INSO-ISO-IEC

27014

1st. Edition
Identical with

ISO/IEC 27014:2013
2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ایران-ایزو-آی ای سی

۲۷۰۱۴

چاپ اول

۱۳۹۲

فناوری اطلاعات – فنون امنیتی - حاکمیت امنیت اطلاعات

Information Technology – Security techniques – Governance of information security

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization

2 - International Electrotechnical Commission

3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)

4 - Contact point

5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات - فنون امنیتی - حاکمیت امنیت اطلاعات »

رئیس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤل سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار)	مدیرکل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء : (اسامی به ترتیب حروف الفبا)	
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس مخابرات ایران
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
سراج زاده، سید هادی (فوق لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
فولادیان، مجید (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات - فنون امنیتی - حاکمیت امنیت اطلاعات » که پیش نویس آن در کمیسیون های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و بیست و سومین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۹۲/۱۱/۲۸ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین ، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد .

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ISO/IEC 27014:2013, Information technology — Security techniques — Governance of information security

فناوری اطلاعات – فنون امنیتی – حاکمیت امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ، تعیین راهنمایی در مورد مفاهیم و اصول حاکمیت امنیت اطلاعات است که از طریق آن سازمان‌ها می‌توانند فعالیت‌هایی مرتبط با امنیت اطلاعات در سازمان را ارزشیابی[۱]، هدایت[۲]، پایش[۳] و ارتباط[۴] کنند.

این استاندارد ملی در تمامی سازمان‌ها در هر اندازه و نوعی کاربردپذیر است.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱، فناوری اطلاعات – فنون امنیتی – سامانه‌های امنیت اطلاعات - مرور کلی و واژگان

۳ اصطلاحات وتعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱، اصطلاحات و تعاریف زیر نیز به کار می‌رود.

۳-۱

مدیریت اجرایی

فرد یا گروهی از افراد هستند که مسؤولیت پیاده‌سازی راهبردها و خط‌مشی‌ها از طرف هیأت حاکمه[۵] را دارند تا اهداف سازمان را به انجام برسانند.

---

1 - Evaluate
2 - Direct
3 - Monitor
4 - Communicate
5 - Governing body

یادآوری ۱- مدیریت اجرایی بخشی از مدیریت عالی را تشکیل می‌دهند: برای شفافیت نقش‌ها، این استاندارد میان دو گروه در مدیریت رده بالا تمایز قائل می‌شود: هیأت حاکمه و مدیریت اجرایی.

یادآوری ۲- مدیریت اجرایی می‌تواند شامل مدیر اجرایی (CEO)[1] ، روسای سازمان‌های دولتی، مدیر ارشد مالی(CFO)[2] ، مدیر ارشد عملیات(COO)[3] ، مدیر ارشد اطلاعات(CIO)[4] ، مدیر ارشد امنیت اطلاعات(CISO)[5] و نقش‌های مشابه شود.

۲-۳
هیأت حاکمه

فرد یا گروهی از افراد هستند که در قبال عملکرد و انطباق سازمان مسؤول می‌باشند.

یادآوری- هیأت حاکمه بخشی از مدیریت رده بالا را تشکیل می‌دهد: جهت شفافیت نقش‌ها، این استاندارد میان دو گروه در مدیریت رده بالا تمایز قائل می‌شود: هیأت حاکمه و مدیریت اجرایی.

۳-۳
حاکمیت امنیت اطلاعات

سامانه‌ای است که فعالیت‌های امنیت اطلاعات سازمان از طریق آن هدایت و کنترل می‌شود.

۴-۳
ذی‌نفع

هر فرد یا سازمانی است که می‌تواند بر فعالیت سازمان اثر بگذارد، از آن تاثیر پذیرد یا برداشت کند که از آن تاثیر می‌پذیرد.

یادآوری- تصمیم‌گیرندگان می‌توانند ذی‌نفع باشند.

۴ مفاهیم

۱-۴ عمومی

حاکمیت امنیت اطلاعات نیاز به هم‌راستا نمودن اهداف و راهبردهای امنیت اطلاعات با اهداف و راهبردهای کسب‌وکار و انطباق آن‌ها با قانون، مقررات و قراردادها دارد. توصیه می‌شود این مسأله از طریق یک رویکرد مدیریت مخاطره ارزشیابی، تحلیل و پیاده‌سازی شده و به وسیله یک رویه کنترل داخلی پشتیبانی شود.

