ارائه‌ی روش بهینه برای استقرار هم‌زمان نظام مدیریت خدمات فناوری اطلاعات و نظام مدیریت امنیت اطلاعات

محمدرضا گودرزی
مصطفی تمتاجی

تاریخ دریافت: ۹۴/۰۵/۰۴
تاریخ پذیرش: ۹۴/۰۶/۱۰

چکیده:

توسعه‌ی فناوری اطلاعات در سازمان‌ها، علی‌رغم مزایای متعدد و غیرقابل انکار، بحث‌های زیادی را نیز به‌دنبال داشته است. ارائه‌ی خدمات فناوری اطلاعات با کیفیت مطلوب و در بستر امن از جمله دغدغه‌های اساسی در ارائه‌ی این نوع خدمات به بخش‌های درون‌سازمانی و برون‌سازمانی است. استانداردهای مدیریت خدمات فناوری اطلاعات و مدیریت امنیت اطلاعات برای رفع این دغدغه توسعه یافته‌اند.

لزوم استقرار این دو استاندارد در سازمان، به‌منظور تضمین کیفیت خدمات و امنیت اطلاعات، موضوع بعدی این مسیر است. در این مقاله، ابتدا مفاهیم و اصول این دو نظام بیان‌شده، سپس چارچوبی برای استقرار هم‌زمان آن‌ها ارائه‌شده است. چارچوب ارائه‌شده از نظر عملیاتی‌بودن مورد تأیید خبرگان قرارگرفته و از نظر جامعیت با محتوای استانداردها، نگاشته‌شده است.

این چارچوب مسیری کارا و اثربخش برای استقرار این دو نظام ارائه‌کرده است و موجب هزینه‌کردن هدفمند منابع در سازمان خواهد شد.

واژگان کلیدی:

فناوری اطلاعات، امنیت اطلاعات، نظام مدیریت خدمت[1]

۱. مقدمه

در فضای پرتلاطم کنونی برای سازمان‌های تجاری و خدماتی مختلف در دنیا، حفاظت از سرمایه‌های اطلاعاتی همانند اطلاعات مالی، سرمایه‌گذاری و پرسنلی و... با جنجال‌های جدی و پرهزینه مواجه است. وابستگی هرچه بیشتر زندگی و کسب‌وکار به فناوری‌های جدید از یکسو وگسترش مسائل، مشکلات و ناامنی‌ها در بهره‌گیری از فناوری از سوی دیگر نقش امنیت اطلاعات را بیش از پیش ضروری ساخته است. از آنجا که این امر کاری سخت و پرهزینه جهت دولت‌ها، سازمان‌ها و شرکت‌هاست، همواره شاهد اعلام سرقت و تخریب اطلاعات از سوی شرکت‌های ناظر و تولیدکنندگان نرم‌افزار امنیت شبکه از سوی هکرهای بین‌المللی رایانه‌ای هستیم. یکی از موانع عمده، تهدیدات امنیتی شایع ناشی از ICT[2] ، وقوع جدی این تهدیدات به‌شکل حملات اطلاعاتی و جنگ اطلاعات است، ازاین‌رو می‌توان گفت مرزهای جغرافیایی و خط مقدم جبهه مفهوم خود را از دست‌داده و سامانه‌ها و شبکه‌های حیاتی کشورها نظیر شبکه‌های نظامی، مخابراتی، آب، برق، گاز، شبکه‌های بانکی و تجاری دچار خدشه وآسیب‌های شدید می‌شوند.[۱]

امروزه با توجه به وابستگی سازمان‌ها به اطلاعات و سیستم‌های مربوط به آن، با تهدیدهای مربوط به اطلاعات و سیستم نیز مواجه هستند که روزبه‌روز پیچیده‌تر می‌شود. به‌دنبال این موضوع، امنیت اطلاعات برای سازمان، نیاز و یک ضرورت است. از طرفی رشد چشمگیر ICT در اواخر قرن بیستم و ظهور عصر دانایی و اطلاعات در قرن حاضر، لزوم توسعه و به‌کارگیری فناوری اطلاعات و ارتباطات (تکفا)[3] درسطح کشور و نیز در حوزه‌ی دفاعی(تکفاد)[4] میهن اسلامی با عنایت به نقش و تأثیرگذاری آن برسامانه‌های C4I[5] به‌نحو بارزی احساس می‌شود. بنابراین، لازم است علاوه بر توسعه وکاربردی‌کردن به تسلط‌یافتن بر فناوری اطلاعات و ارتباطات به‌ویژه در حوزه‌ی دفاعی پرداخته شود. بنابراین، در این مقاله

1. Service Management System (SMS)
2. Information Communication Technology

۳. توسعه‌ی کاربردی فناوری اطلاعات
۴. توسعه‌ی کاربردی فناوری اطلاعات دفاعی

5. Command-Communication-Computer-Control-Integrity

ضمن بررسی اجمالی و مروری بر استانداردهای نظام مدیریت خدمات فناوری اطلاعات و نظام مدیریت امنیت اطلاعات[1]، به موضوع استقرار هم‌زمان آن‌ها در سازمان‌های دفاعی و چارچوب مناسب برای آن پرداخته‌خواهد شد.

