پروژه جلب کنید. اگر تصمیم‌گیرندگان اصلی شرکت از اهمیت سیستم مدیریت امنیت اطلاعات (ISMS) آگاه نباشند، این پروژه در نهایت شکست خواهد خورد .

یک برنامه پروژه تدوین کنید

همان‌طور که هیچ سازمان بالغی بدون برنامه‌ریزی وارد توسعه محصولات یا خدمات خود نمی‌شود، اجرای ISMS نیز نیازمند برنامه‌ای مشخص است تا همه افراد بدانند مسئولیتشان چیست و وظایفشان چه زمانی باید انجام شود .

تشکیل گروه راهبری

اندازه و محدوده گروه راهبری به اندازه سازمان و نقش‌های مرتبط با ISMS بستگی دارد. این گروه مسئول تصمیم‌گیری در زمینه‌های زیر خواهد بود :

-تدوین سیاست‌ها، فرآیندها و اهداف ISMS

-بودجه‌بندی

-ارزیابی ریسک و تصمیم‌گیری درباره نحوه کاهش آن

-تخصیص وظایف

گروه راهبری باید یک اسپانسر اجرایی داشته باشد که مسئول اجرای ISMS و اعطای اختیارات در سازمان باشد .

ارتباطات کلید موفقیت است

در شروع مسیر دریافت گواهینامه، باید کارکنان را درباره موارد زیر آگاه کنید :

