ارائه‌ی مدل هم‌پوشانی استانداردهای مدیریتی[1] و حاکمیتی[2] فناوری اطلاعات

مصطفی تمتاجی
محمد جمال رازقی

تاریخ دریافت: ۹۴/۰۲/۱۳
تاریخ پذیرش: ۹۴/۰۳/۳۱

چکیده:

توسعه و افزایش ضریب نفوذ فناوری اطلاعات، زمینه‌ساز تغییرات بسیاری در ابعاد مختلف سازمان‌ها شده است. این تغییرات باید بر اساس طرح توسعه و استراتژی کلان سازمان، طرح‌ریزی، اجرا و پایش شوند. این امور در سازمان با حاکمیت و مدیریت مرتبط هستند.

اهمیت این موضوع‌ها سبب پیدایش استانداردها و چارچوب‌های متعدد در حوزه‌های حاکمیتی و مدیریتی فناوری اطلاعات شده است. تنوع استانداردها و چارچوب‌ها، انتخاب را برای کسانی که می‌خواهند مجموعه‌ای بهره‌ور از استانداردها و الگوها را در سازمان خود پیاده‌سازی نمایند مشکل کرده است. در این تحقیق ابتدا مفاهیم و ادبیات مطرح در این حوزه مورد مطالعه قرار گرفته سپس استانداردهای متداول در حوزه‌ی نظام‌های مدیریتی و حاکمیتی فناوری اطلاعات معرفی و تحلیل محتوا شده‌اند. تحلیل حاوی یک روش تحقیق مبتنی بر مطالعات کتابخانه‌ای و مقایسه‌ی تطبیقی با هدف مطالعه‌ی ارتباطات است.

سپس مدل هم‌پوشانی این استانداردها ارائه‌شده است. مدل هم‌پوشانی ارائه شده، تمامی استانداردها، الگوهای برتر و چارچوب‌های مطرح در این حوزه را در بر می‌گیرد. این مدل راهنمای مناسبی جهت انتخاب مرجع مناسب و هم‌راستا با اهداف کسب‌وکار برای سازمان‌ها است.

واژگان کلیدی:

نظام مدیریتی، امنیت اطلاعات، فناوری اطلاعات، حاکمیت

۱) مقدمه

تنوع و گستردگی فعالیت‌ها در سازمان‌ها سبب‌شده است تا فرایندگرایی به‌عنوان یک ضرورت اجتناب‌ناپذیر در سازمان قلمداد شود. فناوری اطلاعات با قابلیت‌های تسهیل‌گرانه خود موتور محرک حرکت سازمان به سمت فرایندگرایی است. سازمان‌های قرن حاضر برای افزایش یکپارچگی و استانداردسازی فرایندها، افزایش سرعت روند جهانی‌شدن، بازسازی و تغییرات مکرر تجارت به فناوری اطلاعات نیازمند هستند. فناوری اطلاعات ستون فقرات فرایندگرایی و ایجادکننده و پشتیبانی کننده‌ی آن در سازمان است. استفاده‌ی مؤثر و کارآمد از فناوری اطلاعات در سازمان نیازمند پیاده‌سازی نظام یکپارچه برای حاکمیت و مدیریت آن است.

حوزه‌های گسترده و عمیق مطرح در حاکمیت و مدیریت فناوری اطلاعات از جمله توانایی ایجاد تغییرات سازمانی، مدیریت تغییر، مدیریت سرمایه‌های فکری، طراحی معماری، مدیریت برنامه، مدیریت قراردادها و منابع، تحلیل و طراحی فرایند و ارائه راه‌حل برای الزامات راهبردی سبب‌شده تا پرداختن به این موضوع به‌عنوان یک مسأله چند بعدی مورد

1. Management
2. Governance

توجه قرار گیرد. در این راستا علاوه بر چارچوب‌های ارائه‌شده در مراجع علمی مثل مدیریت‌دانش، BSC, PRINC2, PMBOK, MSP, CMMI, GREEN IT, TOGAF, COSCO, SOX, PC1055 سازمان‌های استانداردسازی نیز به این مسأله توجه کرده و استانداردهایی منتشر کرده‌اند. به‌طورکلی با توجه به رشد روزافزون و چشمگیر فناوری اطلاعات و لزوم استانداردسازی در این حوزه و به‌منظور وجود نگرش جامع نسبت به استانداردسازی در زمینه‌ی مباحث فناوری اطلاعات، سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC)، اقدام به ایجاد کمیته‌ی فنی مشترک (JTC1) به نام "فناوری اطلاعات" با ۱۸ زیرکمیته‌ی فعال کردند که تاکنون ۲۷۲۹ استاندارد در زمینه‌های مختلف فناوری اطلاعات منتشر کرده‌اند[۱]. که در این تحقیق، به معرفی و تحلیل محتوایی تعدادی از این استانداردها و ارائه مدل هم‌پوشانی بین آن‌ها پرداخته‌شده است.

۲) ادبیات تحقیق

گستره‌ی وسیع موضوعات هدایت یک سازمان، امکان مطالعات گسترده در ادبیات تحقیق را برای محقق ناممکن ساخته است. لذا ادبیات تحقیق محدود به اصطلاحات متداولی‌شده است که برداشت‌های متفاوتی از آن‌هاشده و در برخی موارد به‌جای یکدیگر به‌کار می‌روند.

۲-۱) حاکمیت و مدیریت

اصطلاح "Governance" از ریشه‌ی لاتین واژه‌ی "Gubernare" برگفته‌شده است که به معنای حکم‌رانی، اختیارداری، نظارت، فرمان‌برداری و هدایت‌کردن است و قبل از آن برای هدایت‌کردن کشتی به‌کار می‌رفته است. حاکمیت تضمین می‌کند که نیازها، شرایط و انتخاب‌های ذی‌نفعان، مورد بررسی و توجه قرار گرفته، اهداف متعادل و مورد توافق‌شده، جهت‌گیری‌های عمده از طریق اولویت‌بندی و تصمیم‌گیری تعیین‌شده و بر عملکرد و حرکت در مسیر صحیح ترسیم‌شده به‌منظور تحقق اهداف، نظارت شود (EDM). در اغلب شرکت‌ها، حاکمیت مسئولیت هیئت مدیره تحت رهبری رئیس هیئت مدیره است.