۲) نظام مدیریت خدمات فناوری اطلاعات

در سه دهه‌ی اخیر فعالیت‌های بسیاری درزمینه‌ی مدیریت سرویس‌های IT در دنیا صورت‌گرفته و روش‌ها و توصیه‌های گوناگونی ارائه‌شده است. اصلی‌ترین بحران شرکت‌ها و سازمان‌های سرویس‌دهنده‌ی خدمات فناوری اطلاعات، صرف کمترین هزینه‌ی ممکن و ارائه‌ی بهترین کیفیت است. در اختیار داشتن فناوری پیشرفته و نیروی انسانی متخصص به‌تنهایی کارگشا نبوده و مسئله‌ی بسیار مهمی به‌نام روال‌های مدیریت خدمات مطرح می‌شودکه درواقع حلقه‌ی مرتبط‌کننده‌ی فناوری و افراد است.

به‌منظور مدیریت کارآمد فناوری اطلاعات از حدود دهه‌ی ۸۰ میلادی، اداره‌ی کامپیوتر دولت انگلستان چارچوبی را تحت عنوان ITIL[2] "کتابخانه‌ی زیرساخت فناوری اطلاعات" ابداع کرد. این چارچوب مجموعه‌ای مدون از "بهترین تجارب و کارکردها"[3] از طیف وسیعی از شرکت‌ها، سازمان‌ها و افراد خبره درزمینه‌ی فناوری اطلاعات است. این چارچوب شامل مجموعه‌ای از فرایندها و رویه‌ها در سه سطح راهبردی، تاکتیکی و عملیاتی در یک سازمان فناوری اطلاعات است که براساس تجارب به اثبات‌رسیده، می‌تواند خدمات فناوری اطلاعات را در سازمان به‌نحو کارآمدی تأمین و پشتیبانی کند. درواقع ITIL ساختاری فرایندگرا[4] را جایگزین رویکرد سنتی وظیفه‌گرا[5] کرده است.

پیاده‌سازی این چارچوب منجر به افزایش شفافیت سازمانی، بهبود خدمات فاوا، بهینه‌سازی استفاده از منابع، بهینه‌سازی هزینه‌ها، توسعه‌پذیری سازمان، افزایش کیفیت خدمات فاوا و بالاخره انطباق با استاندارد ISO/IEC 20000 (استاندارد سازمانی مدیریت خدمات IT) خواهد شد. خانواده‌ی استانداردهای سری ISO/IEC 20000 مجموعه الزامات و راهنمایی‌هایی برای ارائه‌ی خدمات فناوری اطلاعات ارائه می‌کند که در قالب چارچوب ITIL قابل پیاده‌سازی هستند. برخی از ویژگی‌های کلیدی ISO/IEC 20000 که آن را از سایر استانداردها متمایز و اجرایی‌تر می‌سازد، عبارت‌است از:

- چارچوب مبتنی بر بهترین تجربه‌ها و کارکردها،
- دیدگاه فرایندگرا در مقابل دیدگاه وظیفه‌گرا،
- اجتناب از دیوان سالاری در فرایندها،
- امکان پیاده‌سازی فرایندها به‌صورت تدریجی،
- حاکم‌بودن اصل بهبود مستمر در توسعه‌ی فرایندها،
- تمرکز بر رضایت مشتریان خدمات.

۳) استاندارد برای چارچوب ITIL

در سازمان‌ها و شرکت‌های امروزی وقوع نقص، حادثه و نیز عدم برنامه‌ریزی مناسب در ارائه‌ی خدمات فناوری اطلاعات به‌راحتی به فرایندهای کسب‌وکار و در نتیجه اعتبار سازمان لطمه وارد می‌کند. با پیچیده‌ترشدن خدمات فناوری اطلاعات نیاز سازمان‌ها به روش‌هایی که سطح کیفیت خدمات فناوری اطلاعات را در حد مناسبی نگهداری و آن را ارتقا بخشد، روزبه‌روز بیشتر می‌شود. استفاده از استانداردها و روش‌های مناسب درزمینه‌ی ارائه‌ی خدمات فناوری اطلاعات امری اجتناب‌ناپذیر به‌نظر می‌رسد. در دو دهه‌ی گذشته، چارچوب ITIL یکی از پرکاربردترین روش‌ها در پیاده‌سازی مدیریت خدمات فناوری اطلاعات با محوریت کسب‌وکار بوده است. تعداد محصولات نرم‌افزاری که از این چارچوب پشتیبانی می‌کنند روزبه‌روز درحال افزایش است. پس از مقبولیت روزافزون ITIL، سازمان استاندارد جهانی[6]، استاندارد ISO/IEC 20000 را جهت ارائه‌ی گواهی‌نامه‌ای معتبر در زمینه‌ی مدیریت خدمات فناوری اطلاعات به سازمان‌ها ارائه کرد. این استاندارد، در سال ۲۰۰۵ توسط ISO/IEC JTC1 SC7 تدوین و در سال ۲۰۱۱ مورد بازبینی قرارگرفته است. این استاندارد براساس استاندارد BS 15000 که قبلاً توسط شرکت BSI ایجادشده بود، تدوین‌شده است.

