استاندارد مدیریت حفاظت اطلاعات و نقش آن در عملکرد سازمانها

● محمد اسماعیل حاجیان

● شهلا شهابی

مقدمه

امروزه در هر سازمانی بحث به کارگیری IT و فن‌آوری اطلاعات مطرح است همه جا سخن از سودمندی یا ضروری بودن استفاده از کامپیوتر به میان می‌آید به همین خاطر اغلب مدیران درگیر تصمیم‌گیری برای صرف هزینه یا سرمایه گذاری برای به کارگیری تکنولوژی در سازمان خود هستند اما یک سوال همواره پیش‌رو است که: مرز سرمایه گذاری و تکنولوژی کجاست؟

طبیعی است که تکنولوژی به عنوان یک راه به صرفه‌تر در برابر روشهای دستی یا سنتی است که اهمیت پیدا می‌کند. به همین منظور یک مدیر باید بداند تکنولوژی در کدام بخش از سازمان یا زنجیره فعالیتهایش مفیدتر است و برای پاسخ دادن به این سؤال احتیاج به شاخصهایی برای اندازه‌گیری دارد برای شروع بحث به مرور و تعریف مفاهیم اصلی می‌پردازیم و پیش از همه تفاوت بین فن‌آوری اطلاعات (IT) و information Technology و information system (IS) را توضیح می‌دهیم زیرا این دو مفهوم گر چه به طور ناخواسته به جای یکدیگر به کار برده می‌شوند اما معانی متفاوتی دارند.

فن‌آوری اطلاعات چیست؟

فن‌آوری اطلاعات مجموعه‌ای شامل حداقل یکی از اجزای ۱- سخت‌افزار Hard ware ۲- نرم‌افزار Soft ware ۳- سیستم‌های ارتباطی Telecommunication ۴- ایستگاه کاری Work saion ۵- سیستم‌های خودکار سازی Computer controlled robots ۶- محصولات هوشمند Smart Products می‌باشد.

سامانهٔ اطلاعاتی چیست؟

سامانهٔ اطلاعاتی یکی از نتایج حاصل از به کارگیری فن‌آوری اطلاعات است که به کمک آن اطلاعات مختلف رده‌بندی و طبقه‌بندی می‌شوند تا دوباره به کار گرفته شوند.

انواع سامانه‌ها یا سیستم‌های اطلاعاتی به شرح ذیل می‌باشند:

الف: مدیریت محتوا

ب: مدیریت مستندات و مدارک

ج: مدیریت اطلاعات

د: پشتیبانی تصمیم‌گیری

ه: اطلاعات اجرایی

و: پشتیبانی مدیریت

ز: اطلاعات استراتژیک

براساس کارکردهای مختلف فن‌آوری اطلاعات و ترکیب قابلیت‌های آن سامانه‌های اطلاعاتی شکل می‌گیرند بدین لحاظ برای فهم نقش فن‌آوری در سازمان ابتدا باید کارکردهای پایهٔ آن را شناخت.

کارکردهای پایهٔ فن‌آوری اطلاعات

Basic functions of IT

هر جا که فن‌آوری اطلاعات به کار گرفته شود حداقل یکی از عملیات زیر و معمولاً ترکیبی از آنها اتفاق می‌افتد:

- تبدیل یعنی اطلاعات از یک شکل به شکل دیگر تبدیل می‌شوند مثلاً پخش صوت از یک بلندگو یا اسکن کردن متن یک قرارداد و تبدیل آن به قالب الکترونیک
- ذخیره‌سازی
- پردازش مثل تراز مالی در یک نرم‌افزار حسابداری تعاونی
- تبادل مثل مبادله اطلاعات از یک کامپیوتر به کامپیوتر دیگر در یک شبکه محلی
- تحلیل و همگرایی مثل نرم‌افزارهای هوشمند طراحی صنعتی و الکترونیکی