هیأت حاکمه در نهایت پاسخگوی تصمیمات و عملکرد سازمان به حساب می‌آید. در خصوص امنیت اطلاعات، تمرکز اصلی هیأت حاکمه بر این است تا اطمینان حاصل کنند که رویکرد سازمان در قبال امنیت اطلاعات کارا، اثربخش، قابل قبول و در راستای اهداف و راهبردهای کسب‌وکار معین شده با توجه به انتظارات ذی‌نفعان است. ذی‌نفعان مختلف می‌توانند ارزش‌ها و نیازهای متفاوتی داشته باشند.

---

1 - Chief executive officer
2 - Chief financial officer
3 - Chief operating officer
4 - Chief information officer
5 - Chief information security officer

۲-۴ اهداف

اهداف حاکمیت امنیت اطلاعات عبارتند از:

- هم‌راستا نمودن اهداف و راهبرد امنیت اطلاعات با اهداف و راهبرد کسب‌وکار (هم‌راستایی راهبردی)
- ارزش دادن به هیأت حاکمه و ذی‌نفعان (ارزش دادن)
- اطمینان حاصل کردن از این که مخاطره امنیتی به طور کافی نشان داده می‌شود (پاسخگویی)[1]

۳-۴ برآمدهای مطلوب

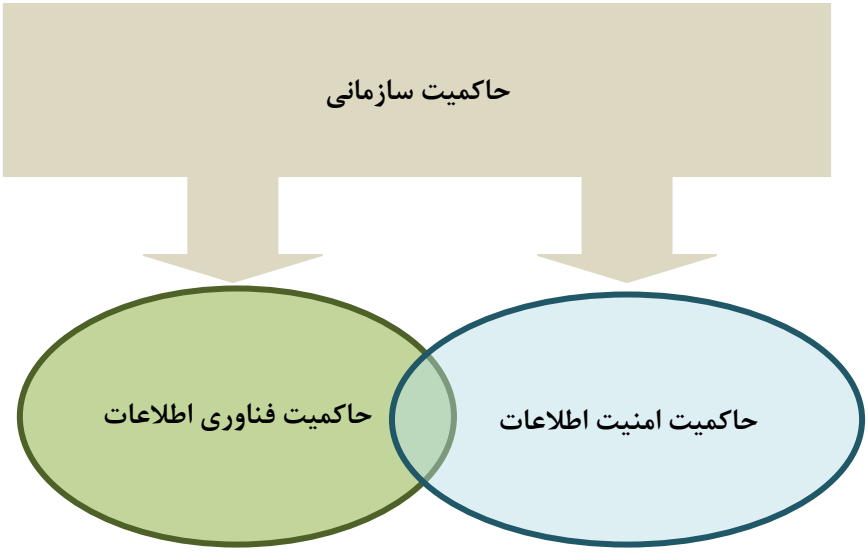
برآمدهای مطلوب از پیاده‌سازی موثر حاکمیت امنیت اطلاعات شامل موارد زیر می‌شود:

- دیدگاه هیأت حاکمه بر وضعیت امنیت اطلاعات
- رویکرد چابک در مورد تصمیم‌گیری در مورد مخاطره‌های اطلاعاتی
- سرمایه‌گذاری کارا و اثربخش در امنیت اطلاعات
- انطباق با الزامات خارجی (قانونی، تنظیم مقرراتی، قراردادی)

۴-۴ رابطه

چندین حوزه مدل حاکمیت دیگر نیز در درون سازمان وجود دارد، مانند حاکمیت فناوری اطلاعات و حاکمیت سازمانی. هر مدل حاکمیت مولفه‌ای جدایی‌ناپذیر از حاکمیت یک سازمان است که اهمیت هم‌راستایی با اهداف کسب‌وکار را نشان می‌دهد. برای هیأت حاکمه مفید است تا یک دید کل نگر و یکپارچه از مدل حاکمیت ایجاد کند که توصیه می‌شود حاکمیت امنیت اطلاعات قسمتی از آن باشد. محدوده‌های مدل‌های حاکمیت گاهی اوقات هم‌پوشانی دارند. برای مثال، رابطه بین حاکمیت امینت اطلاعات و حاکمیت فناوری اطلاعات در شکل ۱ نمایش داده شده است.

1 - Accountability



شکل ۱- رابطه میان حاکمیت امنیت اطلاعات و حاکمیت فناوری اطلاعات

در حالی که محدوده فراگیر حاکمیت فناوری اطلاعات منابع مورد نیاز جهت اکتساب، پردازش، ذخیره‌سازی و انتشار اطلاعات را هدف گرفته است، محدوده حاکمیت امنیت اطلاعات محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات را می‌پوشاند. هر دو طرحواره[1] حاکمیت لازم است توسط فرآیندهای حاکمیتی زیر، سامان‌دهی شوند: ارزشیابی، جهت‌دهی، پایش(EDM)[2]. با این وجود، حاکمیت امنیت اطلاعات به فرآیند داخلی اضافی «ارتباط» نیز نیاز دارد.

