استاندارد BS7799

نویسنده : کیانوش مرادیان
BS7799 LA ، CCNA
ناشر : مهندسي شبکه همکاران سیستم

آیا دارایی های سازمان شما مورد ارزیابی قرار می گیرند؟

BS7799 استانداردی است که شما را قادر به ارزیابی اطلاعات و محافظت از آن می کند در واقع اطلاعات ، کلید موفقیت و رشد هر سازمانی است.

امروزه اطلاعات مهمترین دارایی هرسازمانی می باشد که نظیر سایر وسایل موجود در سازمان دارای ارزش بوده و درنتیجه باید بطور مناسب حفاظت گردد.

دسترسی غیرمجاز و رخنه به اطلاعات روی دیسک ها ، کامپیوترها و استفاده غیرمجاز از آنها تبدیل به معضل شده است و این دسترسی توسط کارمندان یک سازمان،کاربران اینترنت و یا توسط عوامل دیگر صورت می گیرند لذا سازمان ها و شرکت ها ناگزیر به دنبال پیاده سازی موارد امنیتی می باشند.

برای پیاده سازی امنیت تنها توجه به مسائل تکنیکی کافی نیست بلکه ایجاد سیاستهای کنترلی و استاندارد کردن آن و همچنین ایجاد روالهای صحیح درصد امنیت اطلاعات را بالا خواهد برد.

فوائد اجرا و گرفتن گواهینامه BS7799 به شرح زیرمی باشد:

اطمینان از تداوم تجارت و کاهش صدمات توسط ایمن ساختن اطلاعات و کاهش تهدیدها

اطمینان از سازگاری با استاندارد امنیت اطلاعات و محافظت از داده ها

قابل اطمینان کردن تصمیم گیری ها و محک زدن سیستم مدیریت امنیت اطلاعات

ایجاد اطمینان نزد مشتریان و شرکای تجاری

امکان رقابت بهتر با سایر شرکت ها

ایجاد مدیریت فعال و پویا در پیاده سازی امنیت داده ها و اطلاعات

بخاطر مشکلات امنیتی اطلاعات و ایده های خود را در خارج سازمان پنهان نسازید.

استاندارد BS7799 پرسنل،تکنیک ها و ایده ها را ایمن خواهد ساخت.

امروزه داشتن حجم بالای اطلاعات در سازمان نیازمند پیاده سازی استاندارد مناسب در زمینه امنیت می باشد. اهمیت این قضیه در برخی سازمان ها حساس تر می باشد. شرکت های بیمه ، بانک ها و پیمانکاران مختلف نمونه اینگونه سازمان ها هستند. همچنین شرکت های ساختمانی و شرکت های مشاوره ای نیازمند حفاظت از اطلاعات خود و یا بهتر بگوییم اطلاعات سایر سازمان ها می باشند این اطلاعات در قالب طراحی ، نقشه ها و اطلاعات عمومی و . . . هستند. هدف اصلی و نگرش به استاندارد BS7799 در سه قالب جلوگیری ، حفاظت و ثبت اطلاعات می باشد. استاندارد انواع مختلف اطلاعات مربوط به سازمان نظیر امضای الکترونیکی، اسناد مکتوب و . . . را شامل می شود اما بحث پیاده سازی سیاست کنترلی مشخص برای افراد مختلف درون سازمانی و برون سازمانی از اهمیت بالاتری برخوردار است. نحوه اطمینان به پرسنل و روالهای مختلف برای برخورد با افرادی که از شرکت می روند شامل این استاندارد می شود.

BS7799 نتیجه تلاش برای رسیدن به یک قالب مشترک پیاده سازی استاندارد امنیت برای سازمان های مختلف با زمینه کاری مختلف می باشد. امروزه استاندارد ISO راهنمایی خاص را برای رسیدن به این منظور به نام ISO/IEC 17799:2000 ارائه داده است که در واقع تمرینی جدی و عالی برای پیاده سازی امنیت اطلاعات می باشد. این رهنمودها با دقت خاصی در استاندارد BS7799-2:2002 گردآوری شده است که نتیجه پیاده سازی آن اخذ گواهینامه امنیت اطلاعات می باشد. پیاده سازی این استاندارد سبب خواهد شد تا امکان سوء استفاده از اطلاعات ، ازبین رفتن آن و سایر خطرات به حداقل برسد.امنیت اطلاعات برای جلوگیری از دسترسی های غیر مجاز به اطلاعات ایجاد شده است. BS7799 حفاظت از اطلاعات را در سه مفهوم خاص یعنی قابل اطمینان بودن اطلاعات (Confidentiality) ، صحت اطلاعات (Integrity) و در دسترس بودن اطلاعات (Availability) تعریف می نماید.