فن‌آوری‌های نوپدید

از ترکیب کارکردهای بالا فن‌آوری‌های جدیدی پدید آمده است که به تنهایی هویت خاص خود را پیدا کرده‌اند و بسیار پیش می‌آید که یک طرح به کارگیری تکنولوژی در سازمان یکی از این‌ها را به عنوان هدف طرح ذکر می‌کند مثل طرح اتصال شرکت شما به اینترنت. بعضی از فن‌آوری‌ها به قرار ذیل هستند:

الف- چندرسانه‌ای

ب- شبکه‌های کامپیوتری

ث- بسته‌های نرم‌افزاری

ج - انبارهای داده

چ- فن‌آوری بدون سیم

خ - سیستم‌های هوشمند

د - اینترنت

برنامه‌ریزی فن‌آوری اطلاعات

هر برنامه انتقال یا به کارگیری فن‌آوری به سازمان باید به سؤال‌های زیر پاسخ دهد:

- چه؟ برای چه چیزی می‌خواهد در سازمان به کار گرفته شود؟
- کجا؟ برای کدام بخش و کدام فعالیت؟
- چه وقت؟
- چقدر هزینه؟ در ازای چقدر سود؟
- چگونه؟ مراحل انجام کار چیست؟
- توسط چه کسی؟ (درون داد یا برون داد)

فن‌آوری اطلاعات در سازمان

نقش پشتیبانی

در این نقش فعالیت اصلی و محوری سازمان بدون استفاده از فن‌آوری هم انجام می‌شود اما به کارگیری آن به نحوه انجام فعالیتها به شدت کمک می‌کند یا اینکه آن را توسعه می‌دهد مثل به کارگیری اتوماسیون اداری یک تعاونی که با به کارگیری سیستم مالی یا حسابداری انجام‌پذیر می‌شود گرچه می‌توان همان حساب و کتاب‌ها را در دفاتر نگه داشت اما کامپیوتر انجام عملیات حسابداری را تسهیل می‌کند.

نقش محوری

فن‌آوری برای برخی سازمان‌ها نقش محوری دارد به نحوی که بدون به کارگیری آن اگر چه می‌توان به فعالیت ادامه داد اما تفاوت بین به کارگیری و عدم به کارگیری فن‌آوری فاحش است مثل به کارگیری سیستم تایپ کامپیوتری در یک روزنامه یا انتشاراتی. امروزه تقریباً بدون به کارگیری حروفچینی کامپیوتری اداره یک روزنامه یا انتشار یک کتاب غیرممکن است.

نقش استراتژیک

در نقش استراتژیک اصولاً ادامه فعالیت سازمان بدون به کارگیری فن‌آوری بی معنی و مفهوم است مثل شبکه ارتباطی برای فروش بلیط هواپیما یا به کارگیری کامپیوتر در سیستم بانکی

آخرین تقسیم‌بندی کشورهای جهان از دیدگاه رشد در زمینه IT با پنج گروه زیر معرفی شده‌اند: ۱- پیشتازان: این دسته ۱۳ درصدی از کشورهای جهان از جمله آمریکا، سنگاپور، آلمان به عنوان پیشروان توسعه و کاربری فن‌آوری اطلاعات با سرمایه‌گذاری‌های هنگفت در این مسیر حرکت می‌کنند.

۲- تندروندگان: ۱۱ درصد از کشورها مانند ایتالیا با برنامه‌ای مدون و تا اندکی مجارستان و کویت

۳- آیندگان کشورهایی مانند آفریقای جنوبی، شیلی، روسیه با درک موفقیت راهبردی فن‌آوری اطلاعات برنامه‌ریزی‌های کلانی را برای به دست گرفتن این فرصت آغاز کرده‌اند که شامل ۲۲ درصد کشورهای جهان هستند.

۴- آغازگران: این گروه که ۱۹ درصد کشورهای جهان را شامل می‌شوند مانند چین، مصر، فیلیپین در ابتدای راه حرکت به سوی فن‌آوری اطلاعاتند.

۵- بازماندگان: بیشترین کشورهای جهان در این گروه ۳۷ درصدی قرار می‌گیرند که در واقع هیچگونه برنامه مدونی برای توسعه اطلاعاتی ندارند.

