INSO
20334
1st.Edition
2016

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۲۰۳۳۴
چاپ اول
۱۳۹۴

فناوری اطلاعات – چارچوب مخاطره (ریسک) جرم‌شناسی رقمی (دیجیتالی) از منظر حاکمیت

Information technology — Governance of digital forensic risk framework

ICS: 35.080

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 رسمی‌کشور 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 حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود 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 علمیو تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های 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 می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود . بدین ترتیب، استانداردهایی ملی تلقی می‌شوند 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 می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می‌تواند 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 می‌تواند 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 سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. 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 – چارچوب مخاطره (ریسک) جرم‌شناسی رقمی (دیجیتالی) از منظر حاکمیت »

رئیس :	**سمت و/ یا نمایندگی**
مهرشاد، بتول (فوق‌لیسانس مدیریت اجرایی)	رییس اداره فناوری اطلاعات و ارتباطات اداره کل استاندارد خراسان جنوبی رییس سازمان نظام صنفی رایانه‌ای خراسان جنوبی
دبیر :	
پوررضائی، حدیث (لیسانس مهندسی کامپیوتر، نرم‌افزار)	رییس اداره فناوری اطلاعات و ارتباطات اداره کل استاندارد قزوین
اعضاء :	
آذرکار، علی (فوق‌لیسانس مهندسی کامپیوتر، نرم‌افزار)	نماینده سازمان نظام صنفی و رایانه‌ای استان تهران
اسکندرزاده علمداری، رضا (لیسانس مهندسی کامپیوتر، نرم‌افزار)	مدیر عامل شرکت فنی و مهندسی سامانه‌ساز مروارید
پوررضائی، دنیا (لیسانس مهندسی فناوری اطلاعات)	کارشناس شرکت فنی و مهندسی سامانه‌ساز مروارید
حسن نایبی، زهرا (لیسانس مترجمی زبان انگلیسی)	رئیس اداره توسعه منابع انسانی، بودجه و برنامه‌ریزی اداره کل استاندارد قزوین
رضایی، رامین (لیسانس مهندسی برق، الکترونیک)	معاون طرح و توسعه مرکز تحقیقات صنایع انفورماتیک
زرآبادی، سیده فائزه (لیسانس مهندسی کامپیوتر، سخت‌افزار)	کارشناس اداره کل فناوری اطلاعات قزوین
دوست‌محمدی، وحید (فوق‌لیسانس مهندسی صنایع، فناوری اطلاعات)	نماینده مرکز مدیریت راهبردی افتا

فتوحی، حامد
(فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)
کارشناس فناوری اطلاعات استانداری قزوین

محمدیان، بهزاد
(فوق‌لیسانس مهندسی برق، مخابرات)
نماینده مرکز مدیریت راهبردی افتا

یحیایی، مهری
(لیسانس مهندسی فناوری اطلاعات)
مدیر آزمایشگاه های امنیت و کیفیت نرم‌افزار
مرکز تحقیقات صنایع انفورماتیک

فهرست مندرجات

پیش گفتار

استاندارد "فناوری اطلاعات – چارچوب حاکمیت مخاطره (ریسک) جرم‌شناسی رقمی (دیجیتالی) از منظر حاکمیت" که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده است و درسیصد و نود و هفتمین اجلاس کمیته ملی استاندارد فن آوری اطلاعات مورخ ۹۴/۱۲/۰۵ 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 می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های 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 30121:2015, Information technology - Governance of digital forensic risk framework

مقدمه

سازمان‌ها از هر نوعی، با عوامل و تاثیرات داخلی و خارجی مواجه می‌شوند که می‌تواند منجر به رخداد اقدامات قانونی و تعیین سطح خواسته‌های فناوری اطلاعات (IT)[1] و سامانه‌های اطلاعاتی (IS)[2] مرتبط برای افشای شواهد رقمی شود. رخداد اقدام قانونی ممکن است نتیجه یک رویداد غیر قطعی نامشخص، برنامه‌ریزی نشده یا غیرمنتظره باشد یا ممکن است به‌عنوان یک اقدام برنامه‌ریزی شده علیه کارمندان، رقبا یا تامین‌کنندگان خدمات رخ دهد. مهم بودن یا نبودن مخاطره بستگی به سطح مخاطره و نگرش سازمان به مخاطره دارد. نگرش سازمان به مخاطره در معیارهای مخاطره سازمان منعکس می‌شود. از آنجایی که تقریباً به‌طور قطع شواهد رقم کشف خواهند شد و از این رو در معرض افشای قانونی هستند، بهتر است سازمان‌ها توانایی مقابله با چنین اقدامات قانونی را قبل از رخداد، برنامه‌ریزی کرده و توسعه دهند.

