INSO
20431
1st.Edition
2016

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

استاندارد ملی ایران
۲۰۴۳۱
چاپ اول
۱۳۹۴

دارای محتوای رنگی

اطلاعات و دبیزش(مستندسازی) – ارزیابی ریسک (مخاطرات) برای فرایند پیشینه‌ها و سامانه‌ها

Information and Dumentation– Risk assessment for records processes and systems

ICS: 01.140.20

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ 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 حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان صاحب‌نظران 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 علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذینفع 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.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذیصلاح 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 می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد 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 اندازه‌شناسی 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 پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی 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 ملی استاندارد ایران می‌تواند به منظور حفظ بازارهای بین‌المللی 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 صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد 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 Electro technical Commission
3 - International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«اطلاعات ودبیزش(مستندسازی)– ارزیابی ریسک(مخاطرات) برای فرایند پیشینه‌ها و سامانه‌ا»

رئیس	**سمت و / یا نمایندگی**
شکیبائیان، طناز (دکتری آموزش عالی)	کارشناس اداره کل استاندارد مازندران
دبیر	
عرب، هما (کارشناسی کتابداری و اطلاع‌رسانی)	کارشناس اداره کل استاندارد مازندران
اعضا: (به ترتیب حروف الفبا)	
اسدی، سیده مریم (کارشناسی مترجمی زبان انگلیسی)	کارشناس آمار و اطلاعت اداره کل استاندارد مازندران
رستمیان، رحمتعلی (کارشناسی ارشد مدیریت منابع انسانی)	مدیر مالی بهداری و بهداشت شرکت نفت شمال کشور
شریف زاده، سیده زهرا (کارشناس ارشد آموزش زبان انگلیسی)	کارشناس فناوری اطلاعات اداره کل استاندارد مازندران
صدری ، سید حسن (دکتری مدیریت کسب و کار)	مدیر آموزش بهداری و بهداشت شرکت نفت شمال کشور و مدرس
قادری، محمدرضا (کارشناسی مدیریت دولتی)	کارشناس اداره کل استاندارد مازندران
مرید مشتاق صفت، مریم (کارشناسی ارشد مدیریت مالی)	رئیس مالی اداره کل استاندارد مازندران

فهرست مندرجات

عنوان	صفحه
پیش‌گفتار	ح
مقدمه	خ
۱ دامنه کاربرد	۱
۲ مراجع الزامی	۱
۳ اصطلاحات و تعاریف	۲
۳-۱ اصطلاحات مربوط به ریسک	۲
۳-۲ اصطلاحات مربوط به پیشینه	۲
۴ معیارهای ارزیابی ریسک برای سازمان	۳
۵ شناسایی ریسک	۵
۵-۱ کلیات	۵
۵-۲ بستر: عوامل خارجی	۶
۵-۳ بستر: عوامل درونی	۸
۵-۴ سامانه‌های پیشینه‌ها	۱۰
۵-۵ فرایندهای پیشینه‌ها	۱۳
۶ تحلیل ریسک های شناسایی شده	۱۵
۷ ارزیابی ریسک	۱۹
پیوست «الف» (اطلاعاتی) : نمونه‌ای از ریسک‌های وارد شده مستند در ثبت ریسک	۲۴
پیوست «ب» (اطلاعاتی) مثال: سیاهه ای برای شناسایی حوزه‌های عدم اطمینان	۲۵
ب۱ عوامل بیرونی	۲۵
ب۲ عوامل درونی	۲۶
ب۳ سامانه پیشینه‌ها	۲۸
ب۴ فرایند پیشینه‌ها	۳۰
پیوست«پ» (اطلاعاتی) : راهنمای استفاده کنترل‌گرها از استاندارد ISO/IEC27001	۳۴
فهرست منابع	۴۳

پیش‌گفتار

استاندارد «اطلاعات ودبیزش(مستندسازی)- ارزیابی ریسک (مخاطرات) برای فرایند پیشینه‌ها وسامانه‌ها» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده است، در یکصد و هفتادوششمین اجلاسیه کمیتهٔ ملی استاندارد اسناد و تجهیزات اداری وآموزشی مورخ ۹۴/۱۲/۹ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران درصورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط موردتوجه قرار خواهد گرفت.بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی (منابع و مآخذی) که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

1- ISO 18128: 2014 Information and documentation — Risk assessment for records processes and systems

مقدمه

کلیه سازمان‌ها برای عملکرد موفقیت آمیز خود ریسک‌ها را شناسایی ومدیریت می‌کنند. شناسایی و مدیریت ریسک‌ها برای فرایندهای پیشینه‌ها و سامانه‌ها ، مسئولیت متخصصان سازمان است.

این استاندارد برای کمک به متخصصان پیشینه‌ها و افرادی که در سازمان خود برای پیشینه‌ها جهت ارزیابی ریسک‌های مرتبط با فرایند پیشینه‌ها و سامانه‌ها مسئولیتی دارند در نظر گرفته شد.

یادآوری- سامانه به معنی هر برنامه کسب وکاری است که پیشینه‌هایی را تولید و ذخیره می‌کند.

موضوع این استاندارد از وظیفه شناسایی و ارزیابی ریسک‌های کسب‌وکار برای سازمان‌هایی که ایجاد ونگهداری پیشینه‌ها راهبردی است متمایز است. تصمیمات برای ایجاد کردن یا نکردن پیشینه‌ها، در پاسخ به ریسک کسب و کارهای عمومی، تصمیماتی است که باید با تجزیه و تحلیل پیشینه‌های موردنیاز سازمان که متخصصان پیشینه‌ها با همکاری مدیران کسب وکار ایجاد می‌کنند اتخاذ شود. هدف اصلی این استاندارد آن است که سازمان پیشینه‌های فعالیت‌های کسب وکار خود را برای تامین سایر اهداف اجرایی و حداقل مکانیزم برای مدیریت نظام‌مند وکنترل پیشینه‌ها ایجاد کند.

نتیجه ریسک فرایندهای پیشینه‌ها وسامانه‌ها که وارد سازمان می‌شود از دست دادن یا تخریب پیشینه‌هایی است که قابل استفاده، قابل اعتماد، معتبر و کامل نیستند و یا بدون تغیر هستند و بنابراین نمی‌تواند برای اهداف سازمان پاسخ‌گو باشند.

این استاندارد، راهنما و نمونه‌ای را براساس فرایندهای مدیریت ریسک عمومی که در استاندارد ایران- ایزو ۳۱۰۰۰(مراجعه شود به شکل ۰) آمده‌است را برای اجرای ریسک‌های مرتبط با فرایندهای پیشینه‌ها و سامانه‌ها آماده می‌کند که موارد ذیل را پوشش می‌دهد.

الف- شناسایی ریسک؛

ب- تجزیه و تحلیل ریسک؛

پ – ارزیابی ریسک.