مدیریت، فعالیت‌ها را در راستای جهت تعیین‌شده در اسناد حاکمیت برای دستیابی به اهداف شرکت، برنامه‌ریزی می‌کند، سامان دهی می‌کند، اجرا می‌کند و بر آن‌ها نظارت می‌کند (PBRM). در اغلب شرکت‌ها، مدیریت مسئولیت مدیریت اجرایی تحت رهبری مدیر عامل اجرایی (CEO) است. [۲]

۲-۲) حاکمیت سازمانی

ترجمه‌ی واژه‌ی "Corporate Governance" به فارسی معادل‌هایی نظیر حاکمیت شرکتی، حاکمیت سهامی، اداره‌ی سازمانی و راهبری سازمانی داشته است. دراین مقاله از واژه‌ی "راهبری سازمانی" استفاده‌شده است. تعاریف ارائه‌شده برای راهبری سازمانی متنوع است. عمده‌ترین عامل متمایز کننده‌ی این تعاریف را می‌توان پهنه یا گستره شمول راهبری سازمانی دانست. ازیک منظر می‌توان این نظام را رابطه‌ی "مدیران" با "سهامداران" دانست که مبنای نظری آن "تئوری نمایندگی" در شکل محدود خود است. در آن سوی این طیف و درنگرشی وسیع، راهبری سازمانی رابطه‌ی شرکت با تمام ذی‌نفعان خود را بر می‌گیرد که پشتوانه نظری آن را می‌توان "تئوری ذی‌نفع" دانست. حاکمیت شرکتی مجموعه‌ای از نظام‌ها، فرآیندها و ساختارهایی است که با استفاده از سازوکارهای درون‌سازمانی و نیز سازوکارهای برون‌سازمانی در پی کسب اطمینان از رعایت حقوق ذی‌نفعان، پاسخ‌گویی، شفافیت و عدالت در واحد تجاری است. یکی از مهمترین محورهای استقرار حاکمیت شرکتی مناسب در هر بنگاه اقتصادی، ایجاد و استقرار نظام مدیریت ریسک است رعایت خط‌مشی‌ها، الزامات قانونی و قواعد کسب‌وکار از جنبه‌های مشترک مورد بررسی در هر دو نظام محسوب می‌شود. در ادامه برخی تعاریف ارائه‌شده در خصوص حاکمیت سازمانی ارائه‌شده است[۳]

- راهبری سازمانی، شیوه‌های به‌کار گرفته‌شده

توسط مدیران شرکت با هدف تعیین استراتژی‌هایی است که موجب دستیابی شرکت به اهداف تعیین شده، کنترل ریسک و مصرف بهینه منابع می‌شود. (فدراسیون بین‌المللی حسابداران -۲۰۰۴)

- راهبری سازمانی نظامی است که شرکت‌ها را هدایت و کنترل می‌کند. تمرکز اصلی بر ایفای وظیفه مدیران ارشد سازمانی در رعایت اصول شفافیت، درستکاری و پاسخ‌گویی است. (گزارش کادبری-۱۹۹۲)

- راهبری سازمانی، فرآیند نظارت و کنترل عملکرد مدیران شرکت است به‌گونه‌ای که متضمن منافع سهامداران باشد. (پارکینسون- ۱۹۹۴)

- هدف بنیادی در راهبری سازمانی افزایش ثروت سهامداران در بلند مدت است، به‌گونه‌ای که منافع سایر ذی‌نفعان نیز رعایت شود. (بورس اوراق بهادار هندوستان- ۲۰۰۰)

- راهبری سازمانی برای برقراری تعادل بین اهداف اقتصادی و اجتماعی و نیز اهداف فردی و عمومی است. راهبری سازمانی موجبات استفاده‌ی مؤثر از منابع و الزام به پاسخ‌گویی را فراهم می‌سازد و هدف اصلی آن است که منافع ذی‌نفعان و جامعه تا حد ممکن به هم نزدیک شوند. (بانک جهانی-۲۰۰۱)

راهبری سازمانی[1]: نظامی که به‌وسیله‌ی آن سازمان‌ها هدایت و کنترل می‌شوند.

(Adapted from Cadbury 1992 and OECD 1999)

۲-۳) حاکمیت سازمانی فناوری اطلاعات[2]

نظامی که به‌وسیله آن استفاده‌ی فعلی و آتی فناوری اطلاعات هدایت و کنترل می‌شود. حاکمیت سازمانی فناوری اطلاعات شامل ارزیابی و هدایت استفاده‌ی فناوری اطلاعات به‌منظور پشتیبانی سازمان و پایش استفاده برای دستیابی به طرح‌ها و هم‌چنین استراتژی و خط‌مشی‌های استفاده از فناوری اطلاعات در داخل سازمان می‌شود[۴].

۳) روش تحقیق

روش مورد استفاده در این تحقیق روش توصیفی با بهره‌گیری از مطالعات کتابخانه‌ای است. برای بررسی محتوای آشکار پیام‌های موجود در یک متن می‌توان از روش تحلیل محتوی استفاده کرد. در این روش محتوای آشکار پیام‌ها به‌طور کمی و نظام‌دار توصیف می‌شود. مطابق تعریف والیرز و واینر، تحلیل محتوی روشی منظم برای بررسی اطلاعات ثبت‌شده است. کرایپندرف تحلیل محتوی را به‌صورت روش تحقیق برای دستیابی به نتایج تکرارپذیر و معتبر از داده‌ها و زمینه‌های آن‌ها تعریف می‌کند و کرلینچر آن را روش مطالعه و تجزیه و تحلیل ارتباط به شکلی نظام‌مند، عینی و کمی به‌منظور سنجش متغیرها می‌داند.