این استاندارد ملی در مورد آماده‌سازی راهبردی هوشمندانه برای رسیدگی رقمی[3] یک سازمان کاربرد دارد. تمهید جرم‌شناسی، اطمینان می‌دهد که سازمان آماده‌سازی راهبردی مناسب و مرتبطی برای پذیرش حوادث بالقوه یک ماهیت مستند را مهیا کرده است. اقدامات ممکن است در نتیجه نقض‌های امنیتی اجتناب‌ناپذیر، کلاهبرداری و اعلان اشتهار رخ دهند. توصیه می‌شود در هر شرایطی فناوری اطلاعات به‌صورت راهبردی برای به بیشینه‌کردن اثربخشی دسترس‌پذیری شواهد، دستیابی و مقرون به صرفه بودن هزینه‌ها توسعه یابد.

مسئولیت هیأت حاکم، ارائه مسیر راهبردی در تمام موارد مربوط به سازمان است. اطلاع‌رسانی به هیأت حاکم توسط اصول تجارب برتر که راهنمای عمومی در مورد مسائل اطمینان و انطباق را ارائه می‌دهد، انجام می‌شود. این اصول ممکن است از احکام قانونی، استانداردها یا الزامات اجتماعی و فرهنگی به‌دست آمده باشند. در این استاندارد ملی، از اصول استاندارد ملی ایران به شماره ۱۲۰۴۷ برای رهنمود تجارب برتر در حاکمیت فناوری اطلاعات استفاده شده است. (بند ۴)

اصول نیاز به پیاده‌سازی دارند. وظایف حاکمیت، ارزیابی پیشنهادها و برنامه‌ها، نظارت بر عملکرد و انطباق و هدایت راهبرد و سیاست‌ها است. ذینفعان یک سازمان ممکن است دستور الزامی/اجباری را برای حاکمیت ارائه دهند و هیأت حاکم مالک نهایی مخاطره است. چارچوب مخاطره جرم‌شناسی رقمی از منظر حاکمیت، توسط مالکان مخاطره با اتخاذ اقدامات مناسب برای اطمینان از مسیر راهبردی سازمان ایجاد می‌شوند. از این رو، هدف راهبردی پیاده‌سازی اصول و اطمینان از آماده‌سازی کافی برای رسیدگی رقم است. (بند ۵)

چارچوب، به فرآیندهای راهبردی برای ارائه مسیر به مدیران اجرایی و مدیران ارشد نیاز دارد. فرآیندهای راهبردی برای اطمینان از حوزه و دامنه کاربرد مناسب انتخاب شده و اصولا شامل بایگانی، کشف، افشا، توانایی و انطباق معیار مخاطره هستند. (بند ۶)

1-Information Technology
2-Information System
3-Digital Investigation

اهداف به‌دست آمده از اصول، از طریق نشانگرهای کلیدی هدف (KGIs)[1] قابل اندازه‌گیری هستند، اهداف راهبردی به‌دست آمده از راهبردها از طریق نشانگرهای کلیدی عملکرد (KPIs)[2] و اختلاف بین اندازه‌گیری‌های (KGIs) و (KPIs) نشانگری از عملکرد کسب وکار سازمان است (KBIs)[3]. (بند ۷)

پیشنهاد می‌شود این استاندارد ملی همراه با واژگان موجود در راهنمای ISO Guide 73:2009 ؛ ISO/IEC 35802 و استاندارد ملی ایران شماره ۱۲۰۴۷ استفاده شود.

1 - Key Goal Indicators
2 - Key Performance Indicators
3 - Key Business Indicators

فناوری اطلاعات – چارچوب مخاطره (ریسک) جرم‌شناسی رقمی (دیجیتالی) از منظر حاکمیت

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ، تعیین چارچوبی برای نهادهای حاکمیتی سازمان (شامل مالکان، اعضای هیئت‌مدیره، مدیران، شرکا، مدیران اجرایی یا امثال آنها) به بهترین روش می‌باشد. تا سازمان را برای رسیدگی‌های رقمی، قبل از وقوع آنها آماده کند. این استاندارد برای ایجاد فرآیندهای راهبردی (و تصمیم‌ها) مربوط به حفظ، دسترس‌پذیری، دستیابی و اثربخشی هزینه‌های افشای شواهد رقم کاربرد دارد. این استاندارد ملی برای تمام انواع سازمان‌ها با هر اندازه‌ای قابل اجرا 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 می‌شود.