وظایف مورد انتظار از هیأت حاکمه جهت برقراری حاکمیت امنیت اطلاعات در بند ۵ توضیح داده می‌شوند. وظایف حاکمیتی علاوه بر سایر مجموعه استانداردهای خانواده سامانه‌های مدیریت امنیت اطلاعات(ISMS)[3]، همان طور که در کتاب‌نامه بدان اشاره شده است، به الزامات مدیریتی تعیین شده در استاندارد ISO/IEC[4] 27001 نیز مرتبط هستند.

۵ اصول و فرآیندها

۵-۱ مرور کلی

این بند به توصیف اصول و فرآیندهایی می‌پردازد که با هم حاکمیت امنیت اطلاعات را شکل می‌دهند. اصول حاکمیت امنیت اطلاعات قواعد پذیرفته شده برای اقدامات یا رفتار حاکمیتی هستند که به عنوان راهنمایی برای پیاده‌سازی حاکمیت نقش ایفا می‌کنند. فرآیند حاکمیت امنیت اطلاعات مجموعه‌ای از وظایف و روابط متقابل آن‌ها را توصیف می‌کند که حاکمیت امنیت اطلاعات را فراهم می‌سازد. این فرآیند همچنین رابطه

1 - Scheme
2 - Evaluate, Direct, Monitor
3 - Information Security Management Systems
۴ - استاندارد بین‌المللی ISO/IEC 27001:2005 در سال ۱۳۸۷، با شماره ملی ۲۷۰۰۱ منتشر شده است.

میان حاکمیت و مدیریت امنیت اطلاعات را نشان می‌دهد. این دو مولفه در بندهای زیر توضیح داده می‌شوند.

۲-۵ اصول

برآورده ساختن نیازهای ذی‌نفعان و ارزش دادن به هر یک از آن‌ها برای موفقیت امنیت اطلاعات در بلند مدت ضروری است. برای دستیابی به هدف حاکمیتی هم‌راستای نزدیک با امنیت اطلاعات با اهداف کلی کسب‌وکار و ارزش دادن برای ذی‌نفعان، این زیربند شش اصل عمل‌گرا[1] را معین می‌کند.

این اصول مبنای خوبی را برای پیاده‌سازی فرآیندهای حاکمیت امنیت اطلاعات فراهم می‌کنند. توضیح هر اصل اشاره دارد به آنچه که به‌انجام آن توصیه می‌شود، اما تعیین نمی‌کند که اصول به چه نحوی، در چه زمانی و توسط چه شخصی باید پیاده‌سازی شوند زیرا این جنبه‌ها به ماهیت سازمان پیاده‌ساز اصول وابسته هستند. توصیه می‌شود هیأت حاکمه به کارگیری این اصول را لازم بداند و شخصی را با مسؤولیت، پاسخگویی و اختیارات لازم برای پیاده‌سازی آن‌ها مامور کند.

اصل ۱: برقراری امنیت اطلاعات در سطح سازمان

توصیه می‌شود حاکمیت امنیت اطلاعات تضمین کند که فعالیت‌های امنیت اطلاعات فراگیر و یکپارچه هستند. توصیه می‌شود امنیت اطلاعات در سطح سازمانی کنترل شود و جنبه‌های کسب‌وکار، امنیت اطلاعات و سایر جنبه‌های مرتبط در تصمیم‌گیری‌ها لحاظ شوند. توصیه می‌شود فعالیت‌های مرتبط با امنیت منطقی و فیزیکی نیز به دقت هماهنگ شوند.

برای برقراری امنیت در سطح سازمان توصیه می‌شود مسؤولیت و جوابگویی در قبال امنیت اطلاعات در کل گستره فعالیت‌های سازمان برقرار شود. این مسأله به طور معمول از مرزهای سازمان فراتر می‌رود، به عنوان مثال به دلیل ذخیره‌سازی یا انتقال اطلاعات توسط طرفین خارجی.

اصل ۲: پذیرش رویکرد مبتنی بر مخاطره

توصیه می‌شود حاکمیت امنیت اطلاعات بر پایه تصمیم‌های مبتنی بر مخاطره بنا شود. توصیه می‌شود سطح قابل قبول برای امنیت بر پایه مخاطره‌پذیری سازمان مشخص شود، از جمله از دست دادن مزیت رقابتی، مخاطره‌های مسؤولیت و انطباق، اختلالات عملیاتی، آسیب به اعتبار و ضرر مالی.