Confidentiality : تنها افراد مجاز ، به اطلاعات دسترسی خواهند یافت.
Integrity : کامل بودن ، صحت اطلاعات و روشهای پردازش اطلاعات مورد نظر هستند.
Availability : اطلاعات در صورت نیاز بطور صحیح در دسترس باید باشد.

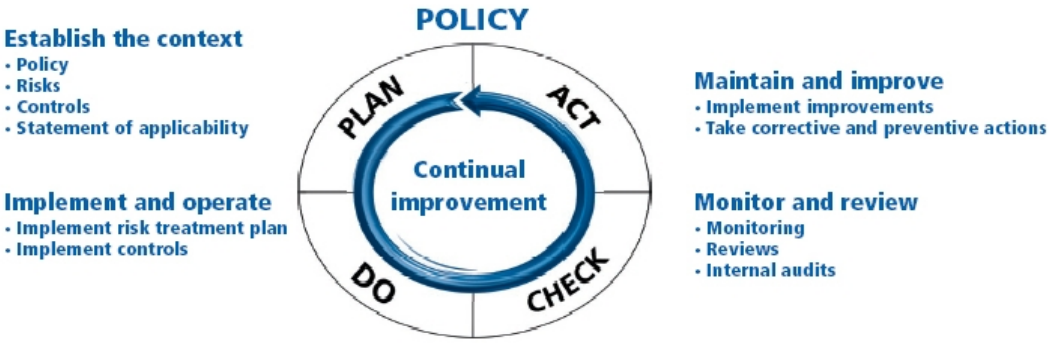
ISO/IEC 17799 Information Technology-Code of practice for information security

کنترلهای زیر موارد پایه ای برای پیاده سازی سیستم امنیت اطلاعات هستند:

۱- سیاستهای امنیتی
۲- امنیت سازمان
۳- کنترل و طبقه بندی دارایی ها
۴- امنیت فردی
۵- امنیت فیزیکی
۶- مدیریت ارتباط ها
۷- کنترل دسترسی ها
۸- روشها و روالهای نگهداری و بهبود اطلاعات
۹- مدیریت تداوم کار سازمان
۱۰- سازگاری با موارد قانونی

BS7799-2:2002 ISMS-Specification with guidance for use

هدف اصلی و اولیه سیستم مدیریت امنیت اطلاعات حفاظت از اطلاعات می باشد. ساختار این پردازش بر پایه رده بندی دارایی های سازمان و درجه اهمیت آن ها بنا نهاده شده است. این دارایی ها ممکن است امضای الکترونیکی ، اسناد مکتوب و یا دارایی های فیزیکی نظیر کامپیوترها و شبکه و یا هرچیز با ارزش دیگری باشد. دراین تعریف حتی افراد مختلف سازمان هم دارایی محسوب می شوند.



تصویر بالا وظایف اصلی و پایه ای را در ISMS یا سیستم مدیریت امنیت اطلاعات نشان می دهد.با دقت در این عکس پویا بودن این سیستم کاملا مشهود است.

BS7799-2002 شامل لیستی از کنترل ها می باشد که نیاز واقعی سازمان به داستن استانداردی کامل و پویا را برطرف می کند.

مراحل اخذ گواهینامه امنیت اطلاعات

سیستم ISMS برای هر سازمان و شرکت برپایه خطرات مختلف محتمل در آن شرکت پیاده سازی می شود که نیازمند به بازرسی های مداوم توسط شخص خبره و آشنا به مفاهیم استاندارد BS7799 دارد.پس از پیاده سازی و بازرسی های دقیق برای اجرای بدون نقص ۱۲۷ کنترل مصوب در استاندارد شخص گواهی دهنده (Certification Body) جهت بازرسی نهایی و تعیین صلاحیت برای دادن گواهینامه امنیت مراجعه کرده و سازمان را مورد ارزیابی دقیق قرار می دهد.برای گرفتن گواهینامه اجرای دقیق کلیه کنترل هایی که قابل پیاده سازی هستند نیاز است.