-دلایل و اهداف دریافت گواهینامه ISO 27001

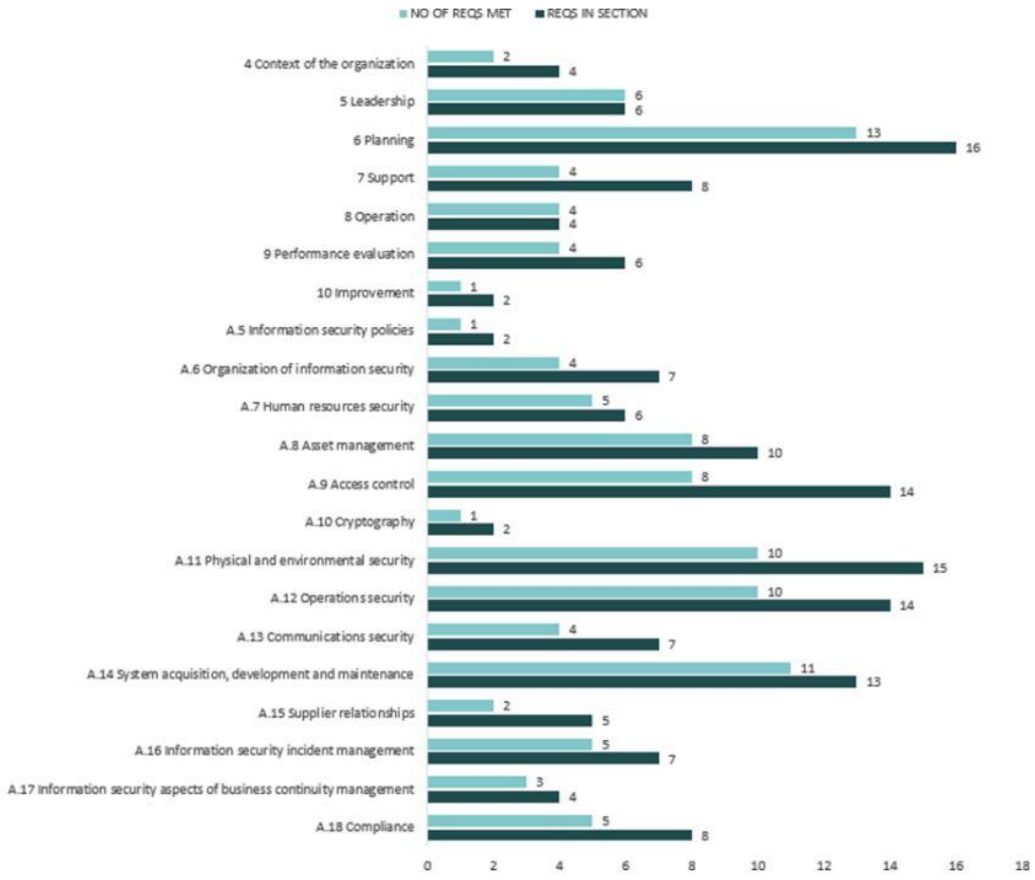
-حمایت و تعهد مدیریت ارشد از این طرح

انجام ارزیابی شکاف اولیه

با انجام ارزیابی شکاف، شما درک بهتری از میزان کار مورد نیاز برای رسیدن به نقطه‌ای که ممیزی گواهینامه ممکن باشد، پیدا خواهید کرد .

کلید انجام یک ارزیابی شکاف دقیق این است که افراد مناسب را درگیر کنید تا درک کاملی از آنچه که در حال حاضر وجود دارد، به دست آورید. ابزارهایی مانند ISO27001 Gap Assessment در کیت ابزار CertiKit می‌توانند ارقام دقیقی از میزان تطابق شما با استاندارد، در هر بخش از آن، ارائه دهند و حتی موقعیت شما را در نمودارهای میله‌ای برای به اشتراک گذاشتن با مدیریت ارشد نشان دهند.

همچنین ایده خوبی است که این ارزیابی را به‌طور منظم در طول پروژه تکرار کنید تا پیشرفت خود را از نقطه شروع اصلی ارزیابی کنید و بررسی کنید که چه پیشرفت‌هایی در راستای تکمیل گواهینامه حاصل شده است.



نمودار شکل 2 که سطح انطباق با استاندارد را در گپ جعبه ابزار ISO27001 نشان می دهد.

ابزار ارزیابی نسخه (ISO27001:2013)

مرحله دوم

محدوده، زمینه و طرف‌های ذی‌نفع

تعیین محدوده ISMS

لزومی ندارد که همه چیز در محدوده سیستم مدیریت شما قرار بگیرد. یکی از گام‌های اولیه این است که محدوده مشخصی برای ISMS خود تعریف کنید و بتوانید توضیح دهید چه چیزهایی در این محدوده نیستند.

این مرحله بسیار مهم است، زیرا تمامی مراحل بعدی بر اساس این محدوده انجام می‌شوند، بنابراین بهتر است وقت کافی برای تعیین دقیق آن صرف کنید. همچنین، باید آنچه که استاندارد "زمینه" سیستم مدیریت می‌نامد را تعریف کنید؛ این شامل محیط داخلی و خارجی سازمان شما می‌شود.

طرف‌های ذی‌نفع

استاندارد ISO 27001 شما را ملزم می‌کند تمامی طرف‌های ذی‌نفعی که برای سیستم مدیریت شما "مرتبط" هستند را تعریف کنید. اما این طرف‌های ذی‌نفع چه کسانی هستند؟

نمونه‌هایی از طرف‌های ذی‌نفع کلیدی:

1. **مشتریان**:

مشتریان ممکن است به طور قراردادی از شما بخواهند که محصولات و خدماتی مطابق با الزامات خاص ارائه دهید.

2. **سازمان‌های قانونی و نظارتی**:

قوانین و مقررات محلی، منطقه‌ای یا ملی که به عنوان یک کسب‌وکار ملزم به رعایت آن‌ها هستید. این قوانین اغلب تأثیر مستقیمی بر سیستم مدیریت شما دارند و شما باید رویه‌ها و کنترل‌هایی برای برآورده کردن این الزامات پیاده‌سازی کنید.