بخش اول این استاندارد، ISO/IEC 20000 -1، با درنظر گرفتن رویکرد فرایند محوری، تلاش می‌کند تا خدمات را به‌صورت مؤثر و مدیریت‌شده‌ای ارائه دهد تا تمامی اهداف کسب‌وکار را در ارتباط با نیازهای

1. Information Security Management System-ISMS
2. IT Infrastructure Library
3. Best Practice
4. Process Oriented
5. Function Oriented
6. International Standards Organization(ISO)

مشتری پوشش دهد.

از مزایای استاندارد ISO/ IEC 20000 می‌توان به موارد زیر اشاره کرد: [۳]

- تخصصی‌بودن برای صنعت فناوری اطلاعات،
- دارای خطوط راهنما برای استقرار، الزامات سامانه‌ی مدیریت کیفیت،
- توجه ویژه به خدمات پس از فروش نرم‌افزار و سخت‌افزار،
- توجه به بودجه‌بندی و کنترل هزینه‌ها در فناوری اطلاعات و نرم‌افزار،
- کنترل مناسب در مراحل مختلف، طراحی، تولید، تحویل و خدمات پس از فروش فناوری اطلاعات و نرم‌افزار،
- امکان‌سنجی مناسب و تخصصی در صنعت،
- مدیریت مناسب تغییرات در فناوری اطلاعات،
- کنترل کیفیت نرم‌افزار و فناوری اطلاعات.

۴) مرور کلی نظام مدیریت امنیت اطلاعات (ISMS)

می‌توان ISMS را رویکرد ساختاریافته‌ای دانست که چگونگی پیاده‌سازی امنیت اطلاعات را در یک سازمان مشخص می‌کند. به‌عبارتی با استفاده از فرایند مدیریتی به سمت بهبود مداوم در سازمان حرکت می‌کند. مجموعه‌ی ISO/IEC 27000 که تحت عنوان خانواده‌ی استاندارد ISMS شناخته‌شده است، شامل استانداردهای امنیت اطلاعات است که به‌طور مشترک توسط سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون علوم الکترونیکی بین‌المللی (IEC) منتشرشده است.

این استانداردها محصول ISO/IEC JTC1، SC27 (زیر کمیته ۲۷) و یک نهاد بین‌المللی است که در سال دوبار جلسه برگزار می‌کنند. درحال حاضر، ۴۴ استاندارد از این مجموعه منتشرشده و قابل دسترس است. این در حالی است که تعداد بیشتری نیز در حال توسعه و آماده‌سازی است. [۴]

سیستم مدیریت امنیت اطلاعات (ISMS) با ارائه‌ی اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش سیستماتیک به مقوله‌ی ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. این مجموعه بهترین توصیه‌ها را بر پایه‌ی تجربیات عملی در مدیریت امنیت اطلاعات، مواجه با مخاطره و کنترل را در تمامی ابعاد سیستم مدیریت امنیت اطلاعات(ISMS) بیان می‌کند. این استاندارد قابلیت اعمال به تمام سازمان با اندازه‌ها و اشکال مختلف را داراست. با توجه به ماهیت پویای امنیت اطلاعات، ISMS روش‌های بازخورد و بهبود مستمر را "طرح‌ریزی، اجرا، پایش و بهبود"[1] به‌کار می‌برد، که تغییرات در تهدید، آسیب‌پذیری و یا اثرات حوادث امنیت اطلاعات را هدف می‌گیرد. از جمله مزایای به‌کارگیری سیستم ISMS می‌توان به مواردی مانند بالارفتن اثرپذیری امنیت اطلاعات، تقویت مشتری محوری، استفاده از استاندارد جهانی، کاربری امنیت اطلاعات، مشخص‌شدن اهمیت اجرای قوانین اشاره کرد.