چارچوب اصلی تحلیل محتوی را در سوال "چه کسی، چه چیزی را و چگونه و با چه تأثیری می‌گوید" توصیف کرده‌اند. گرچه تحلیل محتوی غالباً برای توصیف به‌کار می‌رود ولی در برخی شرایط می‌توان از این روش برای آزمون فرضیه هم استفاده کرد. به‌عبارت دیگر تحلیل محتوی مطالعه‌ی ارتباطات است و یک روش پژوهشی است که به‌صورت منظم و عینی برای توصیف کمی یا کیفی محتوای آشکار ارتباطات به‌کار برده می‌شود. به‌عنوان مثال در تحلیل محتوای کتاب می‌توان به بخش‌های مورد تأکید کتاب و ارتباطات آن‌ها با یکدیگر پی برد. در این مقاله نیز از روش تحلیل محتوی علمی استفاده‌شده است و در آن محقق با مطالعه عمیق منابع و با در نظر گرفتن اهداف تحقیق، محتوی را درک کرده و بر اساس شاخص‌های مناسب آن‌ها را با یکدیگر مقایسه می‌کند. خروجی این تحلیل محتوی و مقایسه تطبیقی می‌تواند جدول مقایسه یا مدل هم‌پوشانی باشد. با توجه به ماهیت تحقیق انجام‌شده و هدف آن، محقق مدل هم‌پوشانی بین استانداردها، الگوهای برتر و چارچوب‌های مطرح در حوزه‌ی حاکمیت و

1. Corporate governance
2. Corporate governance of IT

مدیریت فناوری اطلاعات را ارائه کرده است.

۴) استانداردهای نظام‌های مدیریتی فناوری اطلاعات

۴-۱) استاندارد نظام مدیریت خدمات فناوری اطلاعات IDS-ISO-20000

نظام مدیریت خدمات در ISO-20000-1 به‌عنوان یک نظام مدیریت با هدف هدایت، نظارت و کنترل فعالیت‌های مدیریت خدمت برای ارائه‌دهنده‌ی خدمت تعریف‌شده است. نظام مدیریت خدمت باید شامل آنچه برای برنامه‌ریزی، طراحی، انتقال، تحویل و بهبود خدمات مورد نیاز است، باشد. حداقل این موارد، شامل خط‌مشی‌های مدیریت خدمات، اهداف، طرح‌ها، فرآیندها، رابطه‌های فرآیند، اسناد و منابع است. نظام مدیریت خدمات شامل تمام روال‌ها به‌عنوان یک نظام مدیریت منعطف است. هم‌چنین فرآیندهای مدیریت خدمات نیز به‌عنوان بخشی از نظام مدیریت خدمات در نظر گرفته می‌شود. [۵]

یکپارچه‌سازی و پیاده‌سازی هماهنگ نظام مدیریت خدمات، فراهم‌کننده‌ی کنترل مداوم، اثربخشی بیشتر، بهره‌وری و فرصت‌های بیشتر برای بهبود مستمر است. نظام مدیریت خدمات، سازمان را قادر به استفاده‌ی مؤثر از یک چشم‌انداز مشترک می‌سازد.

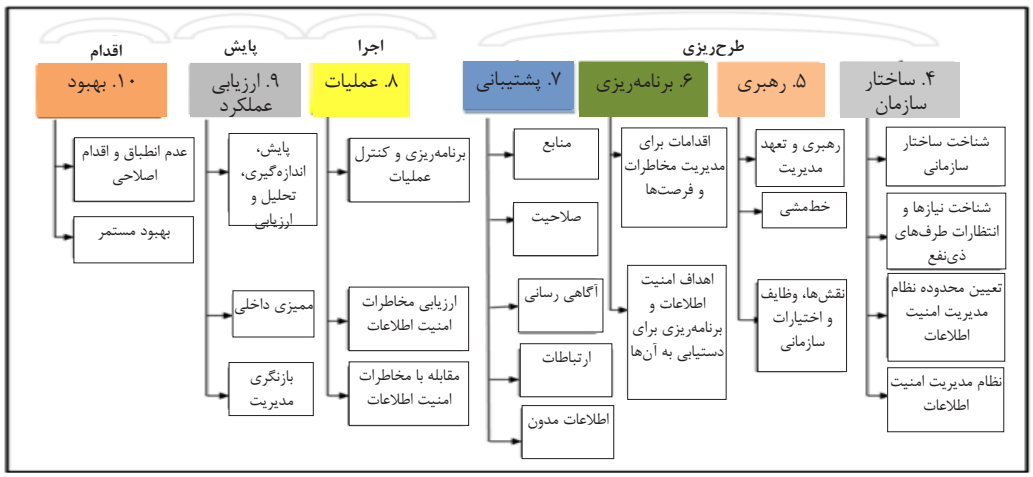
استاندارد ISO/IEC 20000-1 می‌تواند توسط سازمان‌ها یا بخش‌هایی از سازمان که از خدمات استفاده می‌کنند یا آن را ارائه می‌دهند، استفاده شود. هرچند همه‌ی فرایندهایی که توسط استاندارد پوشش داده می‌شوند، توسط فراهم‌کننده‌ی خدمت کنترل می‌شوند و تنها ارائه‌دهنده ی خدمت می‌تواند ادعای انطباق با این استاندارد را داشته باشد، لیکن این استاندارد برای مشتری و ارائه‌دهنده‌ی خدمت ایجاد ارزش افزوده می‌کند. مدیریت خدمت، فعالیت‌ها و منابع ارائه‌دهنده‌ی خدمت را در طراحی، توسعه، انتقال، تحویل و بهبود خدمات برای برآوردن الزامات خدمت مطابق با توافقات انجام‌شده با مشتری، هدایت و کنترل می‌کند. برای برآورده‌سازی الزامات این استاندارد، طیفی از فرایندهای مدیریت خدمات باید توسط ارائه‌دهنده‌ی خدمت پیاده‌سازی شود. مدیریت امنیت اطلاعات یکی از فرایندهای مدیریت خدمت محسوب می‌شود[۶].