3. **تأمین‌کنندگان**:

استاندارد ISO 27001 الزامات متعددی در مورد روابط تأمین‌کنندگان دارد. به ویژه، مدیریت ریسک‌های مربوط به دسترسی تأمین‌کنندگان به دارایی‌های سازمان شما، از جمله سیستم‌ها یا حتی دسترسی فیزیکی به مکان‌ها.

تحلیل منافع و نیازهای ذی‌نفعان

زمان کافی برای شناخت منافع داخلی و خارجی ذی‌نفعانی که ممکن است بر توانایی سیستم مدیریت شما برای دستیابی به نتایج موردنظر تأثیر بگذارند، اختصاص دهید.

این به معنای آن است که باید تأثیر ذی‌نفعان را درک کنید و تصمیم بگیرید که چگونه این منافع را از طریق سیاست‌ها، رویه‌ها، کنترل‌ها یا سایر ابزارهای ISMS مدیریت کنید.

همچنین، الزامات طرف‌های ذی‌نفع می‌توانند ریسک‌هایی را معرفی کنند که باید آن‌ها را شناسایی و کاهش دهید.

نهایتاً، سازمان گواهی‌دهنده ثبت‌شده (RCB) که ارزیابی گواهینامه شما را انجام خواهد داد، باید محدوده سیستم مدیریت شما را بداند.

داشتن محدوده‌ای مستند به شما کمک می‌کند که برای RCB شفاف کنید که ISMS شما از کجا شروع شده و تا کجا ادامه دارد.

مرحله سوم

سیاست‌ها، نقش‌ها و مسئولیت‌ها

نقش‌ها و مسئولیت‌ها

برای عملکرد مؤثر سیستم مدیریت امنیت اطلاعات (ISMS)، چندین نقش کلیدی مورد نیاز است. این نقش‌ها ممکن است بر اساس اندازه و محدوده ISMS تغییر کنند. برخی از این نقش‌ها ممکن است با هم ترکیب شوند و مسئولیت‌ها بین آن‌ها تقسیم شود.

نقش‌های کلیدی شامل:

1. **گروه راهبری امنیت اطلاعات**

(توضیحات این نقش در مرحله اول ذکر شده است).

2. **مدیر امنیت اطلاعات (CISO)**:

این نقش، نقش اصلی در مدیریت امنیت اطلاعات و مسائل مرتبط است و به طور کامل بر امنیت اطلاعات متمرکز است.

3. **مالک دارایی‌های اطلاعاتی**:

مسئولیت اصلی عملیاتی یک یا چند دارایی اطلاعاتی را که در فهرست دارایی‌های اطلاعاتی سازمان تعریف شده‌اند، بر عهده دارد.

4. **مالک ریسک‌های امنیت اطلاعات**:

مسئولیت مدیریت یک یا چند ریسک امنیت اطلاعات را که در طرح درمان ریسک سازمان تعریف شده‌اند، بر عهده دارد.

5. **ممیز امنیت اطلاعات**:

وظایف ممیزی داخلی استاندارد ISO/IEC 27001 را انجام می‌دهد و مسئول بررسی اثربخشی اجرای ISMS و نگهداری آن است.

6. **سایر نقش‌های مرتبط با امنیت اطلاعات**:

- مدیران بخش‌ها
- تکنسین‌های فناوری اطلاعات
- کاربران فناوری اطلاعات

نمودار سازمانی

ایجاد نمودار سازمانی که خطوط گزارش‌دهی و روابط بین تمامی افرادی که در عملکرد ISMS مشارکت دارند را نشان دهد، ضروری است. این نمودار به شفاف‌سازی مسئولیت‌ها کمک می‌کند.

ماتریس مسئولیت‌های ISMS

یکی از رویکردهای مفید برای نشان دادن مسئولیت‌ها در مدیریت بخش‌های مختلف استاندارد ISO 27001، استفاده از جدول RACI است.

جدول RACI شامل:

- مسئول (Responsible): افرادی که مسئول انجام وظایف هستند.