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

استفاده از مراجع الزامی زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ۱۲۰۴۷، راهبری سازمانی فناوری اطلاعات

۲-۲ ISO Guide 73:2009, Risk management – Vocabulary

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف به کار رفته در استاندارد ملی ایران به شماره ۱۲۰۴۷، ISO Guide 73:2009 اصطلاحات و تعاریف زیر نیز به‌کار می‌روند:

۳-۱ شواهد رقمی

اطلاعات یا داده ذخیره یا منتقل شده به‌صورت دودویی که ممکن است به‌عنوان شاهد، به آن اتکا شود.

[مرجع: استاندارد ملی ایران شماره ۲۷۰۳۷]

۳-۲ نهاد حاکمیتی

فرد یا گروهی از افراد که در مورد عملکرد و انطباق سازمان به سودبران[1] پاسخگو هستند.

[مرجع: ISO/IEC TR 38502:2014 ، بند ۲-۹]

1 -Stakeholder

۳-۳ جرم‌شناسی رقمی[1]

وظایف، فنون و شیوه‌های علمی مورد استفاده در رسیدگی به داده یا اطلاعات دودویی ذخیره یا منتقل شده، به منظور اهداف قانونی است.

۳-۴ مخاطره راهبردی

تاثیر عدم قطعیت بر اهداف است.

۴ اصول

۴-۱ مسئولیت

افراد و گروه‌هایی در درون سازمان مسئولیت‌های خود در خصوص عرضه و تقاضای شواهد رقم را درک کرده و می‌پذیرند. آن دسته از افراد مسئولِ رسیدگی، مهارت، استقلال و اختیار انجام آن اقدامات را نیز دارند.

۴-۲ راهبرد

توسعه راهبرد سازمان حفظ، دسترس‌پذیری، دستیابی به و مقرون به صرفه بودن هزینه فعلی و آینده شواهد رقم را در نظر می‌گیرد؛ برنامه‌های راهبردی برای قابلیت‌های شهودی، نیازهای فعلی و در حال انجام سازمان را تأمین می‌کند.

۴-۳ اکتساب

اکتساب دارایی‌های فناوری اطلاعات به‌منظور پشتیبانی از راهبردهای سازمان، بر اساس تحلیل مناسب و مداوم، با تصمیم‌گیری واضح و شفاف ایجاد شده است. تعادل مناسبی بین فواید، فرصت‌ها، هزینه‌ها و مخاطره‌ها، در کوتاه مدت و بلندمدت وجود دارد.

۴-۴ عملکرد

فناوری اطلاعات برای هدف حمایت از سازمان، ارائه خدمات، سطوح خدمت و کیفیت خدمت مورد نیاز برای تحقق الزامات شواهد رقم فعلی و آینده سازمان مناسب است.

۴-۵ انطباق

دارایی‌های فناوری اطلاعات با تمام قوانین و مقررات اجباری منطبق است. سیاست‌ها و شیوه‌ها مطابق با معیارهای مخاطره سازمان به وضوح تعریف، پیاده‌سازی و اجبار شده است.

۴-۶ رفتار انسانی

1- Digital Forensics

سیاست‌ها، شیوه‌ها و تصمیم‌های جرم‌شناسی رقم، احترام به رفتار انسانی شامل نیازهای فعلی و در حال تحول برای تمامی‌افراد در فرآیندهای سازمان را نشان می‌دهد.

۵ چارچوب

۵-۱ اختیار سودبران

توصیه می‌شود هیأت حاکم تشکیل شده و به نمایندگی از طرف ذینفعان، اختیار ایجاد مسیر راهبردی سازمان را داشته و توانایی عملکرد را ایجاد کنند.

۵-۲ استقرار

توصیه می‌شود چرخه کاری نهاد حاکمیتی، با وظایف ارزیابی، هدایت و پایش هم‌راستا بوده و پذیرش سیاست راهبردی، برنامه‌ریزی راهبردی و توانایی راهبردی را تسهیل کند.

۵-۳ ارزشیابی

توصیه می‌شود هیأت حاکم بررسی و قضاوت در مورد الزامات فعلی و آینده شواهد رقم را، شامل راهبردها، پیشنهادها، برنامه‌ها و تمهیدات عرضه (داخلی یا خارجی یا هر دو)، انجام دهد. در ارزشیابی کاربرد فناوری اطلاعات، بهتر است نیاز به تولید شواهد رقم و الزامات فرآیندهای جرم‌شناسی رقم تعیین شوند.