جهت پذیرش مدیریت مخاطره اطلاعات متناسب با سازمان، توصیه می‌شود آن را سازگار و یکپارچه با رویکرد مدیریت مخاطره کلی سازمان انتخاب کرد. توصیه می‌شود سطوح قابل قبول امنیت اطلاعات بر اساس مخاطره‌پذیری سازمان تعریف شوند، از جمله از دست دادن مزیت رقابتی، مخاطره مسؤولیت و انطباق،

1 - Action-oriented principles

اختلالات عملیاتی، آسیب به اعتبار و ضرر مالی. توصیه می‌شود هیأت حاکمه منابع مناسب جهت پیاده‌سازی مدیریت امنیت اطلاعات را اختصاص دهد.

اصل ۳: مشخص کردن جهت تصمیم‌های سرمایه‌گذاری

توصیه می‌شود حاکمیت امنیت اطلاعات یک راهبرد سرمایه‌گذاری امنیت اطلاعات را بر پایه نتایج کسب‌وکار به دست آمده برقرار کند که در کوتاه مدت و بلند مدت منجر به هماهنگ‌سازی میان الزامات کسب‌وکار و امنیت اطلاعات شود و از این رو نیازهای کنونی و در حال افزایش ذی‌نفعان را برآورده سازد.

جهت بهینه‌سازی سرمایه‌گذاری‌های امنیت اطلاعات در پشتیبانی از اهداف سازمانی، توصیه می‌شود هیأت حاکمه تضمین کند که امنیت اطلاعات با فرآیندهای سازمانی موجود برای مخارج سرمایه‌ای و عملیاتی، الزامات قانونی و مقرراتی و گزارش مخاطره یکپارچه است.

اصل ۴: تضمین انطباق با الزامات داخلی و خارجی

توصیه می‌شود هیأت حاکمه تضمین کند که خط‌مشی‌ها و رویه‌های امنیت اطلاعات با قوانین و مقررات الزام‌آور و علاوه بر آن الزامات کسب‌وکار یا قراردادی تعهدآور و سایر الزامات داخلی یا بیرونی مرتبط انطباق دارند.

جهت رسیدگی به موضوع انطباق، توصیه می‌شود هیأت حاکمه با انجام ممیزی‌های امنیتی مستقل اطمینان حاصل کند که فعالیت‌های امنیت اطلاعات به طور رضایت بخشی الزامات درونی و خارجی را برآورده می‌سازند.

اصل ۵: ایجاد یک محیط امنیتی مثبت

توصیه می‌شود حاکمیت اطلاعات بر پایه رفتار انسانی ساخته شود، از جمله نیازهای در حال تکامل تمامی ذی‌نفعان، زیرا رفتار انسانی یکی از عناصر بنیادین برای پشتیبانی از سطح امنیت اطلاعات مناسب است. اگر اهداف، نقش‌ها، مسؤولیت‌ها و منابع به طور مناسب هماهنگ نشوند ممکن است با یکدیگر تضاد پیدا کنند که منجر به شکست در برآورده ساختن اهداف کسب‌وکار می‌شود. از این رو، هماهنگ‌سازی و جهت‌گیری هم‌راستا میان ذی‌نفعان مختلف بسیار مهم است.

جهت برقراری فرهنگ مثبت امنیت اطلاعات، توصیه می‌شود هیأت حاکمه هماهنگ‌سازی فعالیت‌های ذی‌نفعان را لازم بداند و آن را ترویج و پشتیبانی کند تا به یک جهت‌گیری منسجم برای امنیت اطلاعات دست یابد. این موضوع برنامه‌های ارائه آموزش، پرورش و آگاهی امنیتی را پشتیبانی می‌کند.

اصل ۶: بازنگری عملکرد در ارتباط با نتایج کسب‌وکار

توصیه می‌شود هیأت حاکمه تضمین کند که رویکرد اتخاذ شده جهت محافظت از اطلاعات برای پشتیبانی از سازمان و فراهم آوردن سطوح امنیت اطلاعات توافق شده، مناسب است. توصیه می‌شود عملکرد امنیتی در سطوح مورد نیاز برای برآورده ساختن الزامات فعلی و آینده کسب‌وکار نگه داشته شود.