۴-۲) استاندارد نظام مدیریت امنیت اطلاعات (ISO/IEC 27001)

با توجه به چند وجهی بودن مقوله‌ی امنیت و لزوم توجه چند بعدی به آن و هم‌چنین توجه روزافزون به مباحث مدیریت امنیت اطلاعات از طریق برقراری قوانین و ضوابط ملی، منطقه‌ای و بین‌المللی و راهبردهای جدید به‌منظور پاسخ‌گویی به انتظارات و الزامات طرف‌های ذی‌نفع نسبت به اطمینان از امنیت اطلاعات، کمیته‌ی فرعی امنیت تصمیم به تدوین استاندارد "نظام مدیریت امنیت اطلاعات" در کنار استانداردهای فنی گرفت و بر این اساس خانواده‌ی استانداردهای ۲۷۰۰۰ به‌عنوان مرجع بین‌المللی پذیرفته‌شده برای امنیت اطلاعات مطرح شدند. از این خانواده تاکنون بیش از ۳۵ استاندارد منتشرشده یا در حال انتشار است که برخی از آن‌ها در جدول (۱) معرفی شده‌اند[۱].

نظام مدیریت امنیت اطلاعات، بخشی از نظام مدیریت کلان بناشده بر دیدگاه مخاطرات کسب و کار، به‌منظور ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات است. یک نظام مدیریتی مشتمل بر ساختار سازمانی، خط‌مشی‌ها، طرح‌ریزی فعالیت‌ها، مسئولیت‌ها، تجارب، روش‌های اجرایی مدون، فرایندها و منابع است[۷].

استاندارد فوق شامل ۱۴ حوزه، ۳۶ هدف کنترلی و ۱۱۴ کنترل امنیتی به‌منظور اقدامات بازدارنده و نظارتی است. شکل (۱) فهرست الزامات ذکرشده در متن استاندارد را نشان می‌دهد[۸].

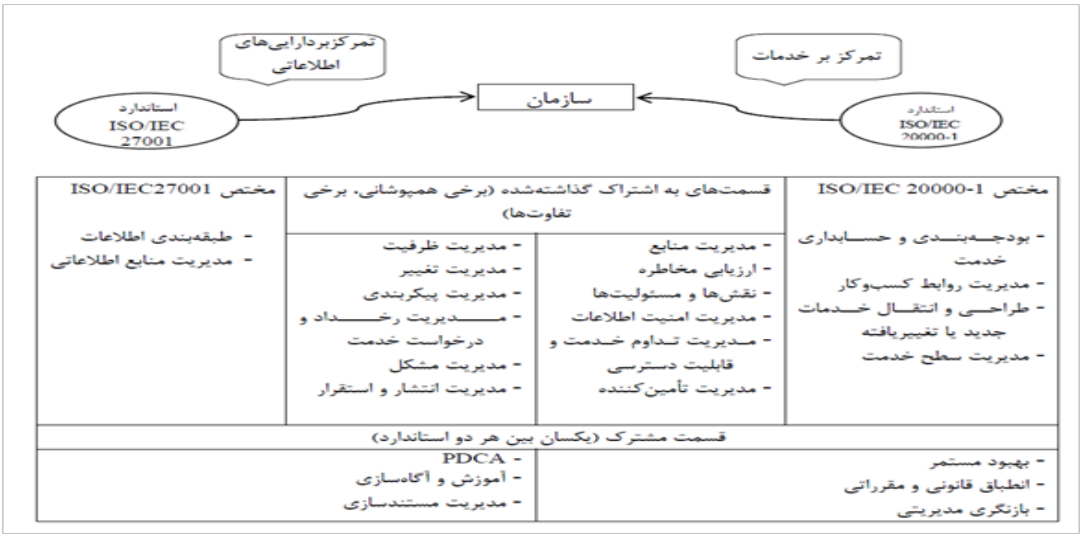


شکل ۱: الزامات استاندارد ۲۷۰۰۱ [ISO/IEC ۲۷۰۰۱:۲۰۱۳]

استاندارد ISO/IEC 27001 چارچوبی برای ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود نظام مدیریت امنیت اطلاعات به‌منظور محافظت از دارایی‌های اطلاعاتی فراهم می‌کند. برای مطابقت با این استاندارد، سازمان باید نظامی مبتنی بر ارزیابی مخاطرات پیاده‌سازی نماید. در این راستا سازمان باید کنترل‌های(سنجه‌های) متنوعی را برای مدیریت مخاطرات انتخاب، پیاده‌سازی، پایش و بازنگری کند. [۶]

۴-۳) تحلیل محتوی استانداردهای ۲۷۰۰۱ و ۲۰۰۰۰

مدیریت خدمات به‌طور مستقیم با کارایی و سودآوری مرتبط است. لیکن مدیریت امنیت اطلاعات اغلب به‌عنوان پایه‌ای برای تحویل خدمت مؤثر لحاظ نمی‌شود. بر این اساس با وجود شباهت‌های بسیار در اهداف کنترلی و کنترل‌ها، مدیریت خدمت نسبت به مدیریت امنیت اطلاعات در اولویت پیاده‌سازی قرار می‌گیرد. باوجود شباهت بسیار این دو استاندارد دارای اهداف متفاوتی هستند. مدیریت خدمات به‌منظور حصول اطمینان از ارائه‌ی خدمات مؤثر طراحی‌شده ولی مدیریت امنیت اطلاعات به‌منظور توانمندسازی سازمان برای مدیریت مخاطرات امنیت اطلاعات و پیشگیری از رخدادهای امنیتی طراحی‌شده است. در بررسی و تحلیل این دو استاندارد در کنار یکدیگر باید به دامنه‌ی کاربرد دو استاندارد و تفاوت محتوایی آن، تفاوت معنایی در اصطلاحات دارایی در مدیریت خدمات و دارایی اطلاعاتی در مدیریت امنیت اطلاعات توجه کرد. [۶]



