پروژه پایانی – چکیده مقاله ۴: مدیریت امنیت اطلاعات ISO 17799

Information Security Management:
Understanding ISO 17799

تهیه کننده:

آرمین کامفیروزی (۸۹۱۷۹۳)

شراره جهانشاه (۸۹۷۱۶۱)

استاد راهنما:
دکتر بوستانی

اسفند ۱۳۹۰

هدف :

حفظ حیات سازمان، حفظ وجهه مقبول سازمان از منظر مشتری، پرسنل، مدیران وسرمایه گذاران این هدف صرفاً با دسته بندی غیر واقعی اسناد و اطلاعات و زدن برچسب های ایمن سازی اطلاعات) محرمانه، (...، جداسازی اتاقها و سایت های تجهیزات پردازش اطلاعات، ایجاد محدودیت های عبور و مرور در برخی اماکن، داشتن اسم رمز برای دسترسی به سیستم ها به دست نمی آید.

به منظور ایمن سازی سرمایه های سازمان اعم از منقول و غیر منقول، معنوی و انسانی سلسله فعالیتهایی مرتبط و با برنامه ریزی باید انجام پذیرد . در صورتی که از وجوه مختلف برای حفظ سرمایه های سازمان برنامه ریزی شود، آگاهی بخشی و آموزشهای لازم به تمامی پرسنل در کلیه سطوح ارائه گردد، کنترلهای مورد نیاز برای حفظ سرمایه ها تعریف و پیاده سازی شوند، مسئولیت های مرتبط با ایمن سازی سرمایه ها تعریف و واگذار شود، به صورت دوره ای تمامی فعالیتها بازبینی و بهینه سازی شوند، شرایط تداوم سازمان تعیین و اجرای آنها برنامه ریزی گردد، آنگاه به طور نسبی می توان ادعا کرد که برنامه ریزی برای حفظ منابع سازمان انجام پذیرفته است.

یکی از روشهای دسترسی به هدف فوق استق رار استاندارد امنیت اطلاعات است که بخش مقدمه آن در زیر آمده است.

استاندارد مدیریت امنیت اطلاعات**ISO/IEC 17799:2000 :**

2IEC 1و ISO سیستم ویژه ای برای تدوین استانداردهای جهانی می باشند . سازمان های از طریق کمیته های فنی تخصصی در زمین ه های مختلف در توسعه IEC و ISO ملی عضو در زمینه های مشترک با IEC و ISO استانداردهای بین المللی مشارکت دارند . کمیته های فنی IESو ISO یکدیگر همکاری و سایر سازمان های بین المللی، اعم از دولتی و غیر دولتی مرتبط با در این زمینه ایفای نقش می کنند.

در زمینه اطلاعات، ISOو IEC یک کمیته مشترک به نام ISO/IEC JTC1 ایجاد کرده اند. پیش نویس استانداردهای بین المللی توسط کمیته فنی مشترک تدوین و به منظور جمع آوری نظرات سازمان های ملی عضو برای آنان ارسال می شود . استاندارد بین المللی پس از پذیرش 75%سازمان های ملی عضو از طریق نظرسنجی منتشر خواهد شد .استاندارد بین المللی **ISO/IEC 1779** توسط انستیتوی استاندارد انگلیس با نام BS 7799 تهیه و بازبینی و به طور همزمان مورد پذیرش این کمیته و سازمان **ISO/IEC**قرار گرفت.