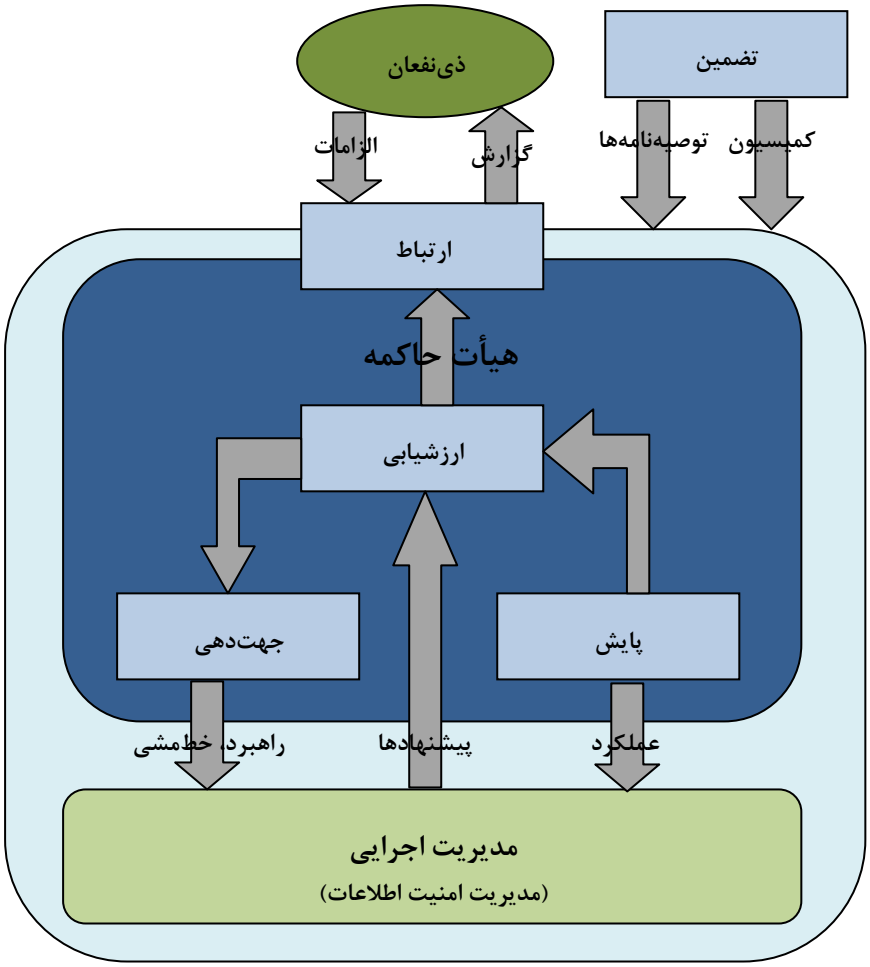
جهت بازنگری عملکرد امنیت اطلاعات از دیدگاه حاکمیت توصیه می‌شود هیأت حاکمه عملکرد امنیت اطلاعات را علاوه بر اثربخشی و کارایی کنترل‌های امنیتی، در ارتباط با تاثیر آن بر کسب‌وکار نیز ارزشیابی کند. این امر با الزام انجام بازنگری‌هایی بر برنامه‌های سنجش عملکرد برای طرح‌های پایش، ممیزی و بهبود می‌تواند میسر شود و از این طریق عملکرد امنیت اطلاعات را به عملکرد کسب‌وکار پیوند می‌دهد.

۵-۳ فرآیندها

۵-۳-۱ مرور کلی

هیأت حاکمه فرآیندهای «ارزشیابی»، «جهت‌دهی»، «پایش» و «ارتباط» را جهت حاکم کردن امنیت اطلاعات اجرا می‌کند. علاوه بر این، فرآیند «تضمین[1]» یک نظر مستقل و عینی در خصوص حاکمیت امنیت اطلاعات و سطح به دست آمده را ارائه می‌کند. شکل ۲ رابطه میان این فرآیندها را نشان می‌دهد.

1 - Assure



شکل ۲- پیاده‌سازی مدل حاکمیت برای امنیت اطلاعات

۵-۳-۲ ارزشیابی

«ارزشیابی» فرآیند حاکمیتی است که میزان واقعی و پیش‌بینی شده دست‌یابی به اهداف امنیتی را بر اساس فرآیندهای فعلی و تغییرات برنامه‌ریزی شده بررسی می‌کند و معین می‌کند جهت بهینه‌سازی دستیابی به اهداف راهبردی در آینده چه تنظیماتی مورد نیاز است.