شکل ۲: مقایسه‌ی مفاهیم در استانداردهای ISO/IEC 27001 و ISO/IEC 20000-1

۵) استانداردهای حاکمیت فناوری اطلاعات

۵-۱) استاندارد حاکمیت فناوری اطلاعات IDS 1338 و ISO 38500

هدف این استاندارد ارائه‌ی چارچوبی از اصول ارزیابی، هدایت و پایش کاربرد فناوری اطلاعات در سازمان برای مدیران است. بیشتر سازمان‌ها از فناوری اطلاعات به‌عنوان ابزار اساسی کسب‌وکار استفاده می‌کنند و تعداد کمی از سازمان‌ها بدون استفاده از آن کارایی مناسبی خواهند داشت. هزینه‌های صرف‌شده در سازمان بخش قابل توجهی از هزینه‌های مالی و منابع انسانی سازمان است، ولی برگشت این سرمایه ملموس نبوده و حتی در برخی موارد اثرات معکوس چشمگیری هم دارد.

علت اصلی دستاوردهای منفی تأکید روی جنبه‌های مالی و فنی فناوری اطلاعات به‌جای تأکید روی زمینه‌ی کاربرد آن در کسب‌وکار است. این استاندارد چارچوبی برای حاکمیت اثربخش فناوری اطلاعات شامل مفاهیم و تعاریف، اصول و مدل ارائه می‌کند.

استاندارد فوق اصول راهنمایی برای مدیران سازمان به‌منظور استفاده قابل قبول، کارآمد و اثربخش فناوری اطلاعات ارائه می‌کند. پیروی از این اصول، در متعادل ساختن مخاطرات و بهره‌گیری از فرصت‌های ناشی از استفاده‌ی فناوری اطلاعات کمک می‌کند. هم‌چنین مدلی برای حاکمیت فناوری اطلاعات در این استاندارد ارائه‌شده است.

چارچوب حاکمیت فناوری اطلاعات سازمانی خوب از شش اصل زیر تبعیت می‌کند. این اصول آنچه باید رخ دهد را بیان می‌کنند و چگونگی اجرا و پیاده‌سازی را مطرح نمی‌کند:[۴]

۱) مسوولیت: افراد و گروه‌ها مسئولیت خود را در رابطه با عرضه و تقاضای فناوری اطلاعات درک و قبول کنند.

۲) راهبرد: راهبرد کسب‌وکار سازمان قابلیت‌های فناوری اطلاعات در حال حاضر و آینده را در نظر گیرد.

۳) اکتساب: اکتساب فناوری اطلاعات بر اساس دلایل معتبر و مبتنی بر تحلیل مناسب و مستمر با تصمیم‌سازی شفاف و روشن باشد.

۴) کارآیی: هدف فناوری اطلاعات پشتیبانی سازمان، ارائه خدمات، سطوح خدمات و کیفیت مورد نیاز الزامات کسب‌وکار است.

۵) انطباق: فناوری اطلاعات با قوانین و مقررات انطباق دارد.

۶) رفتار انسانی: خط‌مشی‌ها، اقدامات و تصمیمات حوزه فناوری اطلاعات برای رفتار انسانی احترام قایل است.

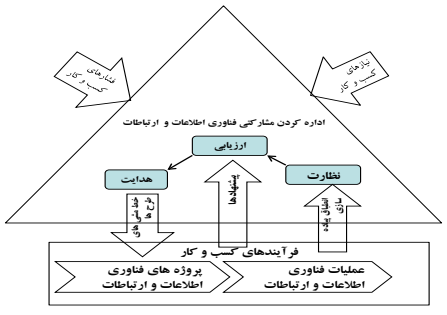
مدیران باید فناوری اطلاعات را از طریق سه فعالیت اصلی حاکمیت کنند:

الف) ارزیابی استفاده‌ی فعلی و آتی از فناوری اطلاعات.

ب) هدایت آماده‌سازی و پیاده‌سازی خط‌مشی‌ها و برنامه‌هایی برای اطمینان از برآورده‌سازی اهداف کسب‌وکار از طریق استفاده از فناوری اطلاعات.

پ) پایش انطباق خط‌مشی‌ها و عملکرد بر اساس برنامه‌های طرح‌ریزی شده.

شکل (۳) مدل حاکمیت فناوری اطلاعات از طریق چرخه‌ی ارزیابی- هدایت- پایش را نشان می‌دهد.



شکل ۳: مدل یکپارچه‌ی حاکمیت فناوری اطلاعات

این استاندارد در ادامه‌ی راهنمایی‌هایی برای پیاده‌سازی اصول شش گانه‌ی حاکمیت شرکتی فناوری اطلاعات بر اساس مدل سه وجهی ارزیابی- هدایت- پایش ارائه می‌کند. [۴]

استاندارد فناوری اطلاعات چارچوب حاکمیت (INSO 17619)[1]

استاندارد چارچوب حاکمیت (معماری خدمت‌گرا SOA 17619)[2]

این استاندارد، چارچوبی است که محتوا و تعاریفی را برای توانمندسازی سازمان در درک و گسترش حاکمیت معماری خدمت‌گرا فراهم می‌آورد. و برای موارد زیر کاربرد دارد:

حاکمیت معماری خدمت‌گرا، شامل رابطه‌ی بین کسب‌وکار، فناوری اطلاعات و حاکمیت معماری سازمانی (EA)؛ این امر به سازمان به درک اثر شدیدی که معرفی معماری سرویس‌گرا در یک سازمان روی حاکمیت دارد، کمک می‌کند.

یک مدل مرجع حاکمیت معماری خدمت‌گرا) و بخش‌های تشکیل‌دهنده‌ی آن؛ که به سازمان در مشخص ساختن روش کار حاکمیت مناسب؛ و گرفتن بهترین شیوه به‌عنوان مبنایی برای یک رویکرد مشترک، کمک می‌کند.

