ISO 27001

سیستم مدیریت امنیت اطلاعات

رشد سریع و سرعت روز افزون تغییرات در علوم و فناوری را در عصر حاضر باید مدیون دسترسی گسترده و فراگیر به اطلاعات دانست. حرکت روبه گسترش جوامع در راستای جامعه اطلاعاتی،موجب رشد وسیع خدمات اطلاعاتی شده و با این نگرش اطلاعات برای یک سازمان، سرمایه ای فوق العاده با ارزش محسوب می شود. با وجود اتصالات گسترده جهانی، اطلاعات می بایست به صورت کنترل شده درمعرض استفاده مخاطبین قرارگرفته و دربرابر تهدیدهای موجود علیه آن ، به نحو مطلوب حفاظت شود. بدین منظور رویکردی تحت عنوان سیستم مدیریت امنیت اطلاعات، حاصل ازتجارب و فعالیت های مستمردردهه ی گذشته درخصوص حفاظت از این مزیت رقابتی سازمان ها پدید آمده است.

دراین خصوص مجموعه ای از استانداردهای مدیریتی و فنی در زمینه امنیت اطلاعات و ارتباطات ، توسط موسسات معتبر بین المللی ارائه گردیده است.

استاندارد BS 7799 (سیستم مدیریت امنیت اطلاعات)، ISO/IEC 17799 (کنترل های مورد نیاز ISMS) و گزارش فنی ISO/IEC TR 13335 (تکنیک های مراحل ایمن سازی اطلاعات و ارتباطات) و نهایتا مجموعه تدوین شده درقالب سری استانداردهای سیستم مدیریت امنیت اطلاعات، ریسک های بحرانی اطلاعات سازمان را کاهش میدهد. این استاندارد برمحرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات سازمان تاکید دارد.

مهم ترین موارد دراین استاندارد ها به شرح زیر می باشد:

- تعیین مراحل ایمن سازی و نحوه شکل گیری چرخه امنیت
- تکنیک های مورد استفاده در هر مرحله ایمن سازی و جزئیات آن
- خط مشی امنیتی و طرح ها و برنامه های تدوین شده و مورد نیاز در این زمینه
- شناسایی،ارزیابی و تدوین راهکارهای برخورد با مخاطرات ریسک در سازمان
- نیاز و نحوه ایجاد تشکیلات سیاست گذار، اجرایی و فنی در زمینه امنیت فضای تبادل اطلاعات
- کنترل های امنیتی مورد نیاز برای حفاظت از سیستم های اطلاعاتی و ارتباطی

فرآیند ممیزی این سیستم بر مبنای قواعد بین المللی صورت میگیرد و شامل مراحل ممیزی مقدماتی (Pre-Audit) به عنوان یک مورد انتخابی و ممیزی صدورگواهینامه (Certification Audit) (مشتمل بردو مرحله ارزیابی مستندات و ممیزی درمحل سازمان) می گردد.

ایمن کارت®