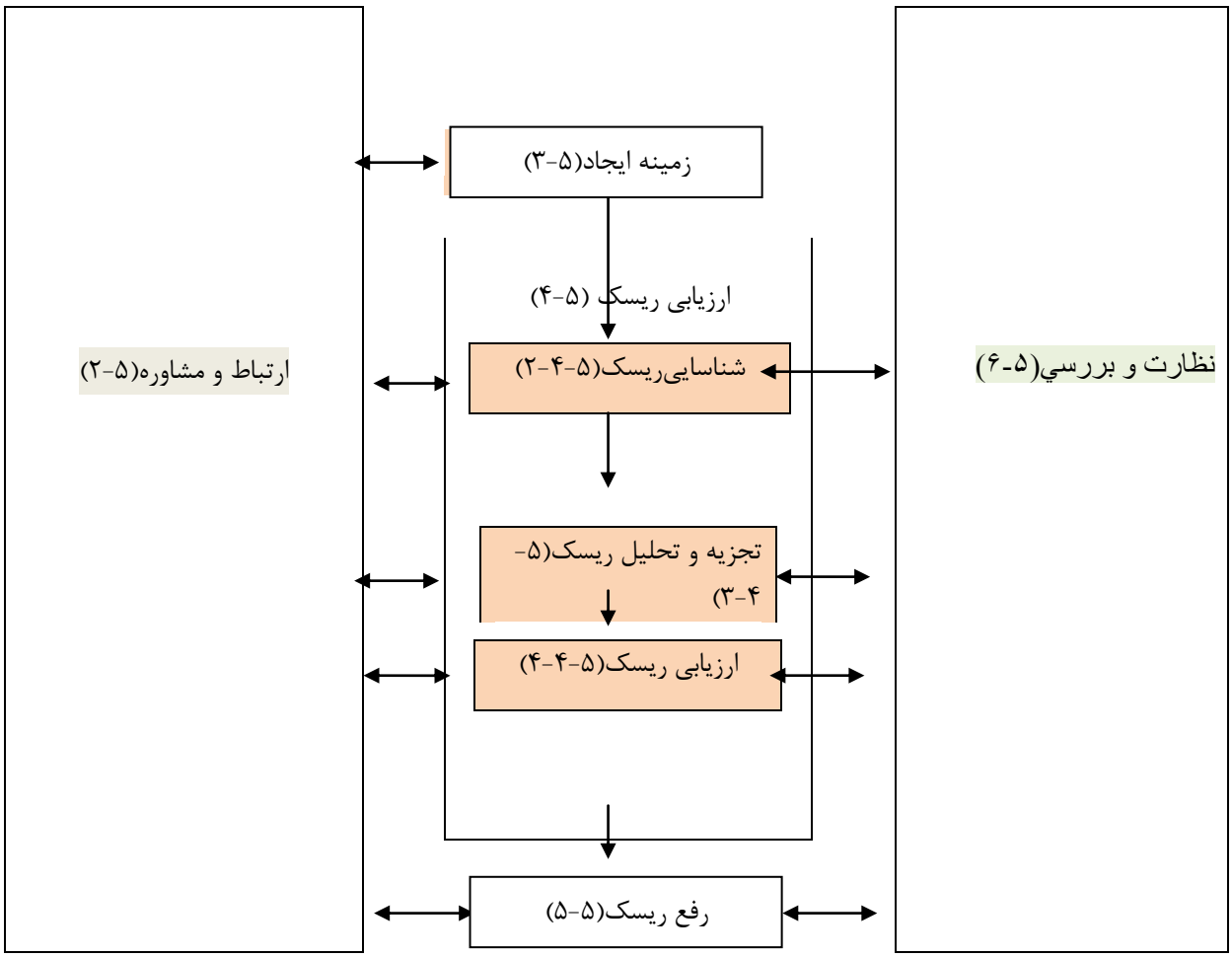
نتایج تجزیه و تحلیل ریسک برای فرایندهای پیشینه‌ها و سامانه‌ها باید در چارچوب مدیریت ریسک عمومی سازمان گنجانده شود، در نتیجه سازمان بهتر می‌تواند پیشینه‌ها خودو کیفیت آنها را برای اهداف کسب وکار کنترل کند.

فهرست جامعی از حوزه های عدم اطمینان مرتبط با فرایندهای پیشینه‌ها و سامانه‌ها به عنوان راهنمایی برای شناسایی ریسکدر بند ۵ ارائه شده است؛

راهنمایی برای تعیین عواقب و احتمالات رویدادهای ریسک شناخته شده با توجه به حضور(یا عدم حضور) و اثربخشی کنترل‌های موجود در بند ۶ ارائه شده است؛

راهنمایی را برای تعیین اهمیت سطح و نوع ریسک‌های شناخته شده در بند ۷ ارائه شده است..

این استاندارد با رفع ریسک سروکار ندارد. وقتی که ارزیابی ریسک‌های مرتبط با فرایندهای پیشینه‌ها سامانه‌ها کامل شود ارزیابی ریسک، مستند شده و به بخش مدیریت ریسک سازمان ابلاغ می‌شود. پاسخ به ارزیابی ریسک‌ها، تعهد قسمتی از برنامه مدیریت ریسک کلی سازمان است. اولویت اختصاص داده شده توسط متخصصان پیشینه‌ها برای ارزیابی ریسک‌هایی است که جهت اطلاع از تصمیمات سازمان درباره مدیریت ریسک‌های آنها ارائه شده است.



شکل ۰- فرایند مدیریت ریسک

اطلاعات و دبیزش(مستندسازی) – ارزیابی ریسک (مخاطرات) برای فرایند پیشینه‌ها و سامانه‌ها

۱ دامنه کاربرد

هدف از تدوین این استاندارد کمک به سازمان در ارزیابی ریسک برای فرایند پیشینه‌ها و سامانه‌ها است،تا بتوانند تداوم پیشینه‌ها را برای مواجه با نیازهای کسب وکارهای شناخته شده تا زمانی که مورد نیاز است، تضمین کنند.

این استاندارد درموارد زیر کاربرد دارد:

الف- ایجاد روش تجزیه‌وتحلیل برای شناسایی ریسک‌های مربوط به فرایند پیشینه‌ها و سامانه‌ها؛

ب- تهیه روش تجزیه و تحلیل اثرات بالقوه رویدادهای مخالف در فرایند پیشینه‌ها و سامانه‌ها؛

پ- تهیه راهنماهایی برای انجام ارزیابی ریسک مرتبط با فرایند پیشینه‌ها و سامانه‌ها و؛

ت- تهیه راهنماهایی برای مستندسازی ریسک‌های شناخته شده وآمادگی برای کاهش آنها.

این استاندارد برای ریسک‌های عمومی مرتبط با فعالیتهای که می‌توان آنها را با مستندسازی پیشینه‌ها کاهش داد، کاربرد ندارد. این استاندارد برای کلیه سازمان‌ها صرف نظر از اندازه، ماهیت فعالیت‌هایشان یا پیچیدگی عملکرد و ساختارشان، کاربرد دارد.