توصیه می‌شود هیأت حاکمه برای اجرای فرآیند «ارزشیابی» اقدامات زیر را دنبال کند:

- تضمین اینکه ابتکارات[1] کسب‌وکار موضوعات امنیت اطلاعات را در نظر می‌گیرند.
- واکنش به نتایج عملکرد امنیت اطلاعات، اولویت‌بندی و آغاز اقدامات لازم

توصیه می‌شود مدیریت اجرایی برای فراهم کردن فرآیند «ارزشیابی» اقدامات زیر را دنبال کند:

- تضمین اینکه امنیت اطلاعات به طور مناسب از اهداف کسب‌وکار پشتیبانی می‌کند.
- ارسال پروژه‌های جدید امنیت اطلاعات با اثر قابل‌توجه به هیأت حاکمه.

1 - Initiative

۵-۳-۳ جهت‌دهی

«جهت‌دهی» فرآیند حاکمیتی است که هیأت حاکمه از طریق آن اهداف و راهبردهای امنیت اطلاعاتی که لازم است پیاده‌سازی شوند را هدایت می‌کند. این هدایت می‌تواند شامل تغییرات در سطوح منابع، اختصاص منابع، اولویت‌بندی فعالیت‌ها، تصویب خط‌مشی‌ها، پذیرش مخاطره مواد و برنامه‌های مدیریت مخاطره شود.
توصیه می‌شود هیأت حاکمه برای اجرای فرآیند «جهت‌دهی» اقدامات زیر را دنبال کند:

- مشخص کردن میزان مخاطره‌پذیری سازمان
- تصویب راهبرد و خط‌مشی امنیت اطلاعات
- اختصاص سرمایه و منابع کافی.

توصیه می‌شود مدیریت اجرایی برای فراهم کردن فرآیند «جهت‌دهی» اقدامات زیر را دنبال کند:

- تهیه و پیاده‌سازی راهبرد و خط‌مشی امنیت اطلاعات،
- هم‌راستا سازی اهداف امنیت اطلاعات با اهداف کسب‌وکار
- ترویج فرهنگ مثبت امنیت اطلاعات

۵-۳-۴ پایش

«پایش» فرآیند حاکمیتی است که به هیأت حاکمه امکان می‌دهد دستیابی به اهداف راهبردی را ارزشیابی کند.
توصیه می‌شود هیأت حاکمه برای اجرای فرآیند «پایش» اقدامات زیر را دنبال کند:

- ارزشیابی اثربخشی فعالیت‌های مدیریت امنیت اطلاعات
- تضمین انطباق با الزامات داخلی و بیرونی
- در نظر گرفتن تغییرات در محیط‌های کسب‌وکار، قانونی و مقرراتی و تاثیرات احتمالی آن‌ها بر مخاطره اطلاعات.

توصیه می‌شود مدیریت اجرایی برای فراهم کردن فرآیند «پایش» اقدامات زیر را دنبال کند:

- انتخاب معیارهای عملکرد مناسب از دیدگاه کسب‌وکار،
- فراهم کردن بازخورد در مورد نتایج عملکرد امنیت اطلاعات به هیأت حاکمه شامل عملکرد اقداماتی که از پیش توسط هیأت حاکمه شناسایی شده‌اند و اثر آن‌ها بر سازمان،
- آگاه ساختن هیأت حاکمه از وقایع جدید تاثیر گذار بر مخاطره‌های اطلاعاتی و امنیت اطلاعات.

۵-۳-۵ ارتباط

«ارتباط» فرآیند حاکمیت دو طرفه‌ای است که هیأت حاکمه و ذی‌نفعان از طریق آن اطلاعات در مورد امنیت اطلاعات را متناسب با نیازهای خاص خود رد و بدل می‌کنند.

یکی از روش‌های «ارتباط» گزارش وضعیت امنیت اطلاعات ست که فعالیت‌ها و موضوعات امنیت اطلاعات را برای ذی‌نفعان توضیح می‌دهد، که نمونه‌هایی از آن در پیوست‌های الف و ب نشان داده شده‌اند.
توصیه می‌شود هیأت حاکمه برای اجرای فرآیند «ارتباط» اقدامات زیر را دنبال کند:

- گزارش به ذی‌نفعان بیرونی که سازمان در سطحی از امنیت اطلاعات متناسب با ماهیت کسب‌وکار خود عمل می‌کند.

- مطلع ساختن مدیریت اجرایی از نتایج هر گونه بازنگری بیرونی که مشکلاتی در امنیت اطلاعات شناسایی کرده‌اند و درخواست اقدامات اصلاحی

- شناسایی الزامات مقرراتی، انتظارات ذی‌نفعان و نیازهای کسب‌وکار با توجه به امنیت اطلاعات.