۵) لزوم به‌کارگیری بندهای ISMS در استقرار ISO/IEC 20000

سازمان‌ها به‌صورت فزاینده‌ای اطلاعات حساسشان را با استفاده از سامانه‌های نرم‌افزاری که به‌صورت مستقیم به اینترنت متصل هستند، ذخیره، پردازش و منتقل می‌کنند. تراکنش‌های محرمانه‌ی مالی شهروندان از طریق اینترنت به‌واسطه‌ی نرم‌افزارهای فروشگاهی، بانکی، پرداخت مالیات و عوارض‌ها، خرید بیمه و سهام، ثبت نام در مدرسه و دانشگاه و نیز با عضویت در شبکه‌ی سازمان‌ها و شبکه‌های اجتماعی مختلف، فاش می‌شوند. افشایی که به واسطه‌ی ارتباط جهانی درحال گسترش است، اطلاعات حساس و سامانه‌های نرم‌افزاری که این‌گونه اطلاعات را مدیریت می‌کنند، در کاربردهای بدخواهانه و غیرمجاز بسیار آسیب‌پذیر می‌کنند. به‌طورکلی سامانه‌های نرم‌افزاری و سایر امکاناتی که به‌واسطه‌ی نرم‌افزار فراهم شده‌اند، بیش از پیش منجر به دسترسی به اطلاعات حساس (شامل شناسه‌های فردی) به‌صورت باز و گسترده شده‌اند. مثال‌های فوق نمونه‌هایی از ارائه‌ی خدماتی است که نیاز به امنیت داشته و ضرورت ادغام ارائه‌ی خدمات رایانه‌ای در بستری امن به مشتریان را نیاز دارد .لیکن استفاده‌ی همزمان از دو

1. Plan-Do – Check - Action

استاندارد، مزایا و معایبی را در پی خواهد داشت.
انتشار استاندارد ISO/IEC 27013 برگرفته ازترکیب استفاده از دو استاندارد بین‌المللی است که مزایای بیشتری را به ارمغان می‌آورد.
استاندارد ISO/IEC 27013 در اولین گام برای سازمان‌هایی که مایل به افزایش کارایی، بهبود خدمات، مدیریت خدمات و امنیت اطلاعات هستند، دستورالعمل ارائه می‌دهند. اجرای استانداردها کمک می‌کند تا تولیدکنندگان اعتبار خود را نزد مشتریان و ذی‌نفعان ثابت کنند و تعهد خود را به حفظ توسعه‌ی پایدار نشان دهند. امروزه سازمان‌ها و شرکت‌ها در هر اندازه و منطقه‌ی جغرافیایی که قرارداشته باشند، با اجرای استانداردها می‌توانند از مزایای اجتماعی و اقتصادی برخوردار شوند. مزایای مهم اجرای یکپارچه عبارت است از: [۲]

- کسب اعتبار برای خدمات کارآمد و مطمئن در مشتریان داخلی و خارجی سازمان،
- کاهش هزینه‌های برنامه‌ی یکپارچه،
- کاهش زمان اجرای لازم برای تدوین یکپارچه‌ی فرایندهای مشترک هر دو استاندارد،
- ترویج درک بین مدیریت خدمات و امنیت کارکنان،
- بهبود فرایند صدور گواهی.

۶) مشکلات ادغام استانداردها

وقتی‌که به‌طور هم‌زمان با دو استاندارد سروکار داریم، بهتر است درک شود که آن‌ها در بیش از یک جهت دارای ویژگی‌های متفاوت هستند. برای مثال محدوده و اهداف متفاوتی دارند [۳ و ۴]. تفاوت در محدوده می‌تواند باعث شود برخی خدمات که درSMS وجود دارند در ISMS مستثنا شوند. به همان اندازه SMS می‌تواند فرایندها و کارکردهای ISMS را مستثنا کند. برای مثال برخی از سازمان‌ها تصمیم می‌گیرند یک ISMS را تنها در توابع عملیاتی و ارتباطی خود پیاده‌سازی کنند، درحالی‌که SMS آن‌ها، مدیریت خدمات کاربرد را شامل می‌شود. به‌طور متناوب ISMS می‌تواند همه‌ی خدمات را پوشش دهد، درحالی‌که SMS تنها خدمات برای مشتریان ویژه و ذی‌نفعان را پوشش می‌دهد. توصیه می‌شود؛ سازمان حوزه‌های کاربرد استانداردها را تا حد امکان تنظیم کند تا اطمینان حاصل شود که سامانه‌ی مدیریت می‌تواند با موفقیت یکپارچه شود. مواردی که باید در طرح‌ریزی برای پیاده‌سازی سامانه‌ی یکپارچه مورد نظر قرار گیرند به قرار زیر است: [۲]

- سایر سامانه‌های مدیریتی که درحال استفاده هستند،
- همه‌ی خدمات و فرایندها و وابستگی آن‌ها در مفهوم سامانه‌ی مدیریت یکپارچه،
- عناصر هر استانداردکه می‌توانند ادغام شوند،
- عناصری که باید جدا بمانند،
- تأثیر سامانه‌ی مدیریت یکپارچه روی مشتری و سایر ذی‌نفعان،
- تأثیر بر فناوری در حال استفاده،
- تأثیر و یا مخاطره بر خدمات و مدیریت خدمت،
- تأثیر و یا مخاطره بر مدیریت امنیت اطلاعات،
- گام‌ها و توالی فعالیت‌های پیاده‌سازی.