این استاندارد عوامل و نظام مقررات را که سازمان در آن فعالیت می‌کند و مجوز ایجاد و کنترل پیشینه‌های سازمان را صادر می‌کند، در زمان شناسی و ارزیابی ریسک مربوط به پیشینه‌های سازمان در نظرمی‌گیرد. تعریف یک سازمان یا شناسایی حدود آن باید ساختار پیچیده ، شرکا و تنظیمات قراردادی برای برون سپاری خدمات و زنجیره تامینی را که ویژگی‌های مشترک دولت و شرکت‌های بزرگ معاصر است را در نظر بگیرد.

شناسایی مرزهای سازمان، اولین قدم در تعریف دامنه طرح ارزیابی ریسک مربوط به پیشینه‌ها 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 جزیی از این استاندارد محسوب می‌شود.

در مورد مراجع دارای تاریخ چاپ و/ یا تجدیدنظر، اصلاحیه‌ها و تجدیدنظرها بعدی این مدارک مورد نظر نیست. معهذا بهتر است کاربران ذی‌نفع این استاندارد امکان کاربرد آخرین اصلاحیه‌ها و تجدیدنظرهای مدارک الزامی زیر را مورد بررسی قرار دهند. در مورد مراجع بدون تاریخ چاپ و / یا تجدیدنظر، آخرین چاپ و یا تجدیدنظر آن مدارک الزامی ارجاع داده‌شده مورد نظر است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

2-1 ISO 30300:2011, Information and documentation — Management systems for records — Fundamentals and vocabulary

2-2 ISO Guide 73:2009, Risk management — Vocabulary

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر کاربرد دارد:

۳-۱ اصطلاح‌های مربوط به ریسک

۳-۱-۱

ریسک

risk

نتیجه عدم اطمینان

یادآوری ۱- هر تاثیری که از آنچه مدنظر است منحرف شده باشد، چه مثبت چه منفی

یادآوری ۲- عدم اطمینان حالتی، هر چند نسبی از نقص در اطلاعات مربوط به فهم یا دانش یک رویداد، پیامدها یا احتمال آن است.

یادآوری ۳- ریسک اغلب با اشاره به رویداد بالقوه و نتایج آن (ISO Guide 73-2009 3.5.1) و پیامدهای آن (ISO Guide 73 – 2009 3.6.1.B) و یا ترکیبی از این دو مشخص می‌شود.

یادآوری ۴- ریسک اغلب بر اساس ترکیبی از پیامدهای یک رویداد (شامل: تغییر شرایط) و احتمال مربوط به بروز آن بیان می‌شود (ISO-G 73-2009 3.6.1.1).

۳-۲ اصطلاحات مربوط به پیشینه

۳-۲-۱

سامانه پیشینه‌ها

records system

سامانه اطلاعاتی که طی گذر زمان، پیشینه‌ها را گردآوری، مدیریت و دسترس‌پذیرمی‌کند.

یادآوری ۱- این امر می‌تواند شامل کاربردهای تجاری یا سامانه‌هایی باشد که پیشینه‌ها را ایجاد و نگهداری می‌کند (ISO: 30300: 2011 3.4.4)

۲-۲-۳

فرایند پیشینه‌ها

records processes

مجموعه‌ای از فعالیت‌هایی است که سازمان به کمک آن‌ها پیشینه‌هایی را ایجاد، کنترل، استفاده، نگهداری و سازمان‌دهی می‌کند.

۴ معیارهای ارزیابی ریسک برای سازمان

۴-۱ ارزیابی ریسک

توصیه می‌شود ارزیابی ریسک‌ها برای فرایندهای پیشینه‌ها و سامانه‌ها، در صورت وجود، جزو فرآیند عمومی مدیریت ریسک سازمان قرارگیرد. دراین حالت محققان پیشینه‌ها بهتر است بستر بیرونی و درونی سازمان و نیز بستر فرایند مدیریت ریسک، از جمله موارد زیر را درنظر بگیرند.

الف- نقش‌ها و مسئولیت‌ها: توصیه می شود نقش متخصص پیشینه‌ها در ارزیابی ریسک مربوط به فرایندهای پیشینه‌ها و سامانه‌ها تعیین شود.

ب- وسعت و دامنه فعالیت‌های ارزیابی ریسک: ارتباطات با سایر حوزه‌های ارزیابی ریسک از جمله امنیت اطلاعات برای پرهیز از حشو و تعارض و ایجاد رویکردی یکپارچه برای ارزیابی ریسک پیشینه‌ها باید روشن و مشخص باشد.

پ- روش‌شناسی: توصیه می‌شود روش‌شناسی استاندارد ارزیابی ریسک را با استفاده از ابزارهای موجود ارزیابی ریسک و گزارش‌دهی آن به فرد یا هویت تعیین شده به‌کار برده شود

ت - معیارهای ریسک: توصیه می‌شود هرجا معیارهای عمومی ریسک برای سازمان تعیین شده باشد ریسک‌های مربوط به فرایندهای پیشینه‌ها و سامانه‌ها هم بر اساس این معیارها ارزیابی شوند.

هر گاه سازمان فاقد فرایند مدیریت عمومی ریسک باشد، لازم است متخصصان پیشینه‌ها ، معیارهای ریسک را قبل از فرایند ارزیابی برای فرایندهای پیشینه‌ها و سامانه‌ها تعیین کنند.

۴-۲ معیارهای ریسک

توصیه می‌شود معیارها مبتنی بر الزامات قانونی مربوط به حقوق و موازین سازمان، شامل موارد زیر باشند:

الف- ماهیت و انواع پیامدهای موردنظر وروش اندازه‌گیری آنها؛

ب- چگونگی بیان احتمالات؛

پ- تعیین سطح ریسک؛

ت- معیارهای تصمیم‌گیری برای برخورد موردنیاز با ریسک؛

ث - معیار تصمیم‌گیری برای ریسک‌های قابل تحمل یا قابل قبول؛

ج - ترکیب ریسک‌ها چگونه محاسبه خواهد شد.

با توجه به ماهیت و انواع پیامدهای مورد نظر در ارزیابی ریسک و فرایندهای پیشینه‌ها و سامانه‌ها ، یک نقطه شروع کلی برای تمامی سازمان‌ها وجود دارد. پیشینه‌ها که معتبر، قابل اعتماد، یکپارچه و قابل استفاده هستند، تا زمانی که لازم باشد، از نیازهای سازمان پشتیبانی می‌کنند. ریسک‌ها براساس قابلیت‌شان در صدمه زدن به آن دسته از ویژگی‌های کلی پیشینه‌ها که عامل شکست در رسیدن به اهداف ملحوظ برای ایجاد آنهاست، شناسایی می‌شوند.