۵-۴ هدایت

توصیه می‌شود هیأت حاکم مسئولیت آماده‌سازی و پیاده‌سازی راهبردها، برنامه‌ها و سیاست‌ها را تفویض کرده و آنها را هدایت کند. توصیه می‌شود برنامه‌ها مسیر راهبرد را برای شواهد رقم، عملیات فناوری اطلاعات و توانایی‌ها تعیین کند. هیأت‌های حاکم بهتر است فرهنگ حاکمیت صحیح فناوری اطلاعات را در سازمان خود با درخواست از مدیران برای ارائه اطلاعات به موقع، پیروی از مسیرهای راهبردی و انطباق با معیارهای مخاطره تشویق کنند.

۵-۵ پایش

توصیه می‌شود هیأت حاکم از طریق سامانه‌های اندازه‌گیری مناسب، عملکرد و انطباق سامانه‌های فناوری اطلاعات را برای شواهد رقمی پایش کند. آنها بهتر است به خود اطمینان مجدد دهند که عملکرد مطابق با برنامه‌های راهبردی است و سطوح مخاطره آن در معیارهای مخاطره سازمان قرار دارد. مسئولیت استفاده موثر، کارآمد و قابل قبول سازمان از فناوری اطلاعات برای اهداف مربوط به شواهد، به عهده نهاد حاکمیتی و غیر قابل واگذاری است.

۶ فرآیندها

۶-۱ راهبرد بایگانی

توصیه می‌شود سازمان بایگانی جامعی برای نگهداری از دارایی‌های اطلاعاتی ایجاد کند. فرآیندهای بایگانی ساختاریافته، کامل، موثر، امن بوده و از جامعیت داده‌ها نگهداری کند.

۶-۲ راهبرد کشف

توصیه می‌شود سازمان توانایی‌های موثر و کارآمد بازیابی اطلاعات را ایجاد کند. دسترسی به موقع و دقیق به اطلاعات سازمان برای تصمیم‌گیری و ارائه شواهد، حیاتی است.

۶-۳ راهبرد افشا

توصیه می‌شود سازمان معیاری را برای امنیت و افشای اطلاعات ایجاد و برای هرگونه ارزیابی مخاطرات رقمی که با آن مواجه است، معیار مخاطره را برای تعیین اینکه آیا مخاطره قابل پذیرش است یا با قبول مخاطره راهبردهای دیگری مورد نیاز است، اعمال کند. اطلاعات افشا شده بهتر است طوری نگهداری شوند که قابل ممیزی باشند.

۶-۴ راهبرد توانایی جرم شناسی رقمی

توصیه می‌شود سازمان سیاست‌ها و برنامه‌هایی را برای اطمینان از حفظ شواهد رقمی و نگهداری و/یا دسترسی به مهارت‌های جرم‌شناسی رقمی طرح‌ریزی کند. سازمان باید فرآیندهایی را نگهداری کند که از جامعیت رسیدگی‌ها، استقلال کارشناسان، و ارزش شهودی اطلاعات دودویی اطمینان دهد.

۶-۵ راهبرد انطباق مخاطره

توصیه می‌شود سازمان در مورد تطبیق مخاطره راهبرد براساس کاربرد معیار مخاطره سازمان برای شواهد رقمی تصمیم‌گیری کند. توصیه می‌شود هیأت حاکم اطمینان حاصل کند که سطح مخاطره در محدوده معیار مخاطره سازمان باقی می‌ماند.

۷ سنجه‌ها[1]

۷-۱ عمومی

توصیه می‌شود سازمان صفت‌های مهم هستار را به‌منظور ارزشیابی برنامه‌ها و پیشنهادها، پایش عملکرد و انطباق، و هدایت راهبرد و سیاست‌ها اندازه‌گیری کند. گزارش‌ها، اطلاعات مورد نیاز برای تصمیم‌گیری آگاهانه را در اختیار هیأت حاکم سازمان قرار می‌دهد.

۷-۲ نشانگرهای کلیدی هدف

نشانگر کلیدی هدف (KGI) سنجه‌های صفات از اهداف اصلی را گزارش می‌دهد. نشانگر کلیدی هدف روشی برای پایش دستیابی به ارزش‌های اصلی ارائه می‌کند.