ایران در بین کشورهای جهان جز همان ۵۰ درصدی است که در دو گروه آخر یعنی آغازگران و بازماندگان فن‌آوری اطلاعات قرار گرفته و از قافله شتابان انقلاب اطلاعاتی عقب مانده است که گفته می‌شود که مهمترین دلیل آن نبود سیاستگذاری راهبردی و دم تدوین برنامه توسعه مبتنی بر فن‌آوری اطلاعات است و این در حالی است که نقش آن همانند ستون فقرات تمدن جدید بشری است که در نیمه دوم قرن بیستم متولد شده است و در حال رشد سریع و حرکت به سوی آینده می‌باشد. برای کشورهای در حال توسعه مثل ایران ضروری است که بینش روشنی داشته باشند و استراتژی دراز مدتی را به منظور تبدیل شدن به بازیگری عمده در عرصه جهانی اتخاذ کنند دیگر آنکه نباید از ذهن دور داشت که اتلاف وقت در اتخاذ این استراتژی کشورها را در بازار مکاره رقابت‌های جهانی به شدت عقب نگاه خواهد داشت.

سیستم مدیریت امنیت اطلاعات

مفهوم ISMS را به صورت مختصر به عنوان نگرشی سیستماتیک به منظور مدیریت بر اطلاعات حساس سازمانی که باید ایمن باشد در نظر می‌گیریم.

درحال حاضر وضعیت امنیت فضای تبادل اطلاعات کشور به ویژه در حوزه دستگاههای دولتی در سطح نامطلوبی قرار دارد از جمله دلایل اصلی آن می‌توان به فقدان زیرساخت‌های فنی و اجرایی امنیت و عدم انجام اقدامات موثر درخصوص ایمن‌سازی تبادل اطلاعات دستگاههای دولتی اشاره نمود.

بخش قابل توجهی از وضعیت نامطلوب موجود امنیت فضای تبادل اطلاعات کشور به واسطه فقدان زیرساختهایی ازقبیل: ۱- نظام ارزیابی امنیتی فضای تبادل اطلاعات ۲- نظام صدور گواهی و - زیر ساختار کلید عمومی ۳- نظام تحلیل و مدیریت مخاطرات امنیتی ۴- نظام مقابله با جرائم مرتبط با فضای تبادل اطلاعات و ۵- سایر زیرساختهای امنیت فضای تبادل اطلاعات کشور می‌باشد از سوی دیگر وجود زیرساختهای فوق قطعاً تاثیر بسزایی در ایمن سازی فضای تبادل اطلاعات کشور خواهد داشت. صرف‌نظر از دلایل مذکور نابسامانی موجود در وضعیت امنیت فضای تبادل اطلاعات دستگاه‌های دولتی از یک سو موجب بروز اخلال در عملکرد صحیح دستگاه‌ها شده و کاهش اعتبار این دستگاه‌ها را در پی خواهد داشت و از سوی دیگر موجب اتلاف سرمایه‌های ملی می‌شود.

علیهذا همزمان با تدوین سند راهبردی امنیت فضای تبادل اطلاعات، توجه به مقوله ایمن‌سازی فضا ضروری به نظر می‌رسد این امر علاوه بر کاهش صدمات و زیان‌های ناشی از وضعیت فعلی امنیت

دستگاه‌های دولتی نقش موثری در فرایند تدوین سند راهبردی امنیت فضای اطلاعات کشور خواهد داشت امروزه امنیت و حفاظت اطلاعات برای یک شرکت تعاونی نیز به منزله موارد زیر می‌باشد:

الف- سرمایه‌ای برای شرکت

ب - اسلحه‌ای در مقابل رقیبان

منابع خطری که می‌تواند طلاعات یک سازمان را تهدید کند را می‌توان در چهار بخش زیر متمرکز نمود:

۱- از داخل سازمان ۲- از خارج سازمان ۳- از روی تصادف ۴- از روی عناد از طرف دیگران

تعریف حفاظت از اطلاعات: اطلاعات یک سرمایه ارزشمند برای سازمان است و احتیاج به حفاظت مناسب دارد. حفاظت اطلاعات ابزاری است برای حفاظت از تهدیدها به منظور استمرار در روند کار، حداقل نمودن خسارات و حداکثر کردن بازگشت سرمایه و ایجاد فرصت‌های شغلی مناسب و مرتبط

تاریخچه تهیه آیین‌نامه حفاظت اطلاعات

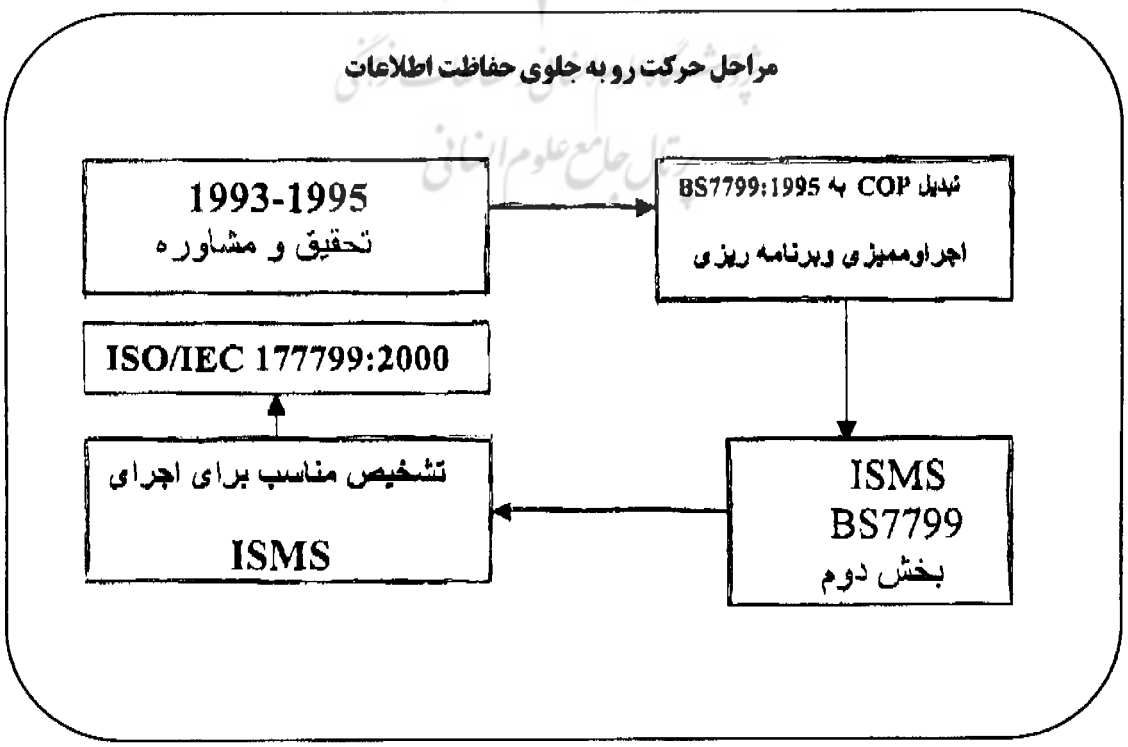
تا سال ۱۹۹۰ اطلاعات به حالت عمومی در سازمان‌ها استفاده می‌شد در دوره‌ای از زمان که نیاز بیشتری به تقسیم اطلاعات وجود داشت هیچ تضمینی برای ایمنی اطلاعات وجود نداشت و کنترل عموماً روی اطلاعات کامپیوتری بود و نه روی بقیه فرم‌های اطلاعاتی. در سال ۱۹۹۳ شرکت DTL با همکاری شرکت‌ها و سازمانهای مدیریتی انگلستان آیین‌نامه‌ای با موضوع حفاظت اطلاعات برای استفاده عموم تهیه کرد که تمام اطلاعات در زمینه داده‌های کامپیوتری، نوشته‌های مکتوب، اطلاعات گفتاری و انواع دیگر اطلاعات را شامل می‌شد که این آیین‌نامه اصول مشترک برای سازمان‌ها به منظور توسعه و سنجش کاربردی مدیریت حفاظت اطلاعات موثر و اطمینان در ارتباطات داخل سازمانی را فراهم می‌نمود.