توصیه می‌شود مدیریت اجرایی برای فراهم کردن فرآیند «ارتباط» اقدامات زیر را دنبال کند:

- آگاه ساختن هیأت حاکمه در مورد هر گونه موضوعی که نیازمند توجه و احتمالا تصمیم‌گیری آن‌ها باشد

- راهنمایی ذی‌نفعان مرتبط در مورد جزئیات اقداماتی که باید در جهت پشتیبانی از دستورالعمل‌ها و تصمیمات هیأت حاکمه انجام دهند.

۵-۳-۶ تضمین

«تضمین» فرآیند حاکمیتی است که هیأت حاکمه از طریق آن فرمان به انجام ممیزی، بازنگری یا صدور گواهی مستقل و عینی می‌دهد.این اقدامات اهداف و فعالیت‌های مرتبط با اجرای فعالیت‌های حاکمیت و انجام عملیات به منظور دستیابی به سطح امنیت اطلاعات مطلوب را شناسایی و تایید می‌کنند.
توصیه می‌شود هیأت حاکمه برای اجرای فرآیند «تضمین» اقدامات زیر را دنبال کند:

- کمیسیون آرا نظرات مستقل و عینی بر نحوه مطابقت با مسؤولیت خود برای دستیابی به سطح امنیت اطلاعات مطلوب

توصیه می‌شود مدیریت اجرایی برای فراهم کردن فرآیند «تضمین» اقدامات زیر را دنبال کند:

- پشتیبانی از ممیزی، بازنگری و صدور گواهی دستور داده شده توسط هیأت حاکمه.

پیوست الف

(اطلاعاتی)

مثالی از وضعیت امنیت اطلاعات

یک سازمان می‌تواند یک گزارش وضعیت امنیت اطلاعات تهیه کند و آن را به عنوان ابزار ارتباطی برای امنیت اطلاعات در اختیار ذی‌نفعان قرار دهد.

توصیه می‌شود سازمان قالب و محتوای گزارش وضعیت امنیت اطلاعات را انتخاب و در مورد آن تصمیم‌گیری کند. پیوست الف، مثالی است که اعلامیه ممیزی امنیت اطلاعات را برای ابراز رضایت به کار می‌گیرد.

جدول ۱- وضعیت امنیت اطلاعات

مدیریت، کنترل‌ها و رویه‌های امنیت اطلاعاتی را که بر پایه ضوابط در xyz (به عنوان مثال مجموعه ISO/IEC 27000، CobiT) بنا شده‌اند، در دوره mmm تا nnn در رویه‌های عملیاتی سازمان و سامانه‌های پشتیبانی شده توسط کنترل‌های مدیریتی سطح بالا که با اثر بخشی کافی به اجرا در آمده‌اند را تایید می‌نماید. این عملکرد، تضمین قابل قبولی فراهم می‌آورد که اهداف کنترل امنیت اطلاعات تعریف شده در ارتباط با محرمانگی، یکپارچگی و دسترس‌پذیری حاصل شده‌اند. مدیریت به شرکت ABC، که به عنوان ممیز امنیت اطلاعات خارجی تعیین شده است، نامه‌ای با این محتوا ارائه کرده است. شرکت ABC توسط هیأت مدیره جهت بررسی ادعاهای مدیریت در خصوص کنترل امنیت اطلاعات انتصاب شد. بررسی‌های آن‌ها مطابق با استانداردهای شناخته شده انجام شد و شامل ارزشیابی اثربخشی طراحی و اجرای کنترل‌های امنیت اطلاعات و فرآیندها از طریق آزمایش‌های موردی بود. در این ارتباط، شرکت ABC نظر خود را به مدیریت ارائه داد مبنی بر اینکه نتایج آزمایش‌های آن‌ها نشان می‌دهد که با در نظر داشتن انتظارات معین شده بر مبنای معیارهای مدیریت شناسایی شده از xyz (به عنوان مثال مجموعه IS0/IEC 27000، CobiT)، کنترل‌ها از جنبه اصولی موثر بوده‌اند. نامه ادعاهای کامل مدیریت و گزارش ممیزی خارجی با تمامی انتظارات شناسایی شده در ارتباط با کنترل‌های امنیت اطلاعات با کمیته ممیزی به بحث گذاشته شده است و به همه اعضای هیأت مدیره ارائه شده است. در صورت درخواست ذی‌نفعان این مطالب به آن‌ها ارائه خواهد شد.