- پاسخگو (Accountable): افرادی که پاسخگوی نتایج هستند و تصمیم نهایی را می‌گیرند.

- مشاور (Consulted): افرادی که برای مشاوره و راهنمایی دخیل هستند.

- اطلاع‌یافته (Informed): افرادی که باید از پیشرفت کار مطلع شوند.

مرحله چهارم

ریسک، فرصت‌ها و امنیت

تعریف فرآیند مدیریت ریسک

قبل از شروع ارزیابی ریسک‌ها، باید فرآیندی مشخص برای مدیریت ریسک‌ها در سازمان تعریف کنید. روش‌ها و رویکردهای مختلفی برای انجام ارزیابی ریسک وجود دارد. انتخاب روشی که مناسب نیازهای سازمان باشد و پیچیدگی بیش از حد نداشته باشد، بسیار مهم است.

نکات قابل توجه:

- انتخاب روش ارزیابی ریسک:

- **ارزیابی کیفی**: بر اساس قضاوت ذهنی، با تعیین احتمال و تأثیر رویدادها در مقیاس عددی (مانند 1-5).

- **ارزیابی کمی**: استفاده از داده‌های قابل تأیید برای تحلیل اثرات ریسک‌ها (مثلاً ریسک A با احتمال 40٪).

- **ارزیابی عمومی**: شناسایی خطرات مشترک و اقدامات کنترلی، که در امنیت اطلاعات نیز قابل استفاده است.

- **الگوها و اسناد مورد نیاز**: برای پشتیبانی از رویکرد انتخابی.

- **مهارت‌ها و توانمندی‌ها**: افراد باید توانایی ارزیابی ریسک‌ها را داشته باشند.

دارایی‌های سازمانی

یکی از بخش‌های مهم استاندارد ISO27001، شناسایی و محافظت از دارایی‌های سازمانی است:

- چه دارایی‌هایی دارید؟

- محافظت در برابر از دست دادن تصادفی، سرقت یا حملات مخرب.

- اطمینان از بازگشت دارایی‌ها هنگام خروج کارکنان.

- **تأثیر بر امنیت اطلاعات**:

- شناسایی دارایی‌هایی که بیشترین تأثیر را بر محرمانگی (Confidentiality)، یکپارچگی (Integrity) یا دسترسی‌پذیری (Availability) دارند.

اشتیاق به پذیرش ریسک (Risk Appetite)

تصمیم‌گیری درباره سطح پذیرش ریسک، تعیین‌کننده رویکرد شما در مدیریت ریسک‌ها خواهد بود:

- **محافظه‌کار**: درمان اکثر ریسک‌ها.
- **کمتر محتاط**: پذیرش یا تأخیر در درمان برخی ریسک‌ها.

ارزیابی و درمان ریسک‌ها

1. **ارزیابی**: شناسایی ریسک‌ها و اقدامات محافظتی (کنترل‌ها).
2. **انتخاب کنترل‌ها**: استفاده از مجموعه کنترل‌های مرجع استاندارد ISO27001 در **ضمیمه A**.
3. **بیانیه کاربردپذیری (Statement of Applicability)**: مشخص کردن کنترل‌های قابل اجرا در سازمان.

برنامه درمان ریسک‌ها

- مستندسازی ریسک‌های پرخطر در یک طرح درمان ریسک (Risk Treatment Plan):
- ارائه این برنامه برای تأیید و دریافت بودجه از تیم رهبری.

اهداف امنیت اطلاعات

اهداف امنیت اطلاعات، جهت‌گیری پیاده‌سازی استاندارد ISO27001 را مشخص می‌کنند:

- اهداف سطح بالا: مرتبط با تعیین محدوده و زمینه ISMS.
- اهداف عملیاتی:
- اهداف کوتاه‌مدت یا سالانه.
- نیازهای وابسته به ذینفعان.
- پاسخ به حوادث امنیتی یا بهبودهایی که باید در زمان مشخصی انجام شوند.

