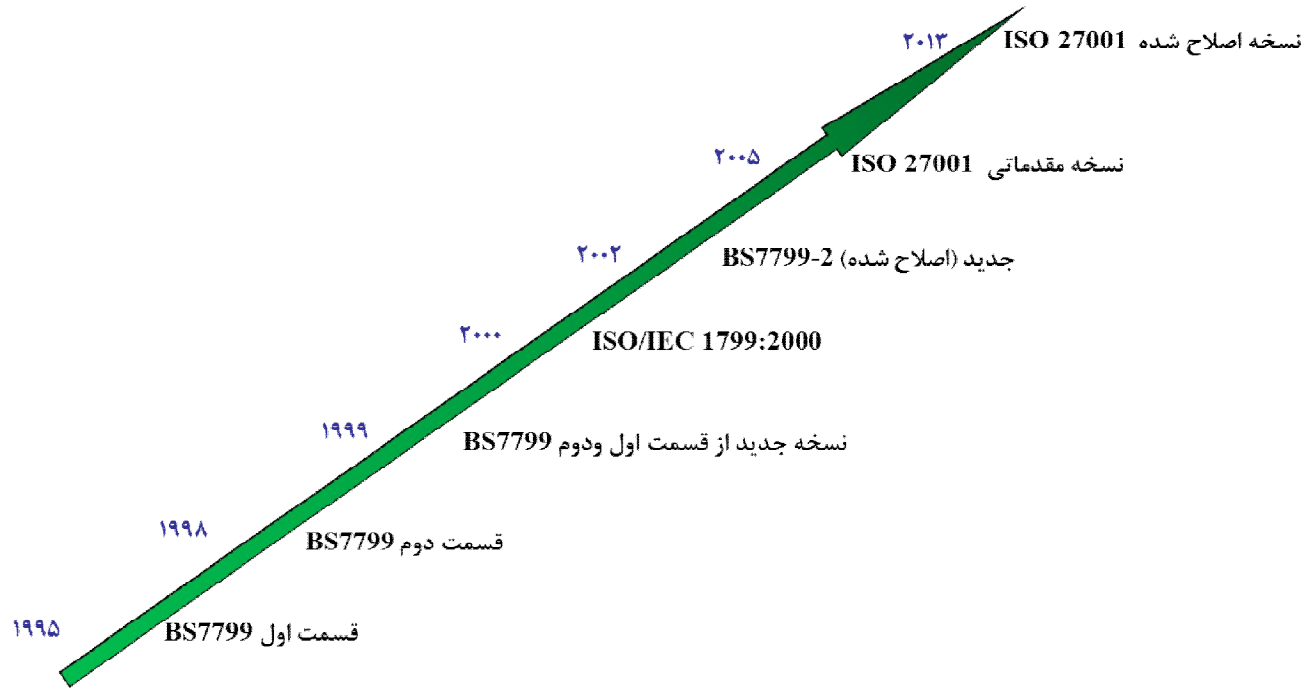
راهکاری بهینه در پیاده‌سازی سیستم مدیریت امنیت اطلاعات مبتنی بر ISO 27001:2013

محمدامین صابریان

بررسی رویه بهبود استانداردهای مدیریتی و رویکرد چارچوب‌هایی نظیر COBIT و ITIL بیانگر این حقیقت است که جهت‌گیری به سمت افزایش ارتباط استانداردهای مدیریتی با کسب و کار هر سازمان و افزایش سوددهی اقتصادی در کنار تسهیل اجرای امور و افزایش کیفیت و کارایی و دقت به واسطه مکانیزه شدن زیرساخت‌های بهره‌گیری از استانداردها است؛ این موضوع در نسخه جدید استاندارد ISO 27001:2013 به وضوح مشهود بوده و مهمترین علامت آن افزودن الزاماتی نظیر استخراج اهداف امنیتی منطبق با کسب و کار سازمان و نیز الزاماتی نظیر پایش و اندازه‌گیری اهداف امنیتی و مخاطرات است. شکل زیر نمایی از تاریخچه این استاندارد را نشان می‌دهد.