سه مولفه کلیدی جهت فراهم کردن تضمین حفاظت اطلاعات عبارت است از: اطمینان داشتن، صحت، قابل دسترس بودن، به این منظور که اطلاعات فقط در دسترس افراد ذیصلاح باشد و نیز ایمنی و صحت کامل از اطلاعات و روشهای فرایند و تضمین آن که فقط کاربران اصلح امکان و قابلیت دسترسی به اطلاعات و سرمایه‌های مربوطه را دارا باشند.

با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵ نگرش سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. براساس این نگرش تامین امنیت فضای تبادل اطلاعات سازمان‌ها دفعتاً مقدور نمی‌باشد و لازم است این امر به صورت مداوم در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح انجام گیرد برای این منظور لازم است هر سازمان براساس یک متدولوژی مشخص اقدامات زیر را انجام دهد:

۱- تهیه طرح‌ها و برنامه امنیتی موردنیاز سازمان

۲- ایجاد تشکیلات موردنیاز جهت



ایجاد و تداوم امنیت فضای تبادل اطلاعات سازمان

۳- اجرای طرح‌ها و برنامه‌های امنیتی مورد اشاره در قسمت اول

در حال حاضر مجموعه‌ای از استانداردهای مدیریتی و فنی ایمن‌سازی فضای تبادل اطلاعات سازمان‌ها ارائه شده‌اند که استاندارد مدیریتی BSVV۹۹ استاندارد انگلیس، استاندارد مدیریتی ISO/IED۱VV۹۹ موسسه بین استانداردها و راهنماهای فنی در این‌زمینه محسوب می‌گردند.

در این استانداردها نکات زیر مورد توجه قرار گرفته است:

الف- تعیین و تبیین مراحل ایمن‌سازی و چگونگی نحوه شکل‌گیری چرخه امنیت اطلاعات و ارتباطات سازمانها

ب- تشخیص جزییات مراحل ایمن‌سازی و تکنیکهای فنی مورد استفاده در هر مرحله از عملکرد چرخه مذکور

پ - ارائه لیست و محتوی طرحها و برنامه‌های امنیتی موردنیاز سازمان

ج- ضرورت و جزییات ایجاد تشکیلات سیاستگذاری و اجرایی فنی تامین اطلاعات و ارتباطات درون و برون سازمانی

ح - کنترلهای امنیتی موردنیاز برای هر یک از سیستم‌های اطلاعاتی و ارتباطی

معرفی استاندارد امنیت اطلاعات

استاندارد BSVV۹۹ موسسه استاندارد انگلیس: استانداردی است برای اجرای الزاماتی برای سیستم مدیریت حفاظت اطلاعات در تشخیص، اداره نمودن و حداقل کردن خطراتی که اطلاعات سازمان را تهدید می‌کند. استاندارد BSVV۹۹ اولین استاندارد مدیریت امنیت اطلاعات است که نسخه اول آن تحت عنوان (BSVV۹۹I) در سال ۱۹۹۵ توسط اداره بازرگانی و صنعتی در انگلستان منتشر گردید و تجدید چاپ به عنوان سری اول از آن در ماه فوریه ۱۹۹۵ صورت پذیرفت که به دلیل نداشتن انعطاف‌پذیری و دارای نگرشی ساده و موجود بودن انتشارات دیگری در این زمینه نظیر (emu, y2K...) فراگیر نشد. نسخه دوم تحت عنوان BSVV۹۹II در ماه MAY سال ۱۹۹۹ با قابلیت برقراری و طرح اعتباری به صورت همزمان در یکسال، پدیداری ابزار پشتیبانی، آغاز پیگیری مقدمات استاندارد توسط سازمان ISO منتشر شد و آخرین نسخه این استاندارد در سال ۲۰۰۲ و در دو بخش تحت عنوان BSVV۹۹۲۰۰۲ منتشر گردید.