۶-۱) هم‌پوشانی‌های دو استاندارد (تشابهات)

مدیریت خدمت و مدیریت امنیت اطلاعات به‌وضوح فرایندها و فعالیت‌های بسیار مشابهی دارند، مگر آنکه یکی از سامانه‌های مدیریتی برخی جزئیات را بیشتر از دیگری برجسته‌کرده باشد. در این خصوص می‌توان به نقاط مشترک زیر اشاره کرد:

- استفاده از چرخه‌ی طرح اجرای بررسی اقدام،
- مدیریت سطح خدمت و گزارش‌گیری،
- تعهد مدیریتی،
- مدیریت ظرفیت،
- مدیریت مخاطرات طرف سوم،
- مدیریت تداوم و قابلیت دسترسی،
- مدیریت پیکربندی،
- بودجه‌بندی و حسابداری.

۶-۲) مقایسه در سطح بندهای دو استاندارد (تفاوت‌ها)

مدیریت خدمت و مدیریت امنیت اطلاعات به‌طورمعمول به‌گونه‌ای تلقی می‌شوند که نه متصل و نه وابسته هستند. برخی از تفاوت‌های این دو استاندارد به‌شرح زیر است:

- مدیریت رخداد و مشکل،
- کاربرد و منظور دارایی،
- طراحی و انتقال خدمت،
- مدیریت و ارزیابی مخاطرات،
- تفاوت‌ها در سطوح پذیرش مخاطره،
- مدیریت تغییر.

۷) روش بهینه‌ی استقرار هم‌زمان استانداردهای مدیریت خدمات فناوری اطلاعات و مدیریت امنیت اطلاعات

استاندارد ISO/IEC 20000-1 ، در ارتباط با ویژگی‌هایی برای طراحی، انتقال، تحویل و بهبود خدمات برای برآوردن الزامات است. این هدف از طریق مجموعه‌ای از فرایندها حاصل‌شده و محدوده‌ی آن، شامل فرایندهای مدیریتی درون سازمان و خدمات، است. استانداردISO/IEC 27001 ، در ارتباط با چگونگی مدیریت مخاطرات امنیت اطلاعات بوده و محدوده‌ی آن، قسمت‌هایی از فعالیت‌های سازمان متقاضی است که تمایل دارند، امن باشند. بنابراین، محدوده‌ی هر دو استاندارد متفاوت معنا می‌شوند. درنتیجه پیاده‌سازی استانداردISO/IEC27001 برای محدوده‌ی مشابه استاندارد ISO/IEC 20000-1 قابل اجراست اما استاندارد ISO/IEC 20000-1 ، نمی‌تواند برکل سازمان اعمال شود مگر برای سازمان‌هایی که کاملاً فراهم‌کننده‌ی خدمت باشند.

سازمانی که درحال طرح‌ریزی برای پیاده‌سازی استانداردISO/IEC 27001 و استانداردISO/IEC 20000-1 است، می‌تواند یکی از سه حالت زیر را داشته باشد.

۷-۱) سازمان دارای ISO/IEC 20000

با توجه به اینکه مدیریت خدمت می‌تواند به‌سادگی به کارایی و سودآوری مربوط شود، در اکثر مواقع مدیریت خدمت در ابتدا پیاده‌سازی‌شده است. ولی مدیریت امنیت اطلاعات در ظاهر، سودآور نبوده، بنابراین، در اغلب موارد ISO/IEC 27000 به‌عنوان پایه‌ای برای تحویل خدمت مؤثر درک نمی‌شود. این مورد مبتلابه اکثر شرکت‌ها بوده و طیف وسیعی از سازمان‌ها را شامل می‌شود. در ادامه به توضیح بیشتر در مورد گام‌های اجرایی آن می‌پردازیم:

گام اول: ارزیابی وضع موجود

هدف از این گام شناخت کامل وضع موجود و همچنین برنامه‌ریزی جهت رسیدن به وضع مطلوب است. در این گام، وضعیت فعلی خدمات فناوری اطلاعات در سازمان به‌طور دقیق مورد ارزیابی قرارگرفته و فهرست خدمات اختصاصی پس از تحلیل و بررسی میزان فاصله بین وضع موجود و استانداردهای پیشنهادی ISO/IEC 27000 مشخص خواهد شد.

گام دوم: اصلاح فرایندهای موجود

در این مرحله، مطالعاتی روی چارچوب ISO/IEC 20000 پیاده‌سازی و انجام‌شده و تمامی فرایندهای جاری آن که به سه گروه (مدیریتی، عملیاتی، پشتیبانی) تقسیم‌بندی و درصورت ضرورت فرایند پشتیبانی به دو گروه عمده‌ی تحویل خدمات و پشتیبانی خدمات تقسیم می‌شوند. توصیه می‌شود، فرایندهای پشتیبانی خدمات که شامل فرایندهایی همانند مدیریت درخواست‌ها، مدیریت دارایی‌ها یا پیکربندی و مدیریت تغییرات، مورد بررسی بیشتر قرارگرفته و با فرایندها و فعالیت‌های ISO/IEC 27000 مورد مطابقت قرار گیرند. این خروجی‌ها به‌صورت مستندات و جلسات آموزشی متعددی تهیه‌شده و مقدمه‌ی تحلیل و طراحی سیستم ISO/IEC 27000 خواهند بود.