روش حیاتی حاکمیت معماری خدمت‌گرا که به سازمان‌ها در سفارشی‌کردن مدل مرجع حاکمیت معماری خدمت‌گرا و درک روش کار حاکمیت معماری خدمت‌گرا به آن‌ها، کم می‌کند.

شکل۴: روابط حاکمیت معماری سرویس گرا

۵-۲) استاندارد حاکمیت امنیت اطلاعات (استاندارد ایران ایزو آی- ای سی ۲۷۰۱۴)

این استاندارد به بیان راهنمایی‌هایی در خصوص مفاهیم و اصول راهبری امنیت اطلاعات در سازمان می‌پردازد. سازمان‌ها با بهره‌گیری از این استاندارد می‌توانند فعالیت‌های مرتبط با امنیت اطلاعات را در سازمان ارزیابی (evaluate)، هدایت (direct)، پایش (monitor) و اطلاع رسانی (تبادل اطلاعات) (communicate) کنند. پیش‌نیاز راهبری امنیت اطلاعات، هم‌راستاکردن اهداف و راهبردهای امنیت اطلاعات با اهداف و راهبردهای کسب‌وکار و انطباق آن‌ها با قانون، مقررات و قراردادها است. مشابه با استاندارد ۲۷۰۰۱ در این استاندارد نیز پیاده‌سازی یک رویکرد مدیریت مخاطرات ارزیابی، تحلیل، پیاده‌سازی و پایش می‌شود.[۹]

اهداف مدیریت امنیت اطلاعات عبارتند از: [۹]

- هم‌راستایی راهبردی: هم‌راستا نمودن اهداف و راهبرد امنیت اطلاعات با اهداف و راهبرد کسب و کار،

1. INSO
2. SOA

- ارزش‌دهی به ذی‌نفعان: شناسایی ذی‌نفعان و ارزش‌دادن به نیازمندی‌های امنیتی آن‌ها،
- پاسخ‌گویی: اطمینان از لحاظ شدن تمامی مخاطرات امنیتی،

دستاوردهای مورد نظر به‌دست‌آمده از پیاده‌سازی مؤثر مدیریت امنیت اطلاعات شامل برآورده‌سازی دیدگاه هیئت رییسه‌ی سازمان در خصوص امنیت اطلاعات، رویکرد چابک در خصوص تصمیم‌گیری در مورد مخاطرات امنیتی، سرمایه‌گذاری کارا و اثربخش در امنیت اطلاعات و انطباق با الزامات قانونی، مقرراتی و قراردادی است.

مدیریت امنیت اطلاعات از اصول و فرایندهایی تشکیل‌شده است. اصول، قواعد پذیرفته‌شده برای اقدامات مدیریت امنیت اطلاعات هستند که به‌عنوان راهنمای برای پیاده‌سازی مدیریت ایفای نقش می‌کنند. فرایندها مجموعه‌ای از وظایف و روابط متقابل آن‌ها را تشریح می‌کنند که زمینه‌ی را برای مدیریت امنیت اطلاعات فراهم می‌کنند. برآورده ساختن نیازهای ذی‌نفعان و لحاظ‌کردن نیازمندی‌های آن‌ها برای موفقیت امنیت اطلاعات در بلند مدت ضروری است. اصول شش‌گانه زیر مبنای مناسبی برای پیاده‌سازی فرایندهای مدیریت امنیت اطلاعات با این رویکرد را فراهم می‌کنند. [۹]

اصل۱: برقراری امنیت اطلاعات در سطح سازمان: مدیریت امنیت اطلاعات باید تضمین کند که فعالیت‌های امنیت اطلاعات فراگیر و یکپارچه هستند.

اصل۲: پذیرش رویکرد مبتنی بر مخاطرات: مدیریت امنیت اطلاعات باید مبتنی بر رویکرد تحلیل و ارزیابی مخاطرات باشد.

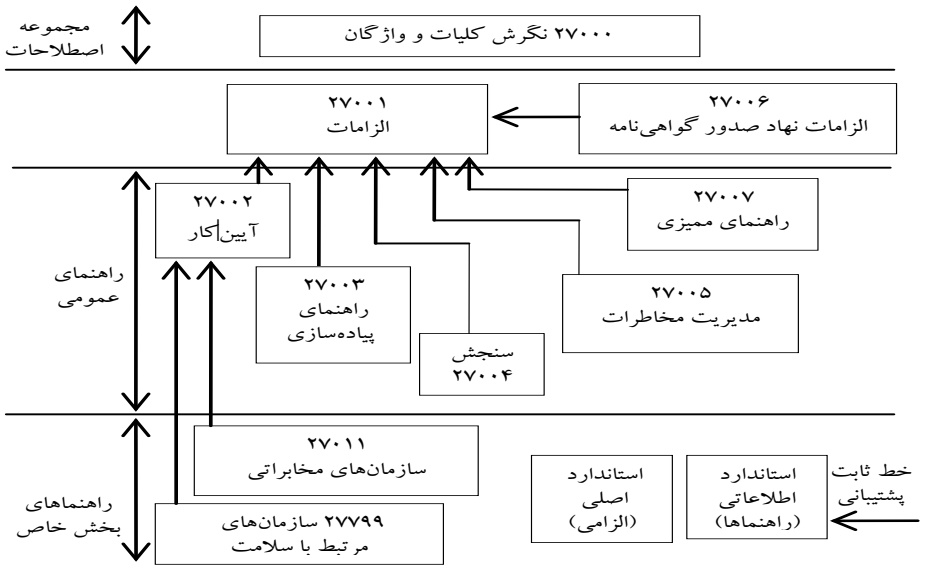
اصل۳: جهت‌دهی مسیر سرمایه‌گذاری: مدیریت امنیت اطلاعات باید راهبرد سرمایه‌گذاری امنیت اطلاعات سازگار با الزامات کسب‌وکار و نیازهای ذی‌نفعان را ترسیم نماید.