یادآوری- **«nnn»**، **«mmm»**، **«ABC»** و **«xyz»** به جای تاریخ و نام‌های واقعی به کار گرفته شده‌اند و باید در گزارش‌های واقعی با تاریخ و نام‌های دقیق جایگزین شوند.

پیوست ب
(اطلاعاتی)
مثالی تفصیلی از وضعیت امنیت اطلاعات

پیوست ب مثالی از یک گزارش وضعیت امنیت اطلاعات نشان دهنده محتوای تفصیلی است. این مثال به طور خاص برای سازمان‌هایی که انتظار دارند با تاکید بر امنیت اعتبار خود را گسترش دهند، کاربرد دارد، به عنوان مثال کسب‌وکارهای حوزه فناوری اطلاعات و ارتباطات. شفافیت رویکرد سازمان در برابر مخاطره‌های امنیتی و آشکارسازی مناسب نیز در افزایش اعتماد تاثیرگذار است. از طریق این فعالیت‌ها می‌توان آگهی عمومی را میان ذی‌نفعان به اشتراک گذاشت.

جدول ۲- وضعیت تفصیلی امنیت اطلاعات

معرفی

- **محدوده** (راهبرد، خط‌مشی‌ها، استانداردها)، **مرزبندی** (واحدهای جغرافیایی/سازمانی)، **دوره‌های پوشش داده شده** (ماهانه، سه ماهه، شش ماهه، سالانه)

وضعیت کلی

- **رضایت‌بخش، تا حدی رضایت‌بخش، غیر رضایت‌بخش**

به روز رسانی‌ها (در جای مناسب و مرتبط)

- **پیشرفت در جهت رسیدن به راهبرد امنیت اطلاعات**

عناصر پایان یافته، در دست اجرا، طراحی شده

- **تغییرات در سامانه مدیریت امنیت اطلاعات**

ممیزی خط‌مشی ISMS، ساختار سازمانی پیاده‌سازی ISMS (شامل واگذاری مسؤولیت‌ها)

- **پیشرفت به سمت صدور گواهی**

صدور مجدد گواهی ISMS، ممیزی‌های امنیت اطلاعات گواهی شده

- **بودجه‌بندی/جذب نیرو/آموزش**

وضعیت مالی، کفایت تعداد، مهارت‌های امنیت اطلاعات

- **سایر فعالیت‌های امنیت اطلاعات**

مشارکت مدیریت پیوستگی کسب‌وکار، برنامه‌های آگاه‌سازی، همکاری برای ممیزی داخلی/خارجی

موضوعات قابل‌توجه (در صورت وجود)

- **نتایج بازنگری‌های امنیت اطلاعات**

توصیه‌نامه‌ها، پاسخ‌های مدیریت، طرح‌های اجرایی، تاریخ‌های مورد نظر

- **پیشرفت از لحاظ گزارش‌های اصلی ممیزی داخلی/خارجی**

توصیه‌نامه‌ها، پاسخ‌های مدیریت، طرح‌های اجرایی، تاریخ‌های مورد نظر

- **رخدادهای امنیت اطلاعات**

برآورد اثر، طرح‌های اجرایی، تاریخ‌های مورد نظر

- **(عدم) انطباق با قوانین و مقررات مرتبط**

برآورد اثر، طرح‌های اجرایی، تاریخ‌های مورد نظر

تصمیم‌های مورد نیاز (در صورت نیاز)

- **منابع اضافی**

توانمندسازی امنیت اطلاعات برای پشتیبانی از ابتکارات کسب‌وکار

کتاب‌نامه

[۱] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فن‌آوری اطلاعات - فنون امنیتی - سیستم‌های مدیریت امنیت اطلاعات - الزامات

[۲] استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فن‌آوری اطلاعات - فنون امنیتی - آیین کار مدیریت امنیت اطلاعات

[۳] استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، فن‌آوری اطلاعات – فنون امنیتی – مدیریت مخاطرات امنیت اطلاعات

[۴] استاندارد ملی ایران شماره X.1051: سال ۱۳۸۸ | استاندارد ملی ایران شماره ۲۷۰۱۱: سال ۱۳۸۹، فنون امنیتی – راهنماهای مدیریت امنیت طلاعات برای سازمان‌های ارتباط از راه دور بر پایه استاندارد ISO\IEC 27002

[5] ISO/IEC 38500, Corporate Governance of Information Technology — A Standard for corporate governance of information technology

[6] ITGI, Information Security Governance framework: 2009

[7] ISF, Standard of Good Practice for Information Security: 2011