مرحله پنجم

شایستگی و آگاهی

سطوح شایستگی کارکنان

برای موفقیت سیستم مدیریت امنیت اطلاعات (ISMS)، لازم است که نقش‌ها و مسئولیت‌ها به‌وضوح مستند شده و برای هر نقش، شایستگی‌ها و الزامات تعریف شود. این اطمینان حاصل می‌کند که کارکنان دانش و مهارت‌های لازم را برای اجرای وظایف مربوط به ISMS دارند.

آموزش و توسعه

استاندارد ISO27001 تأکید دارد که منابع کافی برای عملکرد مؤثر ISMS تأمین شود. این به معنای ارزیابی منابع داخلی سازمان و شناسایی کمبودهاست.

نیازهای آموزشی:

- آموزش تخصصی: برای افرادی که مسئول درک الزامات و تفسیر استاندارد هستند.

- آگاهی عمومی: برای سایر کارکنان درباره سیاست‌ها و رویه‌هایی که باید رعایت کنند.

آگاهی مستمر

- به‌روزرسانی‌های منظم: کارکنان را در جریان برنامه توسعه ISMS و نتایج آن قرار دهید.

- آموزش‌های آگاهی‌بخشی: شامل موضوعات کلیدی امنیت اطلاعات مانند سیاست‌ها، ریسک‌ها، کنترل‌های امنیتی، و آموزش‌های مقدماتی (Induction Training).

پروتکل‌های ارتباطی

یک طرح ارتباطی طراحی کنید که روش‌های ارتباط، مسئولیت هر بخش، و نحوه انتقال اطلاعات را مشخص کند.

اجزای کلیدی طرح ارتباطی:

1. **روش‌های ارتباطی**: ایمیل، جلسات، اطلاعیه‌ها، پورتال‌های داخلی.
2. **مسئولیت‌ها**: مشخص کردن اینکه چه کسی مسئول برقراری ارتباط در هر زمینه است.
3. **محتوا**: شامل سیاست‌ها، تغییرات مهم در ISMS، و نکات ضروری امنیت اطلاعات.

مرحله ششم

اطلاعات مستند

ارجاع‌دهی به اسناد

تمام اسناد مرتبط با سیستم مدیریت امنیت اطلاعات (ISMS)، مانند سیاست‌ها، فرآیندها، رویه‌ها، الگوها و فرم‌ها باید به‌طور منحصر به فرد شماره‌گذاری شوند تا بتوان آن‌ها را شناسایی کرد.

کنترل اسناد

کنترل صحیح اسناد ISMS شامل سیاست‌ها، رویه‌ها و مستندات دیگر، یکی از الزامات کلیدی هر سیستم مدیریت است. این به این معناست که شما باید یک مجموعه مشخص و مستند از رویه‌های کنترل اسناد داشته باشید که چرخه زندگی اطلاعات مستند را پوشش دهد.

مراحل کنترل اسناد

1. **شناسایی**: تعیین چگونگی شناسایی اسناد و مستندات.
2. **ذخیره‌سازی**: روش‌های مناسب برای ذخیره‌سازی و محافظت از اسناد.
3. **بازیابی**: تعریف فرآیندهایی برای دسترسی به اسناد هنگام نیاز.
4. **نگهداری و انهدام**: تعیین مدت زمان نگهداری اسناد و روش‌های انهدام ایمن آن‌ها پس از اتمام دوره‌های قانونی یا عملیاتی.

سیاست‌ها و رویه‌ها

در این مرحله، شما باید تمام اسناد سیاستی و دیگر اسناد پشتیبانی‌کننده را که نهایتاً جزئی از ISMS شما خواهند بود، توسعه دهید. این اسناد به شفاف‌سازی فرآیندهای امنیت اطلاعات و اقدامات پیشگیرانه کمک می‌کنند.