مقدمه:

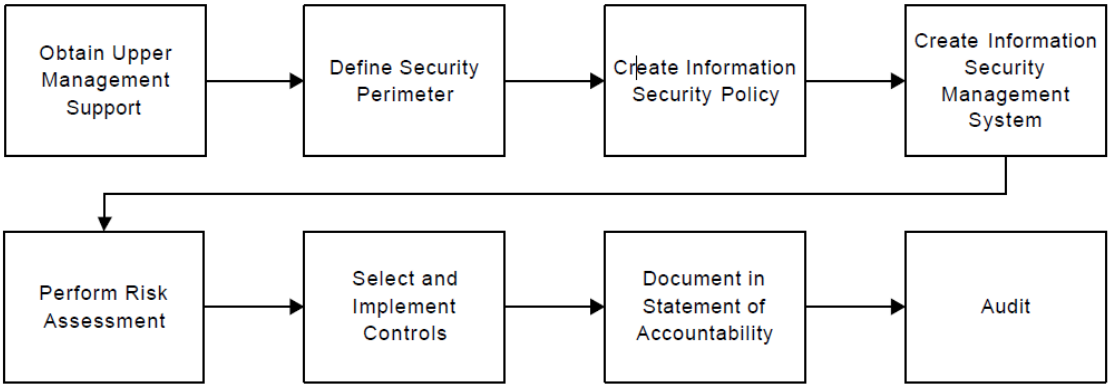
اطلاعات از سرم ایه هایی است که مشابه دیگر سرمایه های مهم کسب و کار3برای سازمان دارای ارزش هستند ،در نتیجه باید به طور مناسبی محافظت شوند . امنیت اطلاعات، به منظوراطمینان از حیات کسب و کار، کاهش خرابیها ، افزایش فرصتهای کسب و کار و بازگشت سرمایه ،محافظت اطلاعات را از حی طه گسترده ای از تهدیدات تضمین می کند. اطلاعات دراشکال مختلفی شامل چاپ یا نوشته شده بر روی کاغذ، ذخیره شده به طور الکترونیکی ، تبادل شده توسط پست یا وسایل الکترونیکی ،ذکر شده در فیلم ها و محاورات وجود دارد. صرفنظر از شکل اطلاعات و ابزارهای ذخیره سازی یا اشتراک آن،اطلاعات همواره باید به طور مناسبی محافظت شود.

امنیت اطلاعات برای حفاظت موارد زیر تعریف شده است:

- محرمانگی: حصول اطمینان از این که فقط افراد دراری مجوز دسترسی، به اطلاعات دستیابی دارند.

- صحت: درستی و تمامیت اطلاعات و روشهای پردازش تأمین گردد.
- قابلیت دسترسی: حصول اطمینان از این که افراد مجاز هر زمان که بخواهند به اطلاعات و سرمایه های مرتبط با آن دسترسی خواهند داشت.

امنیت اطلاعات با ایجاد مجموعه مناسبی از کنترلها شامل سیاستها، روشها، روالها، ساختارهای سازمانی و فعالیتهای نرم افزاری بدست می آید.
برای حصول اطمینان از دسترسی به اهداف ویژه امنیت، کنترلهای فوق می بایست در سازمان پیاده سازی شوند.
چرا به امنیت اطلاعات نیازمندیم:
اطلاعات، پردازشهای پشتیبان آنها، سیستم ها و شبکه ها، سرمایه های مهم کسب و کارمحسوب می شوند . محرمانگی، صحت و قابلیت دسترسی اطلاعات به عنوان اساس و زیر بنای ماندگاری در سطح رقابت، سودمندی، عملکرد صحیح و تأثیر اقتصادی می باشد . سازمانها و سیستم های اطلاعاتی و شبکه های آنها به طور فزاینده با تهدیدات امنیتی گسترده ای مواجه هستند این مخاطرات عبارتند از : بازدارندگی با کمک کامپیوتر، جاسوسی، خرابکاریهای داخلی، خرابکاریهای هدف دار، آب و آتش .
منابع ایجاد خسارت از قبیل ویروسهای کامپیوتری، حملات کامپیوتری و حملات قطع سرویس به صورت فزاینده ای متداول، مؤثر و پیچیده شده اند.
بسته به نوع ابزار، سیستم ها و سرویس های اطلاعا تی سازمانها در مقابل تهدیدات امنیتی به شدت آسیب پذیر شده اند. اتصال شبکه های عمومی و خصوصی و به اشتراک گذاری منابع اطلاعاتی موجود، سبب افزایش مشکلات کنترل دسترسی شده است. تأثیر گرایش به محیط های کامپیوتری توزیع شده اثر بخشی کنترلهای متمرکز و تخصصی را باضعف مواجه کرده است.
اغلب سیستم های اطلاعاتی به طور ایمن طراحی نشده اند . ابزارهای فنی در ارائه امنیت محدود می باشند و برای رفع این محدودیت می بایست از طریق روالها و مدیریت مناسب می توان این محدودیت را برطرف نمود . تعیین نوع کنترلهایی که باید استقرار یابند نی از به طراحی دقیق وتوجه به اجزاء دارد.
مدیریت امنیت اطلاعات، به عنوان حداقل، به مشارکت تمامی پرسنل سازمان،فراهم کنندگان،مشتریان ، شرکاء و دستگاه های بالا و پائین دست نیاز دارد. بهره گیری از مشاوره و اطلاعات متخصصین بیرون سازمان نیز ضروری می باشد.
در شکل زیر مراحل مختلف فرآیند این استاندارد را به صورت گام به گام مشاهده می نمایید:



کنترلهای امنیت اطلاعات چنانچه در مرحله طراحی و نیازسنجی لحاظ شوند به طور قابل ملاحظه ای ارزان و مؤثر خواهند بود.

نحوه تعیین نیازهای امنیتی:

تعیین نیازهای امنیتی سازمان اساسی ترین موضوع در این زمینه است . که از سه منبع اصلی زیر حاصل می شود.

-اولین منبع از تشخیص مخاطراتی که سازمان با آن روبرو است استخراج می شود . در خلال تشخیص مخاطرات، تهدیداتی که سرمایه ها با آن مواجه هستند تعیین می شوند . همچنین آسیب پذیریها و احتمال وقوع آنها ارزیابی شده و تأثیر بالقوه آنها تخمین زده می شود.

-منبع دوم عبارتست ا ز شرایط قانونی،کیفری،نظارتی و قراردادی که سازمان،شرکاء تجاری،طرف قراردادها و تامین کنندگان خدمات باید برآورده نمایند.

-منبع سوم مجموعه مشخصی از مفاهیم،اهداف و شرایط پردازشی اطلاعات است که سازمان برای حمایت از عملکرد خود ایجاد می نماید.

ارزیابی مخاطرات امنیت:

شرایط و نیازهای امنیت به وسیله ارزیابی روشمند مخاطرات امنیتی تعیین می گردند. میزان و وزن برقراری کنترلها در سازمان باید با زیان های احتمالی ناشی از خطاهای امنیتی برابری

داشته باشد. فنون ارزیابی مخاطره می تواند کل سازمان، بخش از آن، سیستم های اطلاعاتی خاص،در صورت امکان سرویس ها یا اجزاء سیستمی خاص، را شامل می شود.

ارزیابی مخاطره، پرداختن سازمان یافته به موارد زیر می باشد:

الف) زیان های احتمالی ناشی از خطاهای امنیتی سازمان، در نظر گرفتن و برآورد نتیجه بالقوه کاهش محرمانگی، صحت و قابلیت دسترسی اطلاعات و سرمایه ها.

ب) نتیجه این ارزیابی به تعیین و هدایت اولویتها و اقدامات مناسب مدیریتی برای مدیریت مخاطرات امنیت اطلاعات و استقرار کنترلهای انتخاب شده برای مقابله با این مخاطرات کمک خواهد کرد . فرایند ارزیابی مخاطرات و انتخاب کنترلها می تواند چندین بار اجراء شد ه تا بخش های مختلف سازمان یا سیستم های اطلاعاتی خاص را شامل می شود.