ISMS سیستم مدیریتی کامل و مجتمع می باشد.

این استاندارد در ردیف ISO 9001:2000 و ISO 14001:1996 برای پشتیبانی و نظارت در صحت اجرا و پیاده سازی می باشد.

چه کسی قادر به گرفتن این گواهینامه است؟

این استاندارد به سازمان ها ، اداره ها ، سایت ها و کلیه زیرمجموعه های اداری قابل اعطاء می باشد. سازمان ها با اندازه هاو پیچیدگی های مختلف قادر هستند با پیاده سازی این کنترل ها گواهینامه معتبر و بین المللی BS7799 اخذ کنند.

آیا استاندارد BS7799 مورد نیاز شماست؟

BS7799 یعنی چه؟

BS7799 استانداردی انگلیسی و راهنمایی برای حفاظت اطلاعات و تجهیزات سازمان می‌باشد. BS7799 در دو قسمت ISO/IEC 17799:2000 و BS7799-2 1999 آمده است.

بخش اول کدهای استانداردی است که راهنمای اولیه برای حفاظت دارایی و اطلاعات یک سازمان می باشد که باید اجرا شود. محدوده این استاندارد صوت،اینترنت ، تلفن ها ، نمابر و . . . را در بر می‌گیرد.

بخش دوم شرایط استاندارد مدیریتی برای مدیریت و امنیت اطلاعات (ISMS) می باشد. با کمک این بخش به سازمانها پیمودن مراحل مختلف این قالب مدیریتی آموزش داده می شود. این قالب، افراد، سیستم IT و پروسه های مختلف را در بر می گیرد.

ISMS یا Information Security Management System برای حصول موارد زیر ایجاد می شود.

- دارایی های با ارزش که نیاز به حفاظت دارند مشخص خواهند شد.
- سازمان را برای مدیریت خطرها آماده می کند.
- کنترل های مختلف را برای این حفاظت ایجاد می کند.
- میزان اطمینان مورد نیاز را مشخص می کند.

کنترل هایی که در BS7799-2:1999 لحاظ شده است به قرار زیر است :

۱- سیاست های امنیتی
۲- امنیت سازمان
۳- دسته بندی دارایی های با ارزش و کنترل آنها
۴- امنیت افراد
۵- امنیت فیزیکی و محیط کار
۶- امنیت ارتباطات و مدیریت اجرا
۷- کنترل دسترسی ها
۸- سیستم نگهداری و ارتقاء
۹- نقشه ادامه Bussiness شرکت
۱۰- سازگاری با موارد قانونی

چرا BS7799 معروف است ؟

بیشتر صحبتها امروزه در مورد BS7799-2 است که در سال 1999 منتشر شده است. دلیل محبوبیت این استاندارد در سالهای اخیر اهمیت بسیارزیادحفاظت اطلاعات می باشد.

امروزه دسته بندی و درجه بندی اهمیت دارایی های با ارزش سازمان توسط مدیریت سازمان مشخص می شود. هر چقدر این دسته بندی و اطلاعات کامل تر باشند پیشبرد اهداف امنیتی یک سازمان آسان تر صورت خواهد پذیرفت. همانطور که می دانید "Knowledge is power".

BS7799-2 یکی از معدود روشهایی است که اطلاعات و امنیت آنها را با جزئیات کامل بیان می کند. در واقع چگونگی مدیریت امنیت اطلاعات توسط BS7799 بیان شده است.

سازگاری

سازگاری با BS7799 سازمان را مجبور می سازد سیستم امنیت اطلاعات را اجرا نموده و مستند نماید همچنین بندهای کنترلی مختلف در آن سازمان اجرا خواهند شد.

گواهینامه

گواهینامه BS7799 در صورت مستند بودن کلیه موارد امنیتی یک سازمان و همچنین به اجرا درآمدن صحیح آنها به سازمان تعلق می گیرد. در واقع پیاده سازی کلیه کنترلهای BS7799 شرط دریافت گواهینامه می باشد.