۱- Metrics

۳-۷ نشانگرهای کلیدی عملکرد

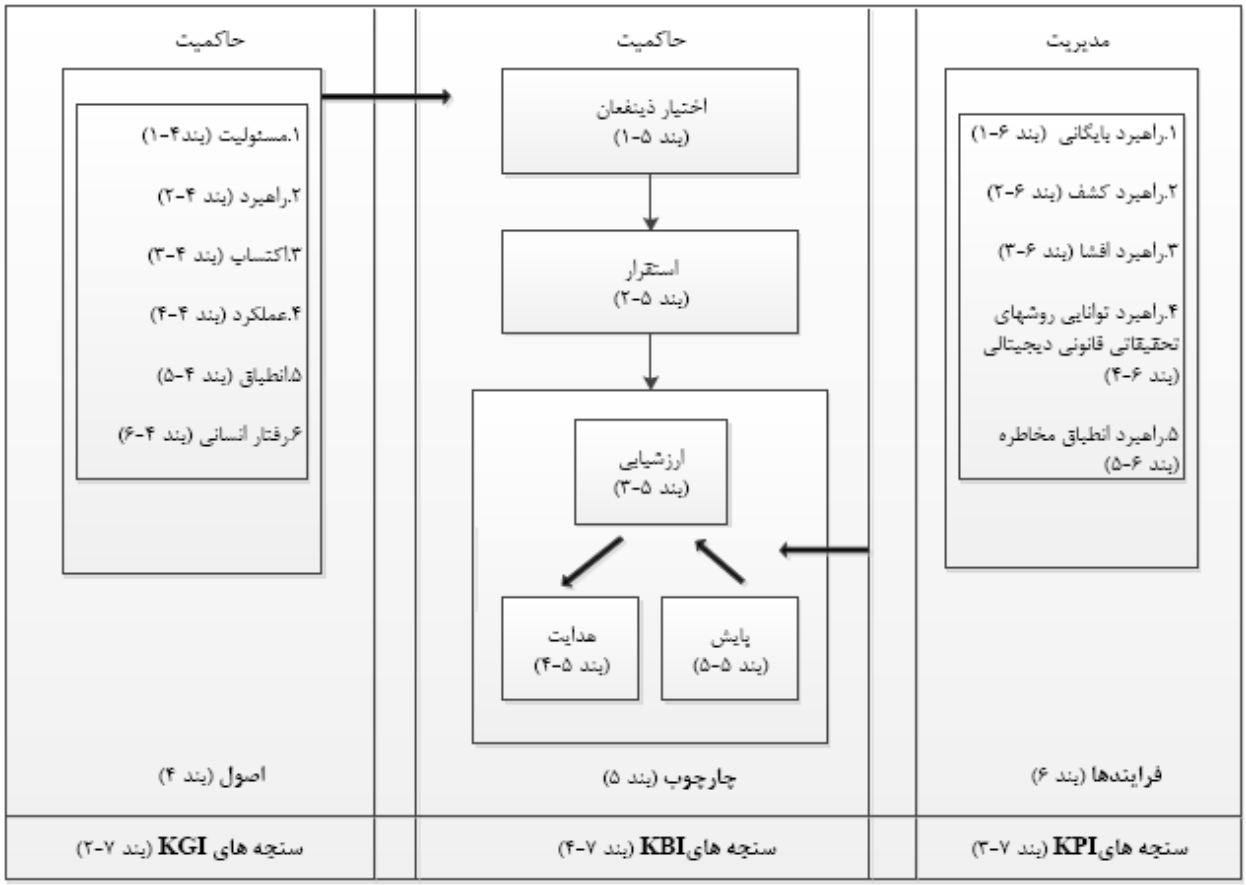
نشانگر کلیدی عملکرد (KPI) سنجه‌های صفات از اهداف عینی را گزارش می‌دهد. نشانگر کلیدی عملکرد روشی برای پایش دستیابی به ارزش‌های فرآیندی ارائه می‌کند

۴-۷ نشانگرهای کلیدی کسب وکار

نشانگر کلیدی کسب وکار (KBI) اختلاف بین نشانگر کلیدی هدف و نشانگر کلیدی عملکرد را گزارش می‌کند. نشانگرهای کلیدی روشی برای پایش دستیابی به پیشرفت سازمان ارائه می‌کنند.

پیوست الف
(اطلاعاتی)
مرورکلی استاندارد ملی

بررسی اجمالی استاندارد ملی در شکل الف -۱ نشان داده شده است.



شکل الف- ۱ مرور کلی استاندارد ملی

پیوست ب
(اطلاعاتی)
کتابنامه

۱- استاندارد ملی ایران ۱۳۲۴۵ : ۱۳۸۹، مدیریت ریسک - اصول و رهنمودها

۲-ISO 31010:2009, Risk Management - Risk assessment techniques

۳-ISO/IEC TR 38502:2014, Information technology - Governance of IT - Framework and model

4-ISO/IEC 35802, Information technology - Governance of IT framework and model