

سیستم مدیریت امنیت اطلاعات (ISMS) راهکاری برای مبارزه با تهدیدات	۱- عنوان محتوا:
سیستم مدیریت امنیت اطلاعات (ISMS)	۲- کلمه کلیدی اصلی
سیستم مدیریت امنیت اطلاعات	۳- کلمه کلیدی مرتبط
یک سیستم مدیریت امنیت اطلاعات (ISMS) باعث جلوگیری و کاهش صدمات ناشی از لو رفتن اطلاعات یک سازمان به کمک امن سازی اطلاعات می شود. همچنین عواملی نظیر نیازها و اهداف سازمان، الزامات امنیتی، اندازه و ساختار سازمان بر طراحی و پیاده سازی سیستم مدیریت امنیت اطلاعات در سازمان تأثیر خواهد گذاشت.	۴- خلاصه محتوا ( ۵۰ تا ۷۰ کلمه)



### سیستم مدیریت امنیت اطلاعات (ISMS) و ضرورت آن در عصر جدید

امروزه مسئله امنیت، یکی از بزرگترین مشکلات و چالش‌های عصر فناوری اطلاعات محسوب می‌شود. در عصر کنونی هیچ سازمانی نیست که خود را بی نیاز از فناوری اطلاعات بداند. حفاظت از اطلاعات و خصوصاً اطلاعات یک سازمان در مقابل حملات مختلف نظیر خرابکاری، فیشینگ و دسترسی غیر مجاز امری به شدت ضروری و

اجتناب ناپذیر به شمار می‌رود. به همین دلیل استفاده از سیستم مدیریت امنیت اطلاعات (ISMS) بسیار مهم و ضروری می‌باشد. چرا که مسئله اطلاعات در سازمان‌ها و شرکت‌های بزرگ جز خط قرمز آنها، ابزار مهم تصمیم‌گیری‌های سازمان و دارای مهم و باارزش محسوب می‌گردند.

با توجه به رشد حملات سایبری در کشور و نامناسب بودن وضعیت امنیتی و تبادل اطلاعات در ایران، نیاز به مدیریت اطلاعات و ایمن‌سازی اطلاعات در سازمان‌ها به شدت احساس می‌شد.

لذا طبق بخشنامه شماره ۱۳۷۱۱-۸۶/م/۳۸۵۰۵ مورخ ۱۰/۰۸/۱۳۸۶ معاون اول محترم رئیس جمهور، ایجاد طرح سیستم مدیریت امنیت اطلاعات (ISMS) جزو وظایف و الزامات دستگاه‌های دولتی و غیر دولتی می‌باشد.

یکی از خدمات مهم شرکت فنی و مهندسی امن پردازان کویر، پیاده‌سازی و مدیریت سیستم مدیریت امنیت اطلاعات (ISMS) می‌باشد.

این سیستم یک راهکار و ابزاری است برای مدیریت و به حداقل رساندن تهدیدات خارجی سازمان که به مدیران این امکان را می‌دهد بتوانند امنیت سیستم‌های یک سازمان را مدیریت کنند. چرا که اطلاعات یک سازمان بخش حیاتی یک سازمان هستند و نیازمند مدیریت اثربخش و قوی جهت جلوگیری از سواستفاده‌ها می‌باشند.

لذا، یک سیستم مدیریت امنیت اطلاعات (ISMS) باعث جلوگیری و کاهش صدمات ناشی از لو رفتن اطلاعات یک سازمان به کمک امن‌سازی اطلاعات می‌شود. همچنین عواملی نظیر نیازها و اهداف سازمان، الزامات امنیتی، اندازه و ساختار سازمان بر طراحی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان تأثیر خواهد گذاشت.

هدف از تهیه این استاندارد بین‌المللی، ارائه مدلی است که بر اساس آن بتوان سیستمی ایجاد کرد که از اطلاعات یک سازمان محافظت کرده و آن را بهبود بخشیده و ارتقا دهد. یک سازمان برای اینکه اثر بخش باشد، باید فعالیت‌ها و اطلاعات مختلفی را مدیریت و سازماندهی کند. بر ورود و خروج اطلاعات نظارت کامل و کافی داشته باشد. امروزه سازمان‌های زیادی کسب و کار خود را به علت از دست دادن عمدی و غیر عمدی اطلاعات شرکت خود (نظیر میزان فروش، فرمول تهیه یک محصول، بازارهای متمرکز و ...) در معرض نابودی قرار داده‌اند. هدف اصلی سیستم مدیریت امنیت اطلاعات هم همین است. جلوگیری از شکست و نابودی شرکت شما به واسطه مدیریت و امن‌سازی اطلاعات سازمان شما.

با توجه به اینکه امروزه استفاده از سیستم مدیریت امنیت اطلاعات امر بسیار ضروری و مهم است، از این رو یکی از خدمات مهم و کلیدی شرکت امن پردازان کویر، ارائه مشاوره، طراحی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) می‌باشد.

با توجه به حساسیت مدیریت امنیت اطلاعات، استفاده از نیروهای متخصص و با تجربه در این زمینه امری بسیار مهم و حیاتی است. تخصص و تجربه دو مسئله حیاتی در استفاده از این سیستم می باشد. چرا که اطلاعات و امنیت اطلاعات شاهرگ حیاتی سازمانها و شرکتهای محسوب می شود. این شرکت با بهره گیری از نیروهای با تجربه و متخصص بومی، سازمانها، شرکتهای و موسسات را در به کارگیری سیستم مدیریت امنیت اطلاعات (ISMS) مبتنی بر استاندارد ISO/IEC 27001، با هزینههای بسیار مناسب و مقرون به صرفه یاری خواهند نمود.

از جمله مزایای پیاده سازی سیستم مدیریت امنیت اطلاعات (ISMS) مبتنی بر استاندارد ISO/IEC 27001، ایجاد یک ساختار برای بهبود مستمر، بومی کردن دانش امنیت اطلاعات در سازمان و همچنین شناسایی داراییها و اطلاعات بحرانی سازمان می باشد.