چند نکته مهم برای سازماندهی اسناد ISMS:

- **ساختار پوشه شبکه‌ای ساده**: برای سازمان‌های کوچک یا متوسط ممکن است استفاده از پوشه‌های شبکه‌ای ساده مناسب باشد.

- **ابزارهای مدیریت اسناد**: برای سازمان‌های بزرگتر، ابزارهایی مانند SharePoint یا ابزارهای اختصاصی ISMS برای مدیریت اسناد و پیگیری مستندات می‌توانند بسیار مفید باشند.

مرحله هفتم

برنامه‌ریزی عملیاتی

شناسایی کنترل‌های پیوست A

در این مرحله، باید کنترل‌های موجود در پیوست A استاندارد ISO 27001 را که تصمیم به اعمال آن‌ها برای خطرات خاص گرفته‌اید، شناسایی کنید. همچنین، باید سیاست‌ها، فرآیندها یا رویه‌های جدید ISMS را که برای مدیریت این خطرات نیاز دارید، مشخص کنید.

اجرای اقدامات

استاندارد از شما می‌خواهد که به شیوه‌هایی که مسائل داخلی و خارجی می‌توانند بر توانایی سیستم مدیریت امنیت اطلاعات شما در دستیابی به نتایج مطلوب تأثیر بگذارند، فکر کنید. بخش عمده‌ای از این مسائل ممکن است در فرآیند ارزیابی ریسک گنجانده شوند، اما ممکن است عوامل دیگری نیز وجود داشته باشند که نیاز به بررسی و ارزیابی داشته باشند.

عوامل مؤثر:

1. **مسائل داخلی و خارجی**: عواملی مانند تغییرات قانونی، تهدیدات امنیتی جدید یا نوسانات اقتصادی می‌توانند تأثیرگذار باشند.
2. **نیازها و انتظارات طرف‌های ذینفع**: نظرات و انتظارات مشتریان، تأمین‌کنندگان و سایر ذینفعان باید در نظر گرفته شود.

بازبینی ارزیابی ریسک

سازمان باید در سیاست و رویه‌های ریسک خود، دفعات بازبینی ارزیابی ریسک‌ها و طرح‌های درمانی را مشخص کند. همچنین باید وضعیت اقدامات و کنترل‌های کاهش ریسک را به‌طور مداوم پیگیری کرده و بر آن‌ها نظارت داشته باشد.

نکات کلیدی برای بازبینی ارزیابی ریسک:

1. **بازبینی منظم**: ارزیابی ریسک‌ها باید به‌طور دوره‌ای بازبینی شود تا اطمینان حاصل شود که آن‌ها به‌روز و مرتبط با وضعیت فعلی هستند.
2. **پیگیری اقدامات**: وضعیت اجرای کنترل‌های کاهش ریسک باید به‌طور مداوم نظارت شود تا از اثربخشی آن‌ها اطمینان حاصل گردد.

اجرای درست این فرآیندها به شما کمک می‌کند تا ISMS به‌طور مؤثر عمل کرده و به اهداف امنیتی خود برسید.

مرحله هشتم

بررسی عملکرد

ممیزی داخلی

حفظ تطابق فرآیندها و بهبود مستمر از اهمیت بالایی برخوردار است. شما زمان، تلاش و منابع مالی زیادی را برای دستیابی به گواهی ISO صرف کرده‌اید، و یکی از چالش‌های اصلی حفظ آن است. ممیزی‌های داخلی روشی برای اطمینان از این است که فرآیندهای تعریف‌شده طبق دستورالعمل پیاده‌سازی می‌شوند و همچنین تغییرات ناشی از پذیرش تکنولوژی‌های جدید، تغییرات در عملیات تجاری یا تغییرات در کادر کلیدی کارکنان را منعطفانه منعکس می‌کنند.