یکی از موارد مهم در تدوین فرایندهای ITIL تهیه و اطلاع‌رسانی فهرستی از خدمات قابل ارائه توسط تیم فناوری اطلاعات است. ارائه‌ی این سرویس یکی از نیازمندی‌های مهم فرایندهاست که به شفاف‌سازی نقش‌های سازمانی، شرح وظایف و نیز تدوین سطوح خدمات و انتظاراتی که کاربران سرویس‌های فناوری اطلاعات سازمان دارند، بسیار کمک می‌کند. در این مورد از بندهای شرایط خصوصی ISO/IEC 27000 استفاده خواهد شد.

گام سوم: طراحی و استقرار فرایندهای ISO/IEC 27000

این مرحله شامل طراحی تک‌تک فرایندها، پیاده‌سازی گام‌به‌گام ISO/IEC 27000 و همچنین سنجش روند پیشرفت فرایندهای چارچوب ITIL را معرفی می‌کند.

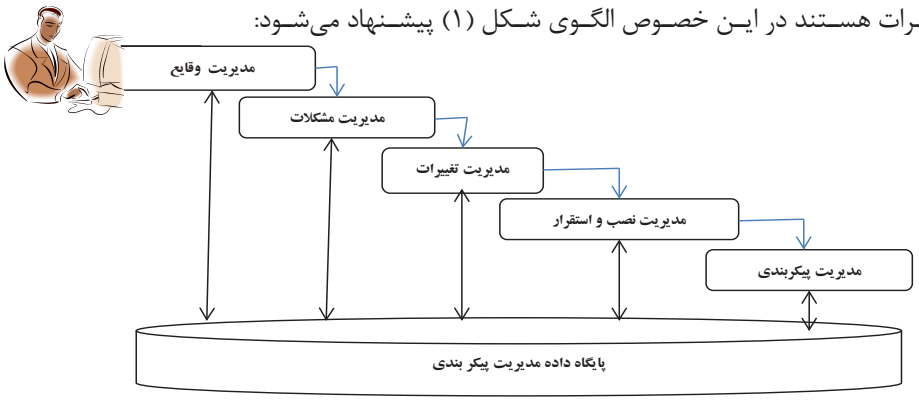
درنتیجه سازماندهی مجدد تیم فعلی براساس طرح آماده و اطلاع‌رسانی سازمانی از جمله کارهایی است که در این مرحله صورت خواهند پذیرفت. تقسیم‌بندی براساس وجوه مشترک فعالیت‌ها و فرایندهای این دو استاندارد است که در جدول(۱) آورده شده است:

جدول ۱: مقایسه‌ی مفاهیم در استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1

۱-۱) مختص ISO/IEC 20000	۱-۲) قسمت‌های به اشتراک گذاشته‌شده (برخی همپوشانی/ تفاوت‌ها)		۱-۳) مختص ISO/IEC 27000
• بودجه‌بندی و حسابداری خدمت (ISO/IEC 27015) • مدیریت روابط کسب‌وکار (ISO/IEC 27031) • طراحی و انتقال خدمات جدید یا تغییریافته • مدیریت سطح خدمت	• مدیریت منابع • ارزیابی مخاطره (ISO/IEC 27005) • نقش‌ها و مسئولیت‌ها • مدیریت امنیت اطلاعات (ISO/IEC 27014) • مدیریت تداوم خدمت وقابلیت دسترسی • مدیریت تأمین کننده (ISO/IEC 27036)	• مدیریت ظرفیت • مدیریت تغییر • مدیریت پیکربندی • مدیریت رخداد و درخواست خدمت • مدیریت مشکل • مدیریت انتشار و استقرار	• طبقه‌بندی اطلاعات • مدیریت منابع اطلاعاتی
۱-۴) قسمت مشترک (یکسان بین هر دو استاندارد)			
• بهبود مستمر (ISO/IEC 27002) • انطباق قانونی و مقرراتی (ISO/IEC 27002) • بازنگری مدیریتی (ISO/IEC 27002)	• PDCA(ISO/IEC 27002) • آموزش و آگاه‌سازی (ISO/IEC 27002) • مدیریت مستندسازی (ISO/IEC 27002)		

استانداردهای خانواده ISO/IEC 27001 که در حوزه‌ی امنیت اطلاعات تدوین‌شده‌اند بسیار متنوع بوده و اکثر فعالیت‌های حوزه‌ی کسب‌وکار را پوشش‌داده و درحال توسعه نیز هستند. نتیجه‌ی تطبیق فرایندهای شکل (۱) با استانداردهای موجود ISO/IEC 27001 در جدول (۱) ثبت‌شده است.