برای موضوع احتمال و فراوانی رویدادها در ارزیابی ریسک به بند ۶-۲ مراجعه کنید. معیارهای ارزیابی ریسک شامل اندازه و دامنه سامانه‌های رکورد در سازمان، تعداد کاربران و استفاده از رکوردها در بخش‌های مختلف سازمان است.

همین‌طور، معیارهای ارزیابی ریسک‌های اثرگذار بر فرآیندهای رکوردها باید مشتمل بر تناوب فرآیند، تعداد سامانه‌های درگیر در آن، اهمیت نسبی آن‌ها در ایجاد و مدیریت پیشینه‌ها، اثرات این فرایندها و قابلیت آن‌ها در حل و فصل اثرات سوء باشد.

۴-۳ تعیین اولویت

به‌طورکلی، سازمان باید تعیین کند چه پیشینه‌هایی برای عملکرد سازمان اصلی و اساسی است و میزان اهمیت هر کدام چقدر است. این‌ها تصمیماتی کاری هستند که بر اساس توصیه‌های متخصصان پیشینه‌ها و مدیران کسب‌وکار گرفته می‌شود.

اولویت تخصیص یافته بر هر یک از رکوردها، انباشتگی آن‌ها، فرایند پیشینه‌ها یا سامانه‌های خاص پیشینه‌ها را می‌توان در ارتباط با پاسخ و واکنش به آسیب‌های عمده اثرگذار بر همه یا بیشتر عملکردهای کسب و کار ارزیابی کرد. برای مثال: نخست بلافاصله پس از بروز یک فاجعه طبیعی پیشینه‌های معینی مانند نشانی‌ها و تلفن‌های تماس امنیتی، پیشینه‌ها اصلی سازمان، جزئیات تماس گروه‌های پاسخگوی طرح فاجعه، جزئیات تماس بیمه‌ای و خط و مشی سازمانی مورد نیاز است. در مرحله دوم، برنامه تداوم کسب و کار سازمان باید عملکردها و پیشینه‌هایی را تعیین و شناسایی کند که در ابتدا باید مورد نظر قرار می‌گرفت.

در جای که ترکیبی از ریسک ها به عنوان هسته عملیاتی برای پیشینه‌های شناسایی شده به‌کار می رود، توجه خاصی لازم است.

۵ شناسایی ریسک

۵-۱ کلیات

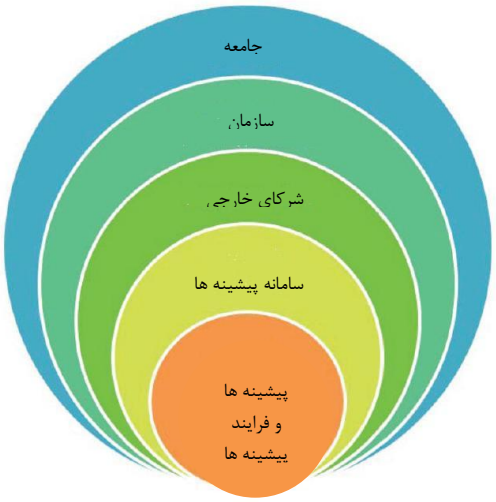
روند شناسایی ریسک‌ها تحت رده‌های زیر سازمان‌دهی می‌شوند: بافت، سامانه‌ها، فرآیندهای دخیل در ایجاد وکنترل رکوردهای سازمان.

بستر(بافت) بیرونی سازمان به عوامل سیاسی واجتماعی، اقتصاد کلان و فناوری و فیزیکی و محیطی اشاره دارد که خارج از کنترل سازمان است و بر عملکردهای آن تأثیر دارد و هنگام تعیین الزامات پیشینه‌های آن مورد توجه قرار می‌گیرد. بستر بیرونی شامل ذی‌نفعان بیرونی علاقمند به امور و عملکردهای سازمان است.

سازمان، بستری (بافتی) درونی هم دارد که عواملی درونی هستند که متخصص (متخصصان) پیشینه‌ها و مسئول در فرایندهای پیشینه‌ها و سامانه‌ها ، کنترلی روی آنها ندارند. بستر درونی شامل عواملی چون ساختار، امور مالی سازمان و فناوری مورد استفاده، منبع انجام فعالیت‌ها (افراد و بودجه) و فرهنگ سازمانی است که همگی آن‌ها بر سیاست‌ها و رویه‌های مدیریت پیشینه‌ها اثرگذار هستند.

رویدادهای بالقوه با اثراتی نا مطمئن می‌توانند درون سازمانی یا برون سازمانی باشند.

اثرات عدم اطمینان حاصل از تغییراتی در بستر بیرونی بر اساس چشم‌انداز سطوح مختلف سازمانی متفاوت است (به شکل ۲ مراجعه شود) البته معلوم می‌شود که همه تغییرات می‌تواند فرصت‌هایی با نتایجی مثبت همراه داشته باشند.



شکل ۱- لایه‌های چندگانه بستر رکوردها و فرآیندهای رکوردهای سازمان

هدف از شناسایی ریسک آن است که آنچه می‌تواند به وقوع بپیوندد و موقعیتی را که وجود دارد و بر قابلیت پیشینه‌ها در برآوردن نیازهای سازمان اثر دارد را شناسایی کند.

فرایند شناسایی ریسک شامل شناسایی علل و منشأ ریسک‌ها، رویدادها ، موقعیت‌ها و شرایطی که دارای تأثیر مادی بر اهداف سازمانی و ماهیت این تأثیر است. روش‌های چندی برای شناسایی ریسک‌های وجود دارد. برای مقایسه روش‌های اصلی به استاندارد IEC 31010 مراجعه کنید. ریسک های شناسایی شده باید در دفتر ثبت مخصوص آن و یا در دفتر ریسک‌های سازمان مستند شود؛ چه این سامانه مخصوص این کار باشد و چه متعلق به سازمان و یا اینکه کلی باشد (به مثال‌های داده شده در پیوست الف مراجعه کنید).

یادآوری- پیوست «ب» نمونه‌ای از بازبینه مبتنی بر ساختار بند ۵ است که می‌توان برای شناسایی ریسک‌های فرایندهای پیشینه‌ها و سامانه‌ها به صورت نظام‌یافته از آن در سازمان استفاده کرد.

۵-۲ بستر: عوامل خارجی

۵-۲-۱ حوزه‌های عدم اطمینان : تغییر در بستر سیاسی – اجتماعی

تغییر در حوزه‌های سیاسی و اجتماعی، چه در سطح ملی و چه در سطح بین‌المللی می‌تواند گرایش عمومی رفتارهای دولت‌ها و سازمان‌ها را تحت‌الشعاع قرار دهد. این امر می‌تواند تغییرات مربوط به قوانین و مقررات باشد که عملکردهای سازمانی و متعاقباً، الزامات پیشینه‌هارا تحت تأثیر قراردهد. امنیت ملی، دسترسی به اطلاعات دولتی و خصوصی، حریم خصوصی، حقوق مالکیت فکری و مسئولیت‌های سازمانی مثال‌هایی از حوزه‌های تغییر رفتار عمومی است که در الزامات پیشینه‌ها مؤثر است.