برنامه ممیزی:

1. باید یک برنامه ممیزی در مراحل اجرایی طراحی شود که تمام بخش‌های استاندارد و سیاست‌ها، فرآیندها و رویه‌هایی را که در دامنه پروژه قرار دارند، پوشش دهد.

2. ممیزی‌های داخلی باید توسط ممیزان مناسب درون سازمان یا از طریق خدمات ممیزی داخلی برون‌سپاری شده از سوی یک شخص ثالث انجام شود.

ممیزی پیش‌گواهینامه:

اجرای یک ممیزی داخلی پیش‌گواهینامه می‌تواند روشی خوب برای ارزیابی آمادگی شما برای دریافت گواهینامه رسمی باشد و همچنین کمک می‌کند تا شکاف‌های انطباق باقی‌مانده شناسایی شوند.

بازبینی اهداف

در این مرحله از برنامه پیاده‌سازی، مهم است که اهداف ISO27001 را دوباره ارزیابی و در صورت نیاز اصلاح کنید. پیشرفت در برابر اهداف باید به‌روزرسانی و پیگیری شود.

بازبینی مدیریت

اگر هنوز جلسه بازبینی مدیریت را برگزار نکرده‌اید، مهم است که حداقل یک جلسه بازبینی مدیریت برگزار کنید، و بهتر است جلسات بازبینی بیشتری قبل از ارزیابی گواهی‌نامه برگزار کنید.

نکات برای جلسه بازبینی مدیریت:

1. جلسه بازبینی باید حداقل شامل الزامات بند 9.3 استاندارد باشد، به ویژه زیرنقاط a9.3، b، c، d، e و f.

2. مشارکت ذینفعان کلیدی در جلسه ضروری است و باید مدیریت ارشد در دستور جلسه شرکت کند.

3. باید صورت‌جلسه و اقدامات کلیدی از جلسه ثبت و مستند شود.

اقدامات اصلاحی

عدم انطباق‌ها و اقدامات اصلاحی مرتبط ممکن است از چندین منبع به‌وجود آید:

- ممیزی‌های داخلی

- حوادث امنیتی

- مشتریان خارجی یا طرف‌های ذینفع

- کارکنان داخلی از پیشنهادات بهبود

- بازبینی مدیریت و سایر بررسی‌های داخلی

اجرای ممیزی‌ها، پیگیری اهداف، بازبینی مدیریت و اتخاذ اقدامات اصلاحی کمک می‌کند تا ISMS به‌طور مؤثر و مطابق با استانداردهای ISO27001 عمل کند و همیشه به‌روزرسانی و بهبود یابد.

مرحله نهم

ارزیابی شکاف‌ها و اقدامات

بروزرسانی تجزیه و تحلیل شکاف

اطمینان حاصل کنید که تجزیه و تحلیل شکاف انجام‌شده پیش از این، تا حد امکان 100% یا بالاترین میزان تکمیل را برای حوزه‌های ارزیابی مطابق با استاندارد نشان دهد.

تخصیص مسئولیت‌ها

تمامی اقدامات ارزیابی شکاف باید به افرادی که صلاحیت و شایستگی لازم برای رسیدگی به آن‌ها و بسته شدن موارد را دارند، اختصاص داده شود.

رسیدگی به اقدامات باز

تأکید کنید که اقدامات ناشی از ارزیابی شکاف‌ها به‌طور کامل مورد توجه قرار گرفته و بسته شده‌اند. اطمینان حاصل کنید که تمامی اقدامات منجر به ایجاد سیاست‌ها/رویهٔ جدید ISMS، تکمیل شده و به‌طور کامل در مخزن ISMS گنجانده شده‌اند.

بروزرسانی پیشرفت برنامه

مدیریت پیاده‌سازی ISO27001 باید تکمیل وظایف را در مقابل برنامه پیاده‌سازی و وضعیت اقدامات تجزیه و تحلیل شکاف‌ها بررسی کند.