قبل از تطابق و حرکت در مسیر داشتن این استاندارد موارد زیر مدنظر هستند.

۱- دانستن وسعت و گستردگی کنترلهای مختلف استاندارد
۲- مشخص کردن کنترلهای وابسته به سازمان
۳- سنجیدن فوائد استاندارد با توجه به هزینه ها و زمان
۴- نیازمندیهای قانونی
۵- نیازمندیهای تنظیمی
۶- ساختار سازمان

ممکن است در این ارزیابی اولیه خیلی از سازمانها به این نتیجه برسند که نیاز برای اجرای کامل استاندارد وجود ندارد و تنها به استاندارد سازی بخشی از سازمان اکتفا نمایند.

چه مواردی جهت این سازگاری لازم هستند؟

اولین قدم برای رسیدن به این مهم برقراری و نگهداری مستندات ISMS می باشد.

۱- دارایی های با ارزش حفاظت شوند
۲- سازمان به سمت مدیریت خطرات پیش برود
۳- کنترلهای موجود در استاندارد لحاظ شود
۴- درجه امنیت مورد نیاز سازمان تعیین شود

سازگاری با BS7799 اجرای شش مرحله را طلب می کند.

مرحله اول : سیاست های امنیت اطلاعات سازمان مشخص می شود.

مرحله دوم : ناحیه اجرای استاندارد مشخص می شود. سازمان مشخص می کند کدام کنترل ها برای سازمان ضروری می باشند . حاصل این کنترل های انتخاب شده به نیازمندیهای سازمان، دارایی های نیازمند به ایمنی ،مکان و تکنولوژی بستگی دارد.

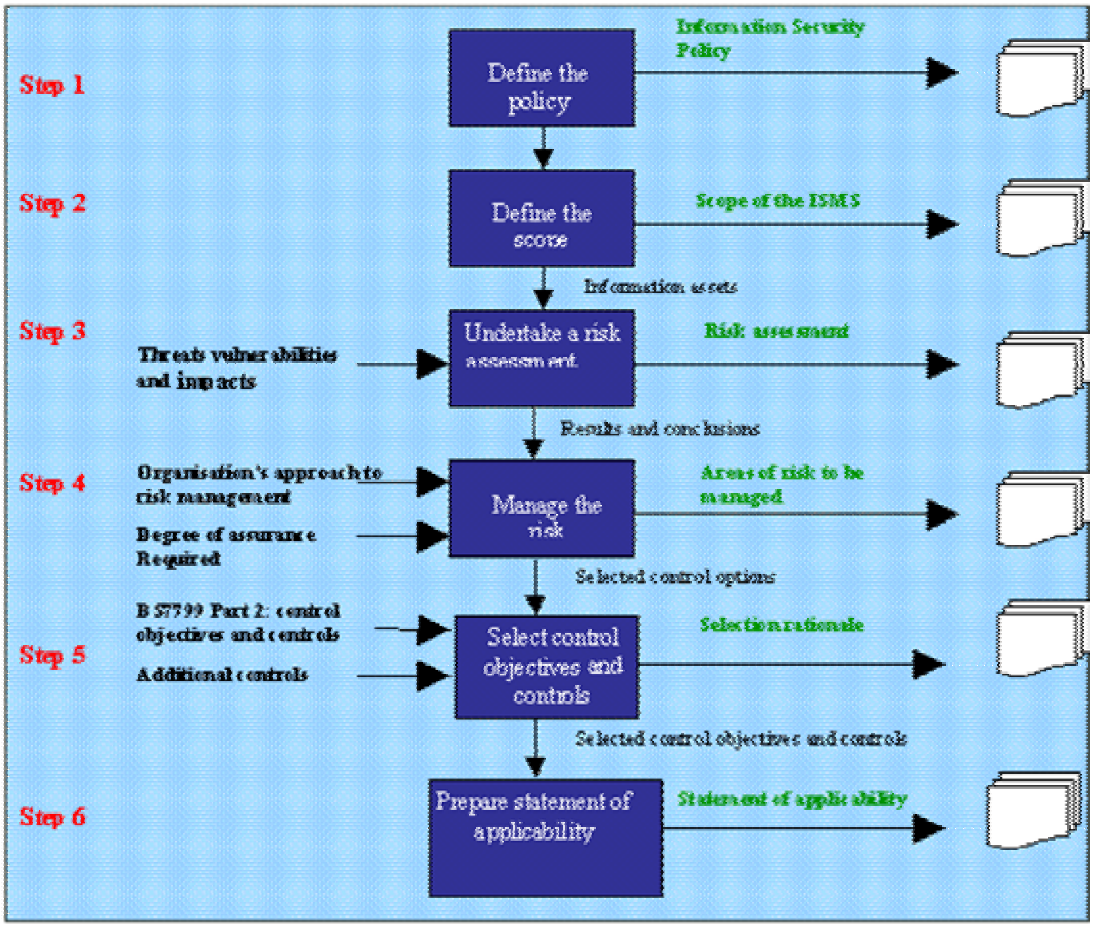
مرحله سوم : ارزیابی خطرات : هدف از این ارزیابی مشخص کردن تهدیدها و مخاطرات دارایی ها می باشد. نتیجه این ارزیابی درجه خطر را مشخص می نماید.