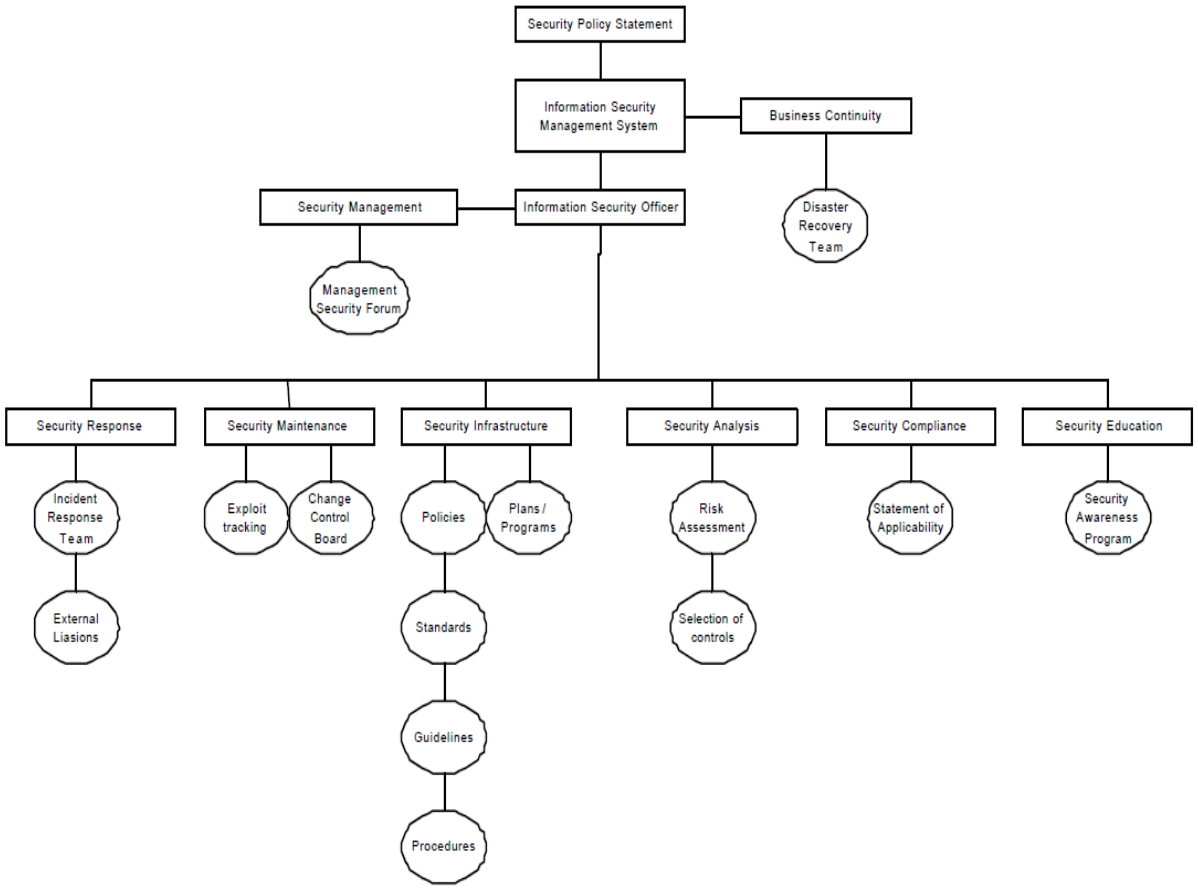
جدول زیر نحوه ارزیابی مخاطرات را نشان می دهد.

Probability of event	Frequency	Rating
Negligible	Unlikely to occur	0
Very Low	2 – 3 times every 5 years	1
Low	< = Once per year	2
Medium	< = Once every 6 months	3
High	< = Once per month	4
Very High	= > Once per month	5
Extreme	= > Once per day	6

انجام بازبینی مستمر و دوره ای مخاطرات امنیتی و کنترلهای استقرار یافته برای رسیدن به اهداف زیر از اهمیت زیادی برخوردار است:

- لحاظ کردن تغییردر اولویتها و نیازهای سازمان
- تشریح آسیب پذیریها و تهدیدات جدید
- اطمینان از مناسب و مؤثر بودن کنترلها

بر اساس نتیجه ارزیابی های قبلی و تغییر سطوح مخاطراتی که مدیریت آمادگی پذیرش آن را دارد، ازبینی باید در سطوح مختلفی اجرا گردد .به منظور اولویت بندی منابع از نظر حوزه مخاطرات اساسی،ارزیابی مخاطرات اغلب در مرحله اول در سطح بالایی انجام می شود و سپس برای شناسایی دقیق مخاطرات،ارزیابی به صورت ریز و جزیی انجام می شود.