اصل۴: تضمین انطباق با الزامات درونی و بیرونی: مدیریت امنیت اطلاعات باید منطبق بر قوانین و مقررات الزام‌آور، الزامات کسب‌وکار و قراردادهای تعهدآور و سایر الزامات مرتبط باشد.

اصل۵: ایجاد یک محیط امنیتی مثبت: مدیریت امنیت اطلاعات باید مبتنی بر شأن و رفتار انسانی و نیازهای در حال تکامل ذی‌نفعان باشد.

اصل۶: بازنگری عملکرد و اثربخشی در نتایج کسب و کار: رویکرد اتخاذشده برای مدیریت امنیت اطلاعات باید زمینه‌ساز محافظت از اطلاعات سازمانی به‌منظور پشتیبانی کسب‌وکار و فراهم آورنده سطوح امنیت اطلاعات مورد نظر باشد.

در شکل زیر روابط استانداردهای این سری را نشان می دهد.



شکل ۵: روابط استانداردهای خانواده ۲۷۰۰۰

فرایندهای راهبری امنیت اطلاعات، علاوه بر چرخه‌ی ارزیابی- هدایت- پایش- اطلاع‌رسانی شامل فرایند تضمین نیز هست. این فرایند یک نظر عینی و مستقل در خصوص راهبری امنیت اطلاعات و سطح به‌دست‌آمده ارائه می‌کند.

۵-۳) تحلیل محتوی استانداردهای IDS 1338 و 27014

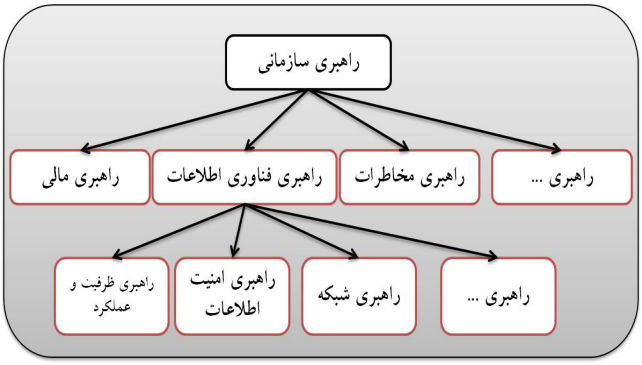
هر سازمان از مدل‌های حاکمیت متعددی بهره می‌گیرد که حاکمیت سازمانی، حاکمیت فناوری اطلاعات و حاکمیت امنیت اطلاعات بخشی از آن هستند. هر مدل حاکمیت مؤلفه‌ی جدایی‌ناپذیر از حاکمیت سازمان است که اهمیت هم‌راستایی با اهداف کسب‌وکار را نشان می‌دهد. هیئت رییسه‌ی سازمان باید یک دیدگاه کل‌نگر و یکپارچه از مدل حاکمیت داشته باشد.

محدوده‌ی حاکمیت فناوری اطلاعات، منابع موردنیاز جهت اکتساب، پردازش، ذخیره‌سازی و انتشار اطلاعات است. محدوده‌ی حاکمیت امنیت اطلاعات محرمانگی، یکپارچگی و دسترس‌پذیری است. هر دو مدل باید شامل چرخه‌ی ارزیابی- هدایت- پایش باشند. لیکن حاکمیت امنیت اطلاعات فرایند داخلی اطلاع‌رسانی نیز شامل می‌شود.

۶) مدل هم‌پوشانی استانداردهای مدیریت و حاکمیت فناوری اطلاعات

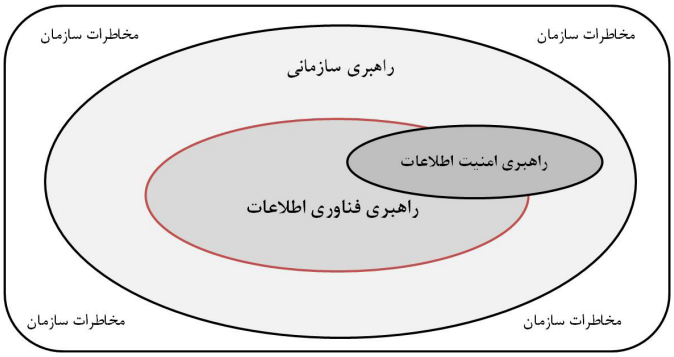
حاکمیت و مدیریت اجزای جدانشدنی هدایت سازمان هستند. لیکن وجود استانداردهای متعدد در این حوزه و عدم تبیین ارتباط بین آن‌ها سبب‌شده تا انتخاب استاندارد مناسب و هم‌چنین اثربخشی به‌کارگیری آن کاهش یابد. در این بخش تحقیق، با توجه به تحلیل محتوای انجام‌شده و در نظر گرفتن نیازمندی‌های سازمان، ارتباط بین این استانداردها بیان‌شده است.

در یک نمای کلی شکل زیر ارتباط بین مفهوم حاکمیت سازمانی با حاکمیت مالی، حاکمیت فناوری اطلاعات، حاکمیت مخاطرات سازمان و ... را نشان می‌دهد.