در این تطبیق تلاش می‌شود که تمامی فعالیت‌های ITIL در زیر چتر امنیتی قرار گیرند که در جدول۱ به چهار قسمت تقسیم‌بندی‌شده است. قسمت‌های (۱-۱ و ۴-۱) با استانداردهای مربوطه در حوزه‌ی ISO/IEC 27001 تطبیق و درج‌شده و قسمت (۲-۱) به‌طور ذاتی امنیتی است. در خصوص قسمت (۲-۱) که هسته‌ی اصلی استقرار بوده و فرایندهای پشتیبانی خدمات که شامل فرایندهایی همانند مدیریت درخواست‌ها، مدیریت دارایی‌ها یا پیکربندی و مدیریت تغییرات هستند در این خصوص الگوی شکل (۱) پیشنهاد می‌شود:



شکل ۱: چرخه‌ی فرایندهای اصلی طراحی‌شده برای استقرار استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1

۷-۲) سازمان دارای استاندارد ISO/IEC 27001

باتوجه به پیاده‌سازی استاندارد ISO/IEC 27001 و وجود زیرساخت امنیتی در سازمان، استقرار استاندارد ISO/IEC 20000-1 مطابق با بندهای اجرایی استاندارد انجام و ممیزی هر دو استاندارد تحت عنوان ISO/IEC 27013 قابل اجرا خواهد بود.

۷-۳) پیاده‌سازی هم‌زمان استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1

استقرار نظام مدیریت امنیت اطلاعات و فرایندهایی که به‌موجب آن در سازمان مستقر می‌شوند با توجه به اینکه این نظام متولیانی به غیر از واحد فناوری اطلاعات سازمان نیز دارد، می‌تواند باعث تفاوت در رویه‌ها و الزاماتی شود که به‌راحتی مورد پذیرش نباشند.

برای پیاده‌سازی هم‌زمان استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 20000-1 توصیه‌های زیر مفید است: [۱]

۱- در همه‌ی موارد باید هدف سازمان تولید مدیریت یکپارچه بادوام باشدکه مطابقت با هر دو استاندارد را امکان‌پذیر سازد. هدف، مقایسه‌ی استانداردها یا مشخص‌کردن اینکه کدام‌یک بهتر است یا بهتر نیست. جایی‌که تعارض بین دیدگاه‌ها وجود دارد، بهتر است به‌گونه‌ای حل شود که الزامات هر دو استاندارد را برآورده کند و اطمینان دهد که سازمان به بهبود مستمر در ISMS و SMS دست می‌یابد.

۲- سامانه‌ی مدیریت یکپارچه ایدئال براساس کاراترین رویکردها از هر دو استاندارد باشد و به‌طور مناسب اعمال شود.

۳- به هر آنچه برای مطابقت با هر دو استاندارد مورد نیاز است، توجه شود.

۴- قابلیت ردگیری مستند بهتر است بین سامانه‌ی مدیریت یکپارچه و الزامات هر دو استاندارد جداگانه اعمال شود.

۵-جهت کاهش تلاش، یک مجموعه واحد از مستندات می‌تواند برای سامانه‌ی مدیریت یکپارچه ایجاد شود.

۷-۴) مطالعه‌ی موردی "شرکت سیستم‌های اطلاعاتی"

شرکت سیستم‌های اطلاعاتی از مجموعه شرکت‌های یک شرکت مادر است که بیش از چهار دهه در ارائه‌ی خدمات IT به سازمان‌ها و شرکت‌های دولتی مشغول به خدمت هستند. در سال ۱۳۷۶ شمسی با توجه به گسترش فعالیت‌های رایانه‌ای در سازمان‌ها، شرکت سیستم‌های اطلاعاتی، اقدام به انجام مهندسی مجدد در کل شرکت و در همین مورد، به‌منظور جلب رضایت مشتریان و کسب سهم بازار بیشتر اقدام به راه‌اندازی سامانه‌ی خدمات پس از فروش و ارائه‌ی خدمات گارانتی و ورانتی در سراسر کشور کرد.

در سال ۱۳۸۶ شمسی جهت بهبودو ارئه‌ی خدمات ویژه، اقدام به برقراری خط ارتباطی ویژه E1 و به‌تدریج راه‌اندازی Help Desk به‌صورت مکانیزه کرد. در سال‌های اخیر به‌منظور ارتقای سطح کیفیت خدمات حوزه‌ی IT مطالعات شرکت درزمینه‌ی استقرار ISO/IEC 20000 بوده و با مشاوره‌ی شرکت‌های صاحب‌نظر اقدام به ترجمه و بازنگری پنج قسمت از اسناد استاندارد ISO/IEC 20000 کرده است. گام فعلی شرکت سیستم‌های اطلاعاتی، یافتن شرکت صادرکننده‌ی گواهی‌نامه‌ی ISO/IEC 20000 جهت انجام ممیزی شخص ثالث است.

رشد تدریجی و هدفمند این شرکت در استقرار ISO/IEC 20000 مشهود بوده وگام بعدی ایجاد بستری امن برای ادامه‌ی حیات آن است که ISO/IEC 27001 به‌عنوان مکملی ایفای نقش خواهد کرد. و درنهایت تلفیق این دو استاندارد، ضرورت استاندارد ISO/IEC 27013 را محقق می‌سازد.