یکی از بهترین مدل‌ها در جهت محقق نمودن الزامات استاندارد ISO 27001:2013 و بهبود مستمر امنیت اطلاعات سازمان، استخراج اهداف امنیتی بر اساس ماموریت‌ها و چشم‌انداز سازمان هدف و ارائه داشبورد مدیریتی جهت ردیابی وضعیت اهداف امنیتی به‌صورت لحظه‌ای است. در داشبورد امنیتی که به‌صورت نمودارهای گرافیکی برای مدیر سازمان نمایش داده می‌شود، باید شاخص‌های مرتبط با هر نمودار که منطبق با هر هدف امنیتی است، از قبل استخراج و وزن‌دهی شده باشد و ارتباط drilldown بین هر نمودار و مخاطراتی که منجر به تعیین مسیر نمودار شده‌اند وجود داشته باشد، به‌طوری که مدیر سازمان در هر لحظه قادر به شناسایی دلایل بالا یا پایین رفتن مخاطرات سازمان خود باشد.

می‌توان داشبورد مدیریتی را مشابه آخرین نسخه چارچوب COBIT منطبق با چارچوب کارت امتیازدهی متوازن (BSC) طراحی کرد و منظرهایی نظیر رشد و یادگیری، فرایندهای داخلی، مشتری و در نهایت مسایل مالی را مدنظر داشت و مخاطرات را با توجه به آن شناسایی و پایش و اندازه‌گیری نمود.

در ادامه مهمترین تغییرات نسخه ISO 27001:2013 با نسخه قبلی منتشر شده در سال 2005 ارائه شده است:

- تغییر بندهای استاندارد و منطبق نمودن آن با سایر استانداردهای مدیریتی

- درخواست استفاده از یک متدولوژی بهبود مستمر امنیت اطلاعات و حذف الزام استفاده از چرخه دمینگ جهت بهبود مستمر
- الزام شناسایی زمینه‌های داخلی و خارجی فعالیت‌های سازمان شامل انواع استانداردها و روش‌های اجرای فعالیت‌ها، طرف‌های بیرونی مرتبط با سازمان و ...
- توسعه شناسایی نیازمندی‌های امنیتی ذی‌نفعان به شناسایی نیازمندی‌های امنیتی کلیه عامل‌های درونی و بیرونی (بخش‌های علاقه‌مند) سازمان که در فعالیت‌های سازمان نقش دارند.
- الزام شناسایی شفاف نیازمندی‌های امنیتی مرتبط با ارتباطات درونی و بیرونی سازمان
- الزام استخراج اهداف امنیتی منطبق با فعالیت‌های سازمان که در این راستا استخراج ماموریت، چشم‌انداز و فعالیت‌های سازمان در جهت تعیین سطح امن‌سازی و برنامه‌ریزی برخورد با مخاطرات بسیار موثر است.
- هدایت و رهبری سیستم مدیریت امنیت اطلاعات به صورت الزامی بر عهده مدیر ارشد سازمان گذاشته شده است.
- جایگزین شدن الزام تعیین مالک هر مخاطره به‌جای تعیین مالک هر دارایی، در این صورت مالک هر مخاطره مسئولیت برخورد با مخاطره را بر عهده خواهد داشت.
- پیامدها، مخاطرات و فرصت‌ها جایگزین اقدامات پیشگیرانه شده و اقدامات پیشگیرانه حذف شده است.
- بر خلاف نسخه قبلی استاندارد که کنترل‌ها از پیوست A استاندارد انتخاب و کاربردپذیری آنها بررسی می‌شد در نسخه جدید استاندارد کنترل‌های در طی فرایند ترمیم مخاطرات تعیین می‌شوند.
- قوی‌تر شدن الزامات مربوط به کارایی، پایش و اندازه‌گیری طرح ترمیم مخاطرات و سطح تحقق اهداف امنیتی
- افزایش اختیارات مرتبط با روش شناسایی مخاطرات و عدم اشاره به الزامات مرتبط با شناسایی تهدیدات و آسیب‌پذیری‌ها در استخراج مخاطرات
- افزایش تعداد حوزه‌های امنیتی مورد بررسی و کاهش مجموع تعداد کنترل‌های مربوط به هر حوزه
- جایگزین شدن اسناد اطلاعاتی به‌جای مستندات و سوابق

اسناد اطلاعاتی که استاندارد ISO 27001:2013 در متن خود، تهیه آنها را الزام نموده است عبارتند از:

- قلمرو سیستم مدیریت امنیت اطلاعات (بند 4.3)
- خط‌مشی امنیت اطلاعات (بند 5.2)
- فرایند ارزیابی مخاطرات امنیت اطلاعات (بند 6.1.2)
- فرایند ترمیم مخاطرات امنیت اطلاعات (بند 6.1.3)
- بیانیه قابلیت کاربرد (بند 6.1.3 d)
- اهداف امنیت اطلاعات (بند 6.2)
- مدارک صلاحیت (بند 7.2 d)
- اطلاعات مستند شده و تعریف شده توسط سازمان که لزوم اثربخشی ISMS را نشان می‌دهند. (بند 7.5.1 b)
- کنترل‌ها و طرح‌ریزی عملیاتی (بند 8.1)
- نتایج ارزیابی مخاطرات امنیت اطلاعات (بند 8.2)
- نتایج ترمیم مخاطرات امنیت اطلاعات (بند 8.3)
- مدارک مرتبط با نتایج پایش و اندازه‌گیری (بند 9.1)
- مدارک مرتبط با برنامه‌های ممیزی و نتایج ممیزی (بند 9.2 g)
- مدارک مرتبط با نتایج بازنگری مدیریت (بند 9.3)
- مدارک مرتبط با ماهیت عدم انطباق‌ها و فعالیت‌های مرتبط انجام شده (بند 10.1 f)
- مدارک مرتبط با نتایج اقدامات اصلاحی (بند 10.1 g)

سری استانداردهای 27000 شامل تعداد زیادی استاندارد و راهنما هستند که استاندارد اصلی آنها ISO 27001 است و این استاندارد به همراه ISO 27002 که به توصیف کنترل‌های پیوست A استاندارد ISO 27001 می‌پردازد، در سال 2013 به روز شده‌اند. استاندارد ISO 27002 به معرفی بهترین نمونه‌ها برای هر یک از کنترل‌های استاندارد می‌پردازد و مشاورین پیاده‌سازی ISO 27001 با مطالعه و بررسی آن می‌توانند مصادیق استفاده از هر یک از کنترل‌های استاندارد در طرح‌های ترمیم هر مخاطره را بررسی و استفاده کنند، البته اجباری به استفاده از آنها نیست. براساس متن استاندارد ISO 27001:2013 جهت آشنایی با اصلاحات و تعاریف به‌کار رفته در استاندارد، به آخرین نسخه از استاندارد ISO 27000 رجوع شود و به منظور آشنایی با زمینه فعالیت‌های درونی و بیرونی سازمان به بند 5.3 از استاندارد ISO 31000:2009 رجوع شود.

پیاده‌سازی سیستم مدیریت امنیت اطلاعات وابسته به زیرساخت‌های تکنولوژی، فرایندی، دانش پرسنلی و سطح هزینه‌ای است که سازمان حاضر به پذیرفتن آن است. مکانیزه کردن امور شناسایی، پایش، اندازه‌گیری مخاطرات و اهداف امنیتی و طرح‌های تداوم فعالیت‌های برخورد با حوادث، وابسته به زیرساخت‌های تکنولوژی سازمان هدف بوده و با توجه به آن هزینه‌های خاص خود را طلب می‌کند، با این وجود با توجه به رویکرد سازمان هدف می‌تون از نرم‌افزارهایی مشابه Excel در جهت مدیریت امور و کاهش هزینه‌ها استفاده نمود که این امر نیازمند بهره‌گیری از توان پرسنلی با توجه به خطمشی‌های سازمان هدف است.

مرکز تحقیقات صنایع انفورماتیک با تجربه‌ای بیش از 20 سال در زمینه انواع استانداردهای مدیریتی و فنی و به‌عنوان اولین شرکت در ایران که موفق به پیاده‌سازی سیستم مدیریت امنیت اطلاعات بر مبنای ISO 27001:2005 و اخذ گواهینامه بین‌المللی آن برای یکی از سازمان‌های بزرگ تحت قرارداد خود شده است و با پشتوانه بیش از 100 پرسنل متخصص و دارا بودن پروانه فعالیت از نظام ملی مدیریت امنیت اطلاعات (نما) به شماره 12416 آماده ارائه خدمات مشاوره در جهت پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سطوح مختلف سازمانی بوده و با دانش کامل نسبت به استاندارد ISO 27001:2013 و سایر استانداردها و چارچوب‌های استانداردسازی فناوری اطلاعات و تخصص بالا در زمینه طراحی و پیاده‌سازی شبکه، اجرای آزمون نفوذپذیری و نیز تخصص ارزیابی امنیت محصولات فناوری اطلاعات، آمادگی خود را در جهت پیاده‌سازی سیستم مدیریت امنیت اطلاعات مبتنی بر ISO 27001:2013 در انواع سازمان‌ها با انواع زیرساخت‌ها و توانمندی‌ها اعلام می‌دارد.