مزایای استفاده از BSVV۹۹:

- دارای ساختاری خوب و مناسب برای شروع
- صنعت گسترده و قابل فهم
- امکان دریافت گواهینامه
- تامین کردن اصول عمومی برای مدیریت حفاظت اطلاعات در سازمان
- فراهم نمودن اطمینان نسبی در شبکه داخلی خرید و فروش

نقاط ضعف

- داشتن تناقض و ناسازگاری در سطوح رده پایین و جزیی سازمان
- امکان حذف و از قلم افتادن محدوده‌هایی که حاوی اطلاعات می‌باشند.

مشخصه‌های کنترلی BSVV۹۹

ده مشخصه که در هر مجموعه کنترلی امنیتی موردنیاز سیستم‌های اطلاعاتی و ارتباطی هر سازمان باید وجود داشته باشد:

۱- تدوین سیاست امنیتی سازمان به منظور تعیین و تبیین خط‌مشی حفاظت اطلاعات:

فراهم کردن مسیر مدیریت و پشتیبانی در مورد حفاظت اطلاعات به ضرورت تدوین و انتشار سیاستهای امنیتی به نحوی که کلیه مخاطبین این سیاستها در جریان جزییات آن قرار گیرند تاکید شده است.

۲- ایجاد تشکیلات تامین امنیت سازمان به منظور سازماندهی داراییها و منابع: تشریح ضرورت ایجاد و جزئیات تشکیلات در سطوح سیاستگذاری اجرایی و فنی به همراه مسؤولیت‌های هر یک از سطوح ارائه شده است تا به کمک آن در مدیریت حفاظت اطلاعات در داخل سازمان سامان بخشید.

۳- دسته‌بندی و کنترل دارایی و سرمایه: نیاز و نحوه دسته‌بندی اطلاعات سازمان و محورهای طبقه‌بندی جهت کمک به تشخیص داراییها و حفاظت از آنها مدنظر می‌باشد.

۴- حفاظت و امنیت پرسنلی: منظور نمودن ملاحظات امنیتی در بکارگیری پرسنل، ضرورت آموزش پرسنل در زمینه اطلاعات و ارتباط جهت کاهش ریسکهای خطاهای پرسنلی، دزدی، کلاهبرداری، بد رفتاری و غیره مورد بررسی قرار می‌گیرد.

۵- حفاظت محیطی و فیزیکی: جهت جلوگیری از دسترسی و دخالت افرادی که صلاحیت ندارند، خرابی و خسارت وارده به اطلاعات سازمان اهمیت و ابعاد امنیت فیزیکی و جزئیات محافظت از تجهیزات و کنترلهای موردنیاز برای این منظور ارائه شده است.

۶- مدیریت عملیات و ارتباطات: برای تضمین صحت و اجرای عملیات برای تسهیل در فرایندهای اطلاعاتی ضرورت و جزئیات روال‌های اجرایی موردنیاز جهت تعیین و تبیین مسؤولیت هر یک از پرسنل، روال‌های مربوط به سفارش، خرید، تست و آموزش سیستم‌ها، محافظت در مقابل نرم‌افزارهای مخرب و ویروس‌های کامپیوتری، اقدامات موردنیاز درخصوص ثبت وقایع و پشتیبان‌گیری از اطلاعات، مدیریت شبکه، محافظت از رسانه‌ها و روال‌ها و مسؤولیت‌های مربوط به درخواست، تحویل و تست سایر موارد تغییر نرم‌افزار ارائه شده است.