در سطح کلی مصادیق حوزه‌های عدم اطمینان، شامل موارد زیر است:

الف- تغییرات قانونی و حقوقی اثرگذار بر الزامات پیشینه‌های سازمان‌ها؛

ب- تغییرات در راهبردهای دولتی اثرگذار بر پیشینه‌های سازمان‌ها وفرایندها و سامانه‌های پیشینه‌های آنها؛

پ- استانداردها و آئین‌کارهای جدید کاربردی اثرگذار بر پیشینه‌های سازمان‌ها و فرایندها و سامانه‌های پیشینه‌های آن‌ها دارند؛

ت- درخواست تغییر برای خدمات پیشینه‌ها؛

ث- تغییر در انتظارات و خواسته‌های ذینفعان؛

ج- تغییر در اعتبار اعتماد توانایی‌های سازمان در ارائه خدماتشان؛

۵-۲-۲ حوزه های عدم اطمینان : محیط‌های اقتصاد کلان و فناوری.

تغییر در حوزه‌های اقتصادکلان، کسب‌وکار، صنعت و فناوری اطلاعات بر رقابت و تقاضای مشتریان تأثیر فراوانی دارد. تغییر می‌تواند تدریجی و مستمر یا حاصل بحران باشد.

اما همچنین باعث ایجاد حوزه عدم اطمینانی می‌شود که می‌تواند فرصت‌های مثبت و بالقوه همراه خود داشته باشد.

نمونه‌هایی از حوزه‌های عدم اطمینان حاصل از این تغییرات در محیط اقتصاد کلان و کسب‌وکار شامل موارد زیر است:

الف- تغییر در مالکیت و یا درآمد سازمان که بر اولویت‌های مدیریتی پیشینه‌ها اثرگذار است؛

ب- تغییر در اهداف، کارکردها و یا عملیات سازمان که الزامات پیشینه‌ها را تغییر می‌دهد؛

پ- فعالیت‌های افزایشی قانونگذران که تقاضای برون سازمانی پیشینه‌ها را افزایش می‌دهد؛

ت- افزایش دعاوی و شکایات که تقاضای برون سازمانی را برای پیشینه‌ها را افزایش می‌دهد؛

ث- شناسایی و رواج فناوری‌های جدید در جامعه.

مثال- استفاده از رسانه‌های اجتماعی در محیط کار، استفاده از ابزارهای محاسباتی تلفن همراه برای کسب و کار.

۵-۲-۳ حوزه‌های عدم اطمینان: محیط و زیرساخت فیزیکی

احتمال فجایع و بحران‌های بزرگ، مقیاس طبیعی و انسانی که کارکرد عمومی سازمان را تحت تأثیر قرار می‌دهد حوزه‌ای عمده است که به شناسایی و ارزیابی نیاز دارد. آسیب بالقوه چنین فجایعی عبارت‌اند از: اثر مستقیم بر پیشینه‌ها و ذخیره آنها و اثر غیرمستقیم بر نقص خدماتی که سازمان به آنها وابسته است مانند تأمین آب و انرژی و دیگر خدمات. حوزه‌های عدم اطمینان از این نوع شامل موارد زیر است:

الف- پدیده‌های مخرب یا ویرانگر محلی یا منطقه‌ای، از جمله زمین‌لرزه، تندباد، طوفان، سونامی، آتش‌سوزی و خشک‌سالی بلند مدت؛

پ- احتمال وجود اعمال جنگ‌طلبانه و تروریستی که موجب صدمات عمده ساختاری یا تخریبی روی حوزه خدمات سازمانی به مشتریان و کاربران می‌شود؛

پ – نقض و تخریب در مدیریت آب، فاضلاب، انرژی، فناوری اطلاعات، سامانه حمل‌ونقل و دیگر خدمات و تسهیلات عمده سازمان.

۵-۲-۴ حوزه‌های عدم اطمینان: تهدیدات امنیتی بیرونی

شناسایی ریسک حوزه باید شامل تهدیدات امنیتی خصمانه بیرونی با اثرات بالقوه تخریب از خدمات‌دهی به مشتریان گرفته تا دسترسی غیرمجاز به سامانه‌ها، از جمله سامانه‌های پیشینه‌ها باشد.

مواردی از تهدیدات امنیتی بیرونی عبارت‌اند از:

الف- دسترسی غیرمجاز از بیرون به سامانه های پیشینه‌ها و تغییرات غیرمجاز در پیشینه‌ها؛

ب- آسیب امنیتی ناشناخته یا بهره‌برداری از آسیب‌شناسی که پایش نمی‌شود و منجر به کاهش ارزش اطلاعات می‌شود.

مثال- استفاده از نرم‌افزار جاسوسی یا نرم‌افزار مخرب و سوءاستفاده از ضعف امنیتی و رخنه‌های اطلاعاتی نرم‌افزار

پ- ایجاد اختلال فیزیکی در ذخیره‌سازی پیشینه‌ها یا فضای سخت‌افزاری فناوری اطلاعات؛

ت- اجتناب از خدمات یا حملات عمدی دیگر به خدمات اینترنتی؛

ث- تخریب فیزیکی؛

چ- فقدان شخص ثالث خدمات‌رسانی که سامانه‌های پیشینه‌ها به آن وابسته است.

یادآوری- ارزیابی ریسک بخشی اساسی در اجرای استاندارد ISO/IEC 27000 از سری استانداردهای بین‌المللی برای امنیت اطلاعات است. این استانداردها، حوزه‌های عدم اطمینان مرتبط با امنیت اطلاعات را در سطح وسیع پوشش می‌دهند.

۵-۳ بستر: عوامل درونی

۵-۳-۱ حوزه‌های عدم اطمینان: تغییرات سازمانی

تصمیمات مدیریتی اثرگذار بر سازمان از جمله ادغام، تصدی‌گری و دیگر تهدیدات، بازسازی، کوچک‌سازی، تأسیس منابع یا محدود کردن خدمات، حوزه عدم اطمینان مهمی در بستر داخلی سازمان است. این تصمیمات فرایندها و سامانه های پیشینه‌ها را تحت‌الشعاع قرار می‌دهد.