۸) نتایج مطالعه‌ی موردی "شرکت آلفا"

شرکت آلفا از مجموعه شرکت‌های یک شرکت مادر و دارای بیش از چهار دهه سابقه در ارائه‌ی خدمات IT به سازمان‌ها و شرکت‌های دولتی است. در سال ۱۳۷۶ با توجه به گسترش فعالیت‌های رایانه‌ای در سازمان‌ها، شرکت آلفا، اقدام به انجام مهندسی مجدد در کل شرکت و در همین ارتباط، به‌منظور جلب رضایت مشتریان و کسب سهم بازار بیشتر اقدام به راه‌اندازی سامانه‌ی خدمات پس از فروش و ارائه‌ی خدمات گارانتی و ورانتی در سراسر کشور کرد.

در سال ۱۳۸۶ جهت بهبود و ارئه‌ی خدمات ویژه اقدام به برقراری خط ارتباطی ویژهE1 و به‌تدریج راه‌اندازی Help Desk به‌صورت مکانیزه و درنهایت استقرار نظام مدیریت خدمات فناوری اطلاعات مبتنی بر استاندارد ISO/IEC 20000-1 کرد.

مشکل بعدی شرکت آلفا الزام مشتریان این شرکت برای حفظ امنیت در تمامی مبادلات فنی و تجاری و محصولات نهایی شرکت بود. مدیران این شرکت با دو استاندارد مواجه بودند. دیدگاه‌های متفاوتی نسبت به این حوزه وجود داشت: آیا استانداردها مکمل یکدیگر هستند؟ آیا استانداردها دارای تناقض هستند؟ آیا اصطلاحات یکسان این استانداردها معانی مشابهی دارند؟ تقدم و تأخر آن‌ها چگونه است؟ دامنه‌ی شمول و اثرگذاری آن‌ها چیست و ... . نتایج کار کارشناسی انجام‌شده و بررسی سایر استانداردهای موجود از جمله استاندارد ISO/IEC 27013 مدیران شرکت را به استفاده از روشی مشابه روش ذکرشده در بند ۷-۱ سوق داد که به‌صورت کارآمد منابع سازمانی را در مسیر مشخص هدایت‌کرده و مسیر روشنی برای استقرار هر دو استاندارد ارائه می‌کند.

تخصیص تیم‌های مجزا و نگرش جزیره‌ای به این استانداردها سبب موازی‌کاری‌های متعدد در سازمان، هدررفتن منابع مالی و سرمایه‌های انسانی‌شده و اثربخشی هریک از استانداردها را نیز کاهش می‌دهد.

۹) نتیجه‌گیری

اگرچه ورود IT به صنایع و شرکت‌ها مزایای فراوانی را به‌دنبال داشته است؛ لیکن فراموش نکنیم "فناوری اطلاعات" یک سکه‌ی دوروست، هم فرصت است و هم تهدید! اگر به همان نسبتی که به توسعه و رواج آن توجه و تکیه می‌کنیم به "امنیت" آن توجه نکنیم می‌تواند به‌سادگی و در کسری از ثانیه تبدیل به یک تهدید و مصیبت بزرگ شود. بنابراین، نیاز روزافزون به استفاده از فناوری‌های نوین در عرصه‌ی اطلاعات و ارتباطات، ضرورت استقرار یک نظام مدیریت امنیت اطلاعات را بیشتر آشکار می‌کند.

همچنین باید درنظر داشت که استقرار هم‌زمان دو نظام مدیریتی(ISMS , SMS) و وجود فرایندهای مشابه می‌تواند برای مدیریت فناوری اطلاعات سازمان مشکلاتی را ایجاد کند. در این مقاله تلاش شد تا با ارائه‌ی مفاهیم دو استاندارد مرجع برای این حوزه (ISO/IEC 20000 و ISO/IEC 27001) و مزایای هریک و بیان ضرورت استقرار هم‌زمان آن‌ها، با توجه به وضعیت شرکت از نظر تقدم استقرار، روشی برای مواجهه با این موضوع ارائه داد. تلاش‌شده است که روش ارائه‌شده قابل کاربرد در صنایع مختلف بوده و شامل خطوط راهنمایی که دربرگیرنده‌ی هزینه‌کرد صحیح منابع سازمانی است، باشد.

مراحل این روش، که بیشتر جنبه‌ی انتزاعی و کیفی دارد، با روش اتخاذشده توسط تیم کارشناسی شرکت آلفا مطابقت‌داشته و از نظر عملیاتی و بهینه‌بودن مورد تأیید کارشناسان خبره قرارگرفته است.

۱۰) منابع و مراجع

۱. مدیریت خدمات فناوری اطلاعات، ۱۳۹۲، انتشارات مؤسسه‌ی آموزشی و تحقیقاتی صنایع دفاعی.

2. ISO/IEC 27013:2012 Information technology-Security techniques-Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.

3.IDS-ISO-20000 Information technology-Service management.

4.ISO/IEC 27001:2013 Information Security Management System Requirements.