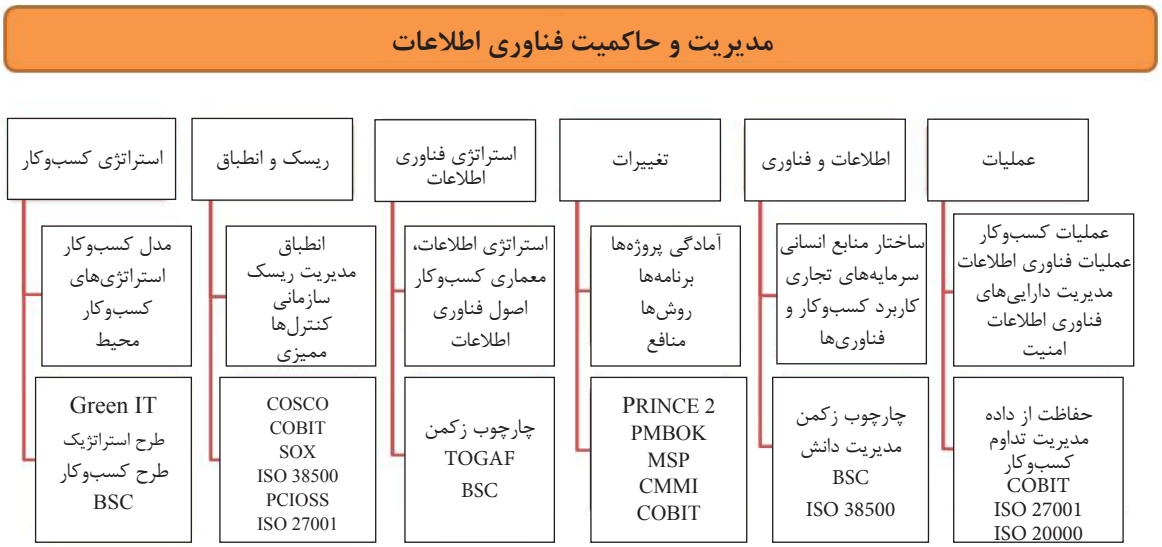
شکل ۶: نمای اول از مدل هم‌پوشانی

در شکل زیر با تمرکز روی حاکمیت سازمانی، حاکمیت فناوری اطلاعات و حاکمیت امنیت اطلاعات ارتباط این سه حوزه با یکدیگر نمایش داده شده‌اند. مدل حاکمیت در هر یک از سه حوزه، در محیط پر از مخاطره سازمان شکل گرفته و باید پاسخگوی مخاطرات باشد.



شکل ۷: نمای دوم از مدل هم‌پوشانی

شکل ۸ مدل هم‌پوشانی استانداردها، الگوهای برتر و چارچوب‌های مدیریت و حاکمیت فناوری اطلاعات را در ۶ وجه استراتژی فناوری اطلاعات، مدیریت مخاطرات، استراتژی کسب‌وکار، عملیات، توازن فناوری با کسب‌وکار و مدیریت تغییرات ارائه می‌کند. لایه‌ی دوم این مدل مهم‌ترین موضوعات مطرح در هر وجه و لایه‌ی سوم، استانداردها و چارچوب‌های کاربردی جهت تحقق لایه‌ی اول را نشان می‌دهد. این مدل از چارچوب حاکمیت فناوری اطلاعات ارائه‌شده توسط Calder-Moir در سال ۲۰۰۵ اقتباس‌شده و تغییرات و اصلاحاتی در آن ایجادشده است. در بهره‌گیری از این مدل باید به هم‌پوشانی دستاوردهای ناشی از به‌کارگیری هر یک از ابزارها و مراجع ذکرشده در لایه سوم توجه کرد.



۷) جمع‌بندی و نتیجه‌گیری

چتر فعالیت‌های فنی و عامل اساسی اثربخشی آن‌ها، وجود نظام مدیریتی کارآمد است. درک صحیح از ماهیت سازمان و انتخاب استاندارد مناسب سبب می‌شود تا منابع سازمان در مسیر صحیح هزینه شوند. نقش فناوری اطلاعات در سازمان‌ها و اثرات انکارناپذیر آن در تغییر سازوکار مدیریت و حتی ایجاد تئوری‌های جدید مدیریت، سازمان را در برابر گزینه‌های جدیدی از نظام مدیریتی و سازوکار حاکمیت قرار می‌دهد.

این مقاله با بهره‌گیری از نتایج مطالعات کتابخانه‌ای ضمن معرفی استانداردهای حاکمیت و مدیریت فناوری اطلاعات که تاکنون تدوین و منتشر شده‌اند، با استفاده از روش تحلیل محتوا، مقایسه تطبیقی و عملیاتی آن‌ها را انجام داده است.

بررسی‌های انجام‌شده در محتوی استانداردها نشان می‌دهد تعدد استقرار استانداردها در یک سازمان نه تنها سبب توسعه و افزایش کارایی و اثربخشی سازمان نمی‌شود، بلکه موجب سردرگمی و اتلاف منابع نیز خواهد شد. از این‌رو انتخاب استاندارد مناسب اهمیت ویژه‌ای دارد.

مدل ارتباط و هم‌پوشانی ارائه‌شده در شکل‌های ۶ و ۷ و ۸، نمای کلی از کارکرد هر یک از موضوعات مورد تحقیق و مراجع موجود نمایش می‌دهد که به سازمان در انتخاب استاندارد متناسب با ماهیت کسب‌وکار خود کمک می‌کند.

گرچه در مدل ارائه شده، ارتباط بین استانداردها، تجربیات برتر و چارچوب‌های موجود با یکدیگر از جمله ITIL، COBIT و ... بیان‌شده است، لیکن مطالعات دقیق‌تر در مفاهیم و کاربردهای هریک ضروری است.

۸) منابع و مراجع

1. Official Website of International Standardization Organization. WWW. ISO. ORG.

۲. احمد بدری- مبانی و ضرورت رکتی- احمد بدری- مجموعه‌ی مقالات همایش راهبری شرکتی- شرکت بورس و اوراق بهادار تهران

3. ISO 38500: 2008: Corporate Governance of Information Technology

4. IDS-ISO-20000-2,Information technology - Service management - Part 2: Guidance on the. application of service management systems,Second edition 2012-02-15.

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

6. ISO/IEC 27001: 2013, Information technology- Security techniques- Information security management systems- Requirements, 2013.

7. ISO/IEC 27002: 2013, Information technology- Security techniques- Code of practice for information security management, 2013.

8. ISO/IEC 27014:2013, Information technology- Security techniques- Governance of information security.

9. ISO/IEC 27000, Information technology- Security Techniques- Information Security Managementsystems- Overview and Vocabulary, 2014

10. Zimmerli, W and et al. (2007), Corporate Ethics and Corporate Governance, Springer, Berlin.