برای مثال:

الف- تغییر مالکیت پیشینه‌ها و سامانه های پیشینه‌ها و انتقال متعاقب پیشینه‌ها به سازمان و بالعکس؛

ب- تغییر مالکیت پیشینه‌ها و سامانه پیشینه‌ها که منجر به انتقال اجباری پیشینه‌ها به سازمان و از سازمان می‌شود؛

پ- تمهیدات دسترسی به پیشینه‌ها برای حق دسترسی مداوم به پیشینه‌ها به دنبال انتقال و مهاجرت؛

ت- انتقال مسئولیت‌های پیشینه‌ها و سامانه های پیشینه‌ها ، بدون مستندسازی کافی؛

ث- فقدان آگاهی مؤثر کارکنان یا شرکا از پیشینه‌ها و سامانه‌های موجود، از جمله آگاهی از رویه‌های بازیابی و کاربرد آنها و نیز درباره پیشینه‌های پیشین به‌جا مانده از تغییرات سازمانی؛

ج- صرف‌نظر از پیشینه‌ها و سامانه‌های پیشینه‌ها ، به ویژه نظام‌های حقوقی که برایشان مسئولیتی تعیین نشده است،

چ- تغییر در اصطلاح قراردادهای خدمتی شخص ثالث؛

ح- خط‌مشی‌های جدید داخلی یا اصلاح موارد موجود در سازمان که فرایندهای سامانه‌های پیشینه‌ها را تحت تأثیر قرار می‌دهد؛

خ- خط‌مشی‌ها و رویه‌هایی که بازنگری و روزآمد نشده‌اند و دیگر به‌کار نمی‌روند و یا متعاقب تغییر سازمانی، متناقض‌یا بی‌ثبات شده‌اند؛

د- تغییر در کارکنان سازمان که مسئولیت برای پیشینه‌ها را تحت‌تأثیر قرار می‌دهد؛

ذ- تغییر در خط مشی کارکنان، بودجه آموزش و فرصت‌هایی که قابلیت افراد مسئول برای پیشینه‌ها را تحت‌الشعاع قرار می‌دهد؛

ر- طرح و بهبود وقایع که روزآمد نشده و در صورت رخداد فاجعه، پیشینه‌ها را تحت‌تأثیر قرار می‌دهد.

۵-۳-۲ حوزه‌های عدم اطمینان: تغییرات فناورانه

شناسایی و رواج فناوری‌ها و سامانه‌های جدید، فرصت‌هایی برای اصلاح و ارتقاء هستند، اما با قابلیت بالقوه در ایجاد اثرات سوء، حوزه‌های عدم اطمینان پدید می‌آورند. این حوزه‌های عدم اطمینان عبارتند از:

الف- تغییر فناورانه اثرگذار بر قابلیت‌سازگاری بین سامانه‌های ایجاد با کنترل پیشینه‌ها؛

پ- سازگاری با چارچوب‌های موجود سامانه‌ها؛

پ- طراحی و اجرای انتقال رکوردها؛

ت- پیکربندی دوباره مسئولیت‌ها وکنترل‌ها بر فرایند پیشینه‌ها؛

ث- کارآیی اجرای تغییرات؛

مثال- کفایت طراحی و مدیریت پروژه برای اجرای سامانه‌عامل یا نرم‌افزار جدید.

ج- میزان تحت پوشش قرار گرفتن خط و مشی‌های موجود توسط فناوری‌های نوینی که سازمان پذیرفته است؛

مثال- استفاده از خدمات ابری، رسانه‌های اجتماعی، شناسایی هویت از طریق امواج رادیویی (RFID[1]) و سامانه‌های فرایند.

ح- ظرفیت مجریان و توسعه‌دهندگان سامانه در استفاده از فناوری‌های جدید برای فهم موارد استفاده از این فناوری‌ها برای الزامات پیشینه‌ها، در مراحل پروژه و اجر؛

مثال- استفاده از نرم‌افزار اشتراکی یا محیط‌ها و یکی برای گسترش سامانه‌های جدیدی که نمی‌توانند به قدر کافی پیشینه‌ها پروژه و مستندات سامانه را فراهم سازند.

خ- ظرفیت زیرساخت‌های فناوری موجود در برآوردن الزامات جدید ناشی از توسعه فناورانه سامانه‌های سازمان یا پیشینه‌ها.

---

1 -Radio Frequency Identifcation

۵-۳-۳ حوزه‌های عدم اطمینان : منابع، افراد و رقابت‌ها

سازمان برای ارائه تمامی کارکردهای خود، از جمله فرایندهای پیشینه‌ها و سامانه‌ها به کارکنان رقابت‌جو وابسته است. متخصصان پیشینه‌ها یا افرادی که در حوزه‌های ارزیابی مدیریت و پیشینه‌ها در شرایطی عدم اطمینان مسئولیتی دارند عبارتند از:

الف- تعداد کارکنان برای ایجاد و کنترل پیشینه‌ها، طراحی و نگهداری سامانه پیشینه‌ها؛

پ- آگاهی بر خط‌مشی و فرآیند پیشینه‌ها؛

ت- آگاهی بر ریسک‌های مربوط به فرآیندها و سامانه‌های پیشینه‌ها و توانایی مدیریت ارشد در تصمیم‌گیری برای تعدیل‌های مناسب؛

ث- مدیریت ارتباطات بین مسئولیت‌های اجرایی برای سامانه‌های پیشینه‌ها و نظرات کاربران اجرایی؛

چ- کفایت رقابت برای ایجاد و کنترل پیشینه‌ها کارکنان؛

ج- فقدان کارکنان کلیدی با مهارت‌های حیاتی و دانش عمیق سازمانی یا تاریخی؛

ح- کیفیت نامناسب سطوح مهارتی کارکنان؛

خ- کفایت ابزارهای ارزیابی کارآیی یا شایستگی کارکنان؛

۵-۳-۴ حوزه‌های عدم اطمینان: منابع مالی و سرمایه‌ای

منابع مالی و سرمایه‌ای موجود برای مدیریت کارآمد، فرایندهای پیشینه‌ها و سامانه‌ها ، هم از محیط بیرونی، اقتصادی و تجاری و هم از سطح و میزان پشتیبانی مدیریت پیشینه‌ها در سازمان تأثیر می‌پذیرد. حوزه‌های عدم اطمینان شامل موارد زیر است:

الف- کفایت منابع مالی برای برآورده کردن تعهدات و اهداف مدیریت پیشینه‌ها؛

ب- کفایت منابع مالی برای خرید، ارتقاء یا نگهداری سامانه‌های مناسب و جامع؛

۵-۴ سامانه‌های پیشینه‌ها

حین ارزیابی تأثیر ریسک بر سامانه‌های ایجاد و کنترل پیشینه‌ها، طراحی سامانه، مسئله نگهداری، پایداری، تداوم، قابلیت سازگاری و امنیت را باید مورد توجه قرار داد. سامانه مورد استفاده سازمان طبق الزامات اقتصادی، تغییر در فعالیت‌ها، کارکنان و تغییر در ساختار و اندازه به مرور زمان تغییر می‌کند. بسیار ضروری است مدیریت ارشد درباره ریسک‌های سامانه‌های پیشینه‌ها اطلاع کافی داشته باشد و مسئولیت پاسخ‌گویی سازمان را به‌عهده بگیرد.

