



# iSMS

Information Security Management System

سیستم مدیریت امنیت اطلاعات، سیستمی به منظور طراحی، پیاده سازی، اجرا، نظارت، بازنگری و بهبود امنیت اطلاعات در سازمان می باشد که به امنیت، با رویکرد فرآیندی و سیستماتیک می نگرد. این سیستم در واقع مجموعه ای از ساختار سازمانی، نیروی انسانی، سیاست های امنیتی، مستندات شناسایی و ارزیابی مخاطرات و کنترل های امنیتی (اعم از منابع انسانی، فیزیکی، سخت افزار، نرم افزار و...) می باشد که وظیفه ایجاد و تداوم امنیت اطلاعات و ارتباطات در سازمان را به عهده دارد. در حال حاضر اکثر سازمان های دولتی و غیردولتی در ایران فاقد چنین سیستمی می باشند ولی به دلیل وابسته شدن روزافزون سازمان ها به تکنولوژی اطلاعات و ارتباطات، افزایش حجم اطلاعات و گسترده شدن ارتباطات و شبکه های رایانه ای و همچنین الزامات هیأت محترم دولت در برنامه پنجم توسعه، نیاز به این سیستم در همه سازمان ها به خصوص دستگاه های اجرائی کشور جدیت بیشتری پیدا نموده است.

با توجه به اخذ گواهینامه مشاوره پیاده سازی در نظام مدیریت امنیت اطلاعات (نما) با رتبه یک از طرف سازمان فناوری اطلاعات ایران، یکی از خدمات کلیدی امن پردازان کویر برای سازمان ها، شرکت های دولتی و خصوصی طراحی و پیاده سازی iSMS می باشد.

## سیستم مدیریت امنیت اطلاعات ISMS

رتبه یک مشاوره استقرار ISMS  
از سازمان فناوری اطلاعات ایران



## ISMS Solution

امن پردازان کویر فعالیت‌های مرتبط با سیستم مدیریت امنیت اطلاعات (ISMS) را براساس نیاز کارفرما، سطح بلوغ امنیتی و شرایط بودجه سازمان، در پنج بسته پیشنهادی ذیل ارائه می‌نماید. پس از انتخاب هر یک از بسته‌ها توسط کارفرما طی مذاکرات و جلسات حضوری، کارشناسان شرکت پیشنهادات فنی و جزئیات بسته‌ها را ارائه خواهند نمود.

### فاز صفر

- شناخت و مستندسازی وضعیت موجود شبکه و امنیت شبکه
- تحلیل وضعیت موجود و ارائه گزارش فنی و مدیریتی
- انجام آزمون نفوذپذیری (Penetration Test)
- ارائه راهکارهای امنیتی و اولویت‌بندی آن‌ها
- امن‌سازی در سطح پیکربندی
- گزارش وضعیت موجود شبکه طبق کنترل‌های امنیتی استاندارد ISO /IEC 27002 و تعیین شکاف موجود

### نظارت

- تعیین دقیق محدوده پیاده‌سازی سیستم
- آموزش اولیه در سطح مدیران و راهبران
- تهیه سند RFP
- مشاوره جهت تعیین شرکت پیمانکار
- نظارت بر فعالیت پیمانکار جهت اجرای اثر بخش سیستم

### طراحی

- آموزش در سطح مدیران، راهبران و کاربران
- شناخت وضعیت موجود با رویکرد امنیتی
- شناسایی و ارزش‌گذاری دارایی‌های اطلاعاتی
- انجام فرآیند مدیریت ریسک (شناسایی، تحلیل و ارزیابی ریسک)
- تهیه طرح مقابله با ریسک (RTP) و تدوین SoA
- ارائه طرح وضعیت مطلوب

کلیه مراحل و فعالیت‌های بسته طراحی براساس الزامات استاندارد ISO 27001: 2013 ارائه می‌گردد.

### طراحی و مشاوره پیاده‌سازی

- انجام کلیه موارد مربوط به بسته طراحی
- شناخت و تحلیل وضعیت فرآیندی و گردش مدارک سازمان
- بررسی و پیشنهاد ابزار و زیرساخت مناسب جهت پیاده‌سازی اثر بخش سیستم
- کمک به کارفرما جهت استقرار و عملیاتی نمودن سیستم

### بازنگری و بهبود

- ممیزی وضعیت موجود در محدوده استقرار یافته
- تطبیق و طراحی جدید در محدوده استقرار یافته و نیاز به توسعه
- مشاوره پیاده‌سازی در محدوده تأیید شده