انتخاب کنترلها:

پس از تعیین و تعریف نیازهای امنیتی ،انتخاب و استقرار کنترلها جهت اطمینان از کاهش خاطرات به سطح قابل قبول انجام خواهد شد .کنترلها را می توان از متن استاندارد ۱۷۷۹۹ یا مستندات دیگر انتخاب و یا کنترلهای جدیدی برای پوشش مناسب نیازهای مشخص را طراحی نمود. روشهای مختلفی برای مدیریت مخاطرات وجود دارد که در استاندارد ۱۷۷۹۹ نمونه هایی از ذکر این نکته ضروری است که برخی کنترلها برای هر محیط یا سیستم اطلاعاتی یا برای هرسازمان قابل پیاده سازی و اجراء نخواهد بود . به طور مثال تفکیک وظائف و مسئولیتهای پرسنل می تواند یکی از کنترلهایی باشد که از خطا و مخاطره پیشگیری می نماید اما ممکن است در سازمانهای کوچک امکان تفکیک وظائف وجود نداشته باشد.

نقطه آغاز امنیت اطلاعات :

به منظور استقرار امنیت اطلاعات تعدادی از کنترلها به مثابه مأخذ اساسی نقطه آغاز خواهند بود.این کنترلها نیازهای پایه قانونی یا به عنوان بهترین روشهای متداول برای امنیت اطلاعات خواهند بود.

کنترلهای اساسی که برای هر سازمان از جنبه قانونی باید درنظرگرفته شود:

الف) حفاظت داده و اطلاعات خصوصی افراد

ب) محافظت از بایگانی ها و سوابق سازمانی

ج) حقوق سرمایه های معنوی

کنترلهایی که باید به عنوان بهترین روشها برای امنیت اطلاعات در نظر گرفته شوند:

الف) مستند سیاست امنیت اطلاعات

ب) تعیین مسئولیتهای امنیت اطلاعات

ج) آموزش و یادگیری امنیت اطلاعات

د) گزارش وقایع امنیتی

ه) مدیریت تداوم سازمان

کنترلهای فوق در اغلب محیط ها و سازمان ها قابل اعمال هستند . لازم به ذکر است یادآوری نماید اگر چه همه کنترلها ی ذکر شده در این استاندارد مهم هستند اماارتباط هر کنترل باید از نظر مخاطره ای که سازمان با آن مواجه است تعیین گردد .اگر چه ایده فوق به عنوان نقطه آغاز مناسبی در نظر گرفته شده است اما نباید جایگزین انتخاب کنترلها بر اساس روش ارزیابی مخاطرات گردد.

عوامل اساسی موفقیت:

تجربه نشان داده است که عوامل زیر اغل ب در موفقیت استقرار امنیت اطلاعات در سازمان حیاتی هستند:

- اقتباس سیاستهای امنیتی ، اهداف و فعالیتها از اهداف سازمان
- انطباق روش استقرار امنیت اطلاعات با فرهنگ سازمان
- پشتیبانی و مشارکت موثر و ملموس مدیریت
- درک درست از نیازهای امنیتی،ارزیابی و مدیریت مخاطرات
- گزارش آگاهی در خصوص سیاست امنیت اطلاعات و استانداردها برای پرسنل

و پیمانکاران

- برقراری آموزشها و یادگیری مناسب
- وجود سیستم متوازن و کامل ارزیابی به منظور ارزیابی مدیریت امنیت

اطلاعات و ارائه بازخورد برای بهبود