یادآوری ۱- تمامی ارجاعات به سامانه‌ها در این بخش را می‌توان ارجاعاتی به سامانه پیشینه‌های مطرح شده در بند ۳-۲-۱ نیز دانست .

یادآوری ۲- هنگام شناسایی ریسک‌های مرتبط با سامانه‌ها در سازمان‌هایی که استاندارد ISO/ IEC 27001 را به‌کار می‌برند، متخصصان پیشینه‌ها باید چگونگی تعدیل ریسک‌ها را توسط این استاندارد در برخی حوزه‌ها مدنظر قرار دهند. در سازمان‌هایی که استاندارد ISO/ IEC 27001 اجرا نمی‌شود، کنترل‌گرهای آن را می‌توان برای فعالیت‌های تعدیلی به‌کار گرفت. پیوست «پ » حاوی جدولی است که مصادیق حوزه‌های عدم اطمینان را با سامانه‌های پیشینه‌ها و کنترل‌گرهای ISO/ IEC 27001 به هم مرتبط می‌کند.

۵-۴-۱ حوزه‌های عدم اطمینان: طراحی سامانه

طراحی و پیکربندی سامانه برای ایجاد و دوام پیشینه‌ها ضرورت دارد. این امر با روند شناسایی ریسک برای فرایندهای رکوردها تداخل ایجاد می‌کند. مستندسازی گاهی از پیکربندی سامانه پایه‌ای برای پیدا کردن سایر حوزه‌های ریسک در سطح سامانه همچنین برای فرایندهای سامانه می‌سازد.

یادآوری – برای فرایندهای پیشینه در سامانه‌ها به بند ۵-۵ مراجعه کنید.

بر اساس تجارب کنونی، شناسایی ریسک‌ها در طراحی سامانه، به‌ویژه در بستر رقمی شامل موارد زیر است:

الف- تعریف پیشینه‌ها به‌گونه‌ای‌که سامانه، رکوردهایی مناسب و کافی برای مقاصد سامانه ایجاد و مدیریت کند؛

مثال- تمامی عناصر پیشینه‌ها در پایگاه اطلاعاتی تراکنشی، شناسایی و مدیریت می‌شود تا بتوان تراکنش‌ها را بازیابی و بازآفرینی کرد.

ب- شناخت مناسب و کافی الزامات نگهداری؛

مثال- دوره‌های نگهداری و «راه‌اندازی» برای فعالیت‌های سازمانی در عناصر پیشینه تعیین می‌شوند.

پ- شناسایی و مستندسازی تمامی فرایندهای ضروری پیشینه‌ها که باید سامانه آن‌ها را مدیریت کند؛

ت- اثربخشی طراحی سامانه‌های پیشینه‌ها مناسب برای کارکنان و فناوری سازمان؛

ث- مذاکره وابسته به پشتیبانی کارگزار؛

ج- دسترسی به مستندات کارگزار.

۵-۴-۲ حوزه‌های عدم اطمینان: نگهداری

نگهداری از سامانه‌های پیشینه‌ها در درجه اول به بسترهای نرم‌افزاری فناوری و جنبه‌های پشتیبانی سامانه‌ها اشاره دارد که متأثر از تغییرات ساختاری در سازمان، به کارگیری سامانه‌های جدید، تغییرات فناورانه و رقابت و همراهی در پشتیبانی فنی است.

حوزه‌های عدم اطمینان شامل موارد زیر است:

الف- تغییر در سامانه‌های کسب و کار سامانه‌های عملکردی که بر سامانه‌های پیشینه‌ها اثر می‌گذارند؛

ب- میزان مهارت مجریان سامانه و درک آنان از الزامات مدیریت پیشینه‌ها در سامانه؛

پ- قابلیت اعتماد سامانه‌های تأمین‌کننده و توانایی آنها در حفظ و نگهداری سامانه روزآمد از لحاظ فناوری؛

ت- کفایت مستندسازی رویه‌ها برای نگهداری عملیاتی؛

ث- کفایت مستندسازی فنی سامانه‌ها؛

ج- کفایت تهیه نسخه پشتیبان مستند شده برای سامانه‌های پیشینه‌ها؛

چ- کفایت بازسازی از نسخه‌های پشتیبان.

۵-۴-۳ حوزه‌های عدم اطمینان: پایداری و پیوستگی

پایداری سامانه‌های پیشینه‌ها به پایش تغییرات در بستر درونی و بیرونی سازمان بستگی دارد. به‌نحوی که سامانه پیشینه‌ها روزآمد می‌شوند تا به نیازهای حاصل از تغییر پاسخگو باشند.

طراحی پیوستگی برای سامانه‌های پیشینه‌ها، طراحی سازمان برای پیوستگی سازمانی را در نظر دارد. در غیاب یک برنامه‌ریزی مستمر برای کسب و کار در سازمان، متخصص پیشینه‌ها، سامانه‌های پیشینه‌ها را برای تثبیت اولویت‌ها و رویه‌های بازسازی بعد از صدمه دیدن خدمت‌رسانی ارزیابی می‌کند.

حوزه‌های عدم اطمینان شامل موارد زیر است:

الف- تغییر در بستر بیرونی و درونی که بر الزامات پیشینه‌ها سازمان تأثیر می‌گذارد؛

ب- کفایت روند پایش تضمین کیفیت برای شناسایی تغییرات حاصل در الزامات پیشینه‌ها؛

پ- کفایت ارزیابی از هزینه‌های واقعی اجرا و نگهداری سامانه‌های پیشینه‌ها، از جمله منابع انسانی؛

ت- کفایت شناسایی و مستندسازی سامانه‌های پیشینه‌ها؛

ث- نگهداری و دسترس‌پذیری به مستندات و اختصاصات سامانه؛

ج- کفایت مستندسازی تصمیمات گرفته شده حین اجرای سامانه‌های پیشینه‌های موجود برای تمامی کاربرانی که به آن‌ها نیاز دارند؛

چ- توانایی سامانه پیشینه‌ها برای اینکه قابل استفاده بودن پیشینه‌ها را حفظ نماید؛

ج- ظرفیت وارد کردن پیشینه‌ها از سامانه‌های قانونی و دیگر سامانه‌های تجاری.