هرگونه مشکل یا موانع پیشرفت باید به گروه راهبری گزارش شود و در صورت لزوم، با حامی اجرایی مطرح گردد.

روش‌های الزامی

در استاندارد ISO27001 و کنترل‌های مربوطه، چندین روش الزامی وجود دارد که باید تهیه شوند، مانند بیانیه کاربردپذیری و فهرست دارایی‌ها. همه این موارد باید صادر شوند و تا حد امکان در حالت پیش‌نویس نباشند پیش از ممیزی مرحله 1.

ریسک‌ها و اقدامات

بررسی کنید که طرح درمان ریسک به‌روز است و اقدامات به‌طور مستمر پیگیری و پیشرفت می‌کنند.

مسائل و تصویب

اطمینان حاصل کنید که ISMS شامل اسناد کاملاً منتشر و تأییدشده است، هرچند ممکن است در هر مقطعی اسناد در حالت پیش‌نویس باشند، اما اگر بیشتر ISMS در حالت پیش‌نویس یا با اسناد و سیاست‌های منتشرنشده باشد، این امر به‌ویژه در ممیزی گواهینامه ممکن است مشکل‌ساز باشد.

فهرست دارایی‌ها به‌روز شده

بررسی کنید که فهرست دارایی‌ها به‌طور کامل تکمیل شده و هر دارایی جدیدی که به‌تازگی خریداری شده یا دارایی‌های اطلاعاتی دیگر که شناسایی شده‌اند، به‌طور لازم اضافه شده باشند.

مرحله دهم

برنامه‌ریزی نیازهای گواهینامه شما

انتخاب یک بدنه گواهینامه (RCB)

در این مرحله، ممکن است بخواهید با یک بدنه گواهینامه ثبت‌شده (RCB) که قادر به انجام ممیزی گواهینامه در مراحل بعدی است تماس بگیرید. توصیه می‌شود که یک RCB معتبر را نسبتاً زود انتخاب کرده و با آن آشنا شوید، از جمله زمان‌های در دسترس بودن آن‌ها و هزینه‌های مربوطه. این کار از بروز مشکلات غیرمنتظره در مراحل بعدی جلوگیری می‌کند.

هزینه‌ها و بودجه

هزینه‌های اولیه گواهینامه به عوامل مختلفی مانند تعداد سایت‌ها و کارکنان و صنعت شما بستگی دارد. همچنین هزینه‌های حفظ گواهینامه باید در برنامه‌ریزی مالی گنجانده شود.

در این مرحله، شما باید آماده باشید تا RCB مورد نظر خود را انتخاب کنید و تاریخ‌های ارزیابی را آغاز کنید.

ممیزی‌ها و ارزیابی‌ها

یکی از جنبه‌های کلیدی ISO27001، نیاز به انجام ممیزی‌های داخلی برای ISMS است. پیش از هرگونه ارزیابی گواهینامه توسط RCB، باید تمامی جنبه‌های ISMS خود را طبق استاندارد ISO27001 ممیزی کرده باشید یا حداقل در حال تکمیل این ممیزی‌ها باشید.

آماده‌سازی برای ممیزی

پس از انجام مراحل آماده‌سازی، شما آماده‌اید تا ممیزی از سوی بدنه گواهینامه انجام شود. این فرایند در دو مرحله صورت می‌گیرد که به‌طور راحتی به آن‌ها مرحله اول (Stage One) و مرحله دوم (Stage Two) گفته می‌شود. مرحله اول شامل بازبینی اسناد است تا ارزیابی شود که چقدر آماده هستید و محدوده شما چقدر به‌خوبی تعریف شده است. اگر بازبینی مرحله اول هیچ مشکلی عمده‌ای نداشته باشد، سپس می‌توانید تاریخ ممیزی مرحله دوم را تنظیم کنید. اگر این ممیزی با موفقیت انجام شود، گواهینامه شما صادر شده و تمام تلاش‌های شما به نتیجه می‌رسد.