مرحله چهارم : مدیریت خطرها می باشد. محدوده مدیریت خطر توسط سیاستهای امنیتی اطلاعات و همچنین میزان امنیت مورد نیاز سازمان مشخص خواهد شد.

مرحله پنجم : انتخاب کنترل ها در بند ۴ استاندارد BS7799 لحاظ شده است که باید اجرا شوند.

مرحله ششم : امکان پذیری اجرا مدنظر قرار گیرد

یک سازمان نیاز به مستند کردن کنترلهای انتخاب شده دارد. بعضی از این کنترلها به دلیل ماهیت سازمان نیاز به اجرا ندارند که باید مشخص شوند.



شش مرحله اصلی در BS7799

آیا باید گواهینامه گرفت ؟

تصمیم گیری در این مورد کاملا خصوصی است و به موارد زیر و میزان اهمیت امنیت در یک سازمان بستگی دارد.

۱- محدوده امنیتی مشخص شود

۲- مستندات و اجرا با کنترلهای مصوب در استاندارد سازگاری داشته باشد.

۳- استثنا ها مشخص و توجیه منطقی شوند.

بعد از این مراحل می توان برای دریافت گواهینامه BS7799 اقدام کرد لذا نیاز به حضور ارزیاب و کارشناسان BS7799 پیدا خواهد شد.

اجرای پیش نیازها پروسه پرزحمت و مداومی را طلب می کند که باید با دقت و کاملا دقیق اجرا شود. برای اجرا این پیش نیازها نیاز به مرور دوره ای توسط ارزیاب های BS7799 می باشد که در صورت اخذ گواهینامه BS7799 این بازدید توسط ارزیابان BS7799 هر سه سال تکرار خواهد شد.

در آخر ، نتایج اخذ این مدرک و مفید بودن آن در پیشبرد اهداف سازمان باید کاملا مدنظر قرار گیرد.

البته اعتباری که یک سازمان در نتیجه اخذ این مدرک خواهد گرفت باید مورد توجه قرارگیرد.

تفکر اینکه اخذ این گواهینامه ۱۰۰٪ اطلاعات شما را امن می کند کاملا اشتباه است و تنها شما قادر شده اید خطرات را تا حد زیادی پیش بینی کرده ، قانونمند نموده و خنثی نمایید.

چه مواردی برای اخذ گواهینامه مورد نیاز است؟

برای دریافت این گواهینامه کلیه سازگاریها با بندهای استاندارد صورت پذیرد همچنین نیاز به بازدیدهای دوره ای توسط ارزیابهای BS7799 می باشد. پس از محقق شدن کلیه مراحل و ارزیابی های مختلف و سازگاری کامل، شخص گواهینامه دهنده ازشرکت معتبر BSI جهت بازدید نهایی و اعطای گواهینامه مراجعه خواهد کرد . در صورت عدم تطابق بیش از یک کنترل مهم اعطای گواهینامه به آینده و بازدید بعدی منوط خواهد شد.

نتیجه : BS7799-2 استانداردی مدیریتی برای حفاظت از اطلاعات و دارایی های با اهمیت یک سازمان می باشد و اگر سازمان شما نیازمند امنیت اطلاعات است BS7799 نظر شما را تامین خواهد کرد.