۷- کنترل دسترسی و دستیابی به اطلاعات: نیازمندی‌های کنترل دسترسی، نحوه مدیریت دسترسی پرسنلی، مسؤولیت کاربران، ابزارها و مکانیزم‌های

کنترل دسترسی به شبکه، کنترل دسترسی در سیستم‌های عامل و کلیه نرم‌افزارهای کاربردی، استفاده از سیستم‌های مانیتورینگ و کنترل دسترسی در ارتباط از راه دور شبکه مورد توجه می‌باشد تاسطح دسترسی افراد به اطلاعات قابل کنترل شود.

۸- توسعه و نگهداری سیستم‌ها: تعیین نیازمندی‌های امنیتی سیستم‌ها، امنیت در سیستم‌های کاربردی، کنترل‌های رمزنگاری، محافظت از فایل‌های سیستم و محافظت و ملاحظات امنیتی موردنیاز در توسعه و پشتیبانی سیستم به منظور بیان آنکه حفاظت اطلاعات سیستمی می‌باشد.

۹- مدیریت تداوم فعالیت سازمان: رویه‌های مدیریت تداوم فعالیت، نقش تحلیل ضربه در تداوم فعالیت، طراحی و تدوین طرح‌های تداوم فعالیت، قالب پیشنهادی برای طرح تداوم فعالیت و تست آن با طرح‌ریزی مناسب، پشتیبانی و ارزیابی مجدد به منظور جلوگیری از به تعلیق درآمدن فعالیت‌ها و حفاظت از فرایندها در شکست و حوادث نابهنگام و غیرمنتظره مخرب.

۱۰- تطابق و پاسخگویی به نیازهای امنیتی: در این قسمت مقررات مورد نیاز درخصوص پاسخگویی به نیازهای امنیتی و سیاستگذاری‌های مرتبط درخصوص ابزارها و مکانیزم‌های بازرسی امنیتی سیستم‌ها به منظورجلوگیری از نقص در هر کدام از قانون‌های مدنی، موارد قانونی قراردادها و الزامات استاندارد.

اطلاعات یک سرمایه ارزشمند برای سازمان است و احتیاج به حفاظت مناسب دارد. حفاظت اطلاعات ابزاری است برای حفاظت از تهدیدها به منظور استمرار در روند کار، حداقل نمودن خسارات و حداکثر کردن بازگشت سرمایه و ایجاد فرصت‌های شغلی مناسب و مرتبط

فاکتورهای کلیدی برای اجرای استاندارد BSVV۹۹

- تعریف خط‌مشی حفاظت
- تعیین دامنه کاربر ISMS
- ایجاد تعهد به ارزیابی ریسک
- مدیریت ریسک
- انتخاب اهداف کنترل و اجرای آن
- آماده نمودن آیین‌نامه‌ای قابل اجرا

نتایج استقرار استاندارد BSVV۹۹

- سنجش مقدار حفاظت از اطلاعات
- اجرای مجموعه کنترلها
- ایجاد روشی برای برقراری اهداف و دادن پیشنهاد برای بهبود
- تبیین بنیان و اساس برای استاندارد حفاظت اطلاعات داخلی
- رسیدن به اعتبار، صداقت و اطمینان بالا
- کاهش هزینه‌ها
- تطابق قوانین و مقررات

براساس آخرین آمارهای بین‌المللی تنها ۴۰ درصد از سازمانها از حملات صورت گرفته به سیستم‌های اطلاعاتی خود آگاه می‌شوند که متاسفانه از این میان تنها حدود ۴۰ درصد آنها برای مقابله اقدام می‌کنند.

استاندارد BSVV۹۹ معماری سازمانی تیم مدیریتی امنیت اطلاعات را با تکیه بر تدوین سیاستها و راهکارهای امنیتی و با مستندسازی داراییهای اطلاعاتی سازمان و تعیین ریسکهای موجود احتمالی تدوین نموده و کنترلهای موردنیاز را در سه لایه تکنولوژی شامل سیستم‌های امنیتی شبکه، سیستم‌های عامل سرورها، پایگاه داده و... و فرآیندهای سازمان و افراد شامل امنیت فیزیکی و اجرای آموزشهای لازم پیاده‌سازی می‌کند. ●