۵-۴-۴ حوزه های عدم اطمینان : قابلیت سازگاری

سامانه های پیشینه‌ها به دیگر سامانه‌هایی که دارای نقطه آسیب پذیر هستند، وابسته و مرتبط هستند. حوزه های عدم اطمینان شامل موارد زیر است:

الف– کفایت روند شناسایی وتخصیص قابلیت سازگاری موردنیاز بین سامانه‌های پیشینه‌ها و دیگر سامانه های کسب وکار؛

ب– وابستگی نظام پیشینه‌ها به منابع داده ای بیرونی از سامانه پیشینه‌ها و قابلیت تبادل داده، پیونددهی یا ارجاع دهی به داده‌ها در این سامانه(مانند سامانه‌های ابری و دیگر خدمات بیرونی ذخیره سازی)؛

پ– سازگاری استانداردها یا مشخصه‌ها برای تبادل پیشینه‌ها یا قابلیت سازگاری بین سامانه‌ها؛

ت– اثربخشی قابلیت سازگاری سامانه پس از تغییرات یا ارتقاء فناورانه به سامانه‌های یکپارچه؛

ث– مدیریت فراداده‌ای مرتبط با کنترل پیشینه‌ها بین‌سامانه‌ها برای حفظ استفاده‌پذیری ومفهوم پیشینه‌ها.

۵-۴-۵ حوزه‌های عدم اطمینان: امنیت

ارزیابی ریسک امنیتی سامانه‌های پیشینه را با استفاده از سری استانداردهای ISO/ IEC 27000 به‌عنوان بخشی از سامانه مدیریت امنیت اطلاعات، هرگاه که لازم باشد، می‌توان به‌کار برد. استانداردها یا الزامات امنیت سامانه اطلاعات ملی موجود برای سامانه‌های پیشینه‌ها نیز قابل اجرا است.

پیوست‌های «ب تا ث» در استاندارد ISO/ IEC 27005، شامل نمونه‌هایی از حوزه‌های عدم اطمینان است که برای هر نوع سامانه اطلاعاتی به کار گرفته می‌شود. عدم اطمینانی‌های خاص‌تر برای سامانه‌های پیشینه‌ها موارد زیر را هم شامل می‌شود.

الف–کفایت خط‌مشی امنیت سازمان با توجه به پیشینه‌ها، فرایندهای پیشینه‌ها و سامانه‌ها؛

ب- توانایی برای تصویب و تضمین اجرای مقررات دسترسی و مجوزهای مربوط به پیشینه‌ها، فرایندهای پیشینه‌ها و سامانه‌ها

پ- خط و مشی کنترل برای شخص ثالث‌ها که به نمایندگی از سازمان کار می‌کنند و بر ذخیره، دسترسی و کنترل پیشینه‌ها و سامانه‌های پیشینه‌ها اثرگذار هستند.

۵-۵ فرایندهای پیشینه‌ها

شناسایی ریسک بر ایجاد پیشینه‌ها (عناصر پیشینه‌ها) و فرایندهای کنترل برای مدیریت پیشینه‌ها و سامانه‌های پیشینه‌های متمرکز است.

یادآوری - متخصص پیشینه‌ها برای راهنمایی درباره طراحی پیشینه‌ها و فرایندهای پیشینه‌ها به ISO 15489-1, ISO/TR 15489-1, ISO 23081-1, ISO 23081-2, ISO /TR 23081-3 مراجعه می‌کنند.

۵-۵-۱ حوزه‌های عدم اطمینان: طراحی پیشینه‌ها

حوزه‌های عدم اطمینان در فرایندهای طراحی عبارت‌اند از:

الف– فعالیت‌های کسب و کار برای شناسایی الزامات پیشینه‌ها به درستی تحلیل شده‌اند؛

ب- گردآوری الزامات پیشینه‌ها برای هر فرآیند کسب و کار، از جمله جامعیت نیازهای همه ذی‌نفعان قابل درک است؛

پ- کفایت طراحی پیشینه‌ها (مانند شناسایی محتوا و تعریف ابر داده‌ها برای شناسایی، توصیف، کاربرد، تاریخچه، رویداد و برنامه‌ریزی برای رویداد) نیازها را مرتفع می‌کند؛

ت- طرح شماتیک نام‌گذاری و طبقه‌بندی برای مقاصد موردنظر مناسب است.

۵-۵-۲ حوزه‌های عدم اطمینان: ایجاد پیشینه‌ها و اجرای سامانه پیشینه‌ها

حوزه‌های عدم اطمینان در فرایندهای ایجاد و اجرا به‌شرح ذیل می‌باشد:

الف- نقاط ایجاد و داده‌گیری کلیه عناصر پیشینه‌ها (از نظر زمان، انسجام و کامل بودن) برای فرایند کسب و کار و پیشینه‌ها مناسب هستند؛

ب- کارآمدی ادغام ایجاد پیشینه‌ها و فرایند پیشینه‌ها با فرایندهای کسب و کار در جایی که مناسب باشد؛

پ- مسئولیت‌های ایجادکنندگان پیشینه و کارگزاران (در صورت متفاوت بودن) در تراکنش‌های تجاری به درستی تعریف و مستند شده باشد؛

ت- تعیین مسئولیت‌ها برای گرفتن پیشینه‌های سازمان از محیط‌های بیرونی برآورنده نیازها باشد؛

ث- خصوصیات فراداده‌ای به اندازه کافی مستند و نگهداری شوند؛

ج- فرایندهای مدیریت و ثبت دسترسی به پیشینه‌ها به اندازه کافی مستند و پایش شوند.

۵-۵-۳ حوزه‌های عدم اطمینان: فراداده

حوزه‌های عدم اطمینان در فرایندهای مدیریت فراداده عبارت‌ند از:

الف- خصوصیات فنی فراداده برای مستندسازی پیشینه‌ها قابل دسترس است؛

ب- مدیریت ویژگی‌ها، امکان به روز رسانی را در صورت نیاز، فراهم می‌کند

۵-۵-۴ حوزه‌های عدم اطمینان: استفاده از پیشینه‌ها و سامانه‌های پیشینه‌ها

حوزه‌های عدم اطمینان در فرایندهای دسترسی و استفاده عبارت‌اند از:

الف- ثبات و خط سیر زمانی بازیابی و دسترسی به پیشینه‌ها در صورت نیاز؛

ب- کفایت مدیریت مجوزهای کاربر برای تمامی فرایندهای پیشینه‌ها؛

پ- مدیریت تخلفات امنیتی یا دیگر کنترل‌های دسترسی؛

ت- حفظو نگهداری پیشینه‌هایی‌که چه افرادی دسترسی داشته‌اندو یا تغییراتی در طول‌زمان‌در پیشینه‌ها داده‌اند؛

ث- کفایت روند آموزش کارکنان استفاده کننده از این فرایندها؛

ج- انطباق با این رویه‌ها.

۵-۵-۴-۱ حوزه‌های عدم اطمینان: نگهداری قابلیت استفاده

حوزه‌های عدم اطمینان در فرایندهای حفظ و نگهداری عبارتند از:

الف- حفظ هدفمند بودن فراداده‌های پیشینه‌ها در طول زمان، به ویژه وابستگی داده‌ها از سامانه‌های بیرونی یا پیوند به آن‌ها؛

ب- کفایت فرایندهای پیشینه‌های برای حفظ درستی و اعتبار پیشینه‌ها در طول زمان؛

پ- حفظ دسترس‌پذیری به پیشینه‌ها در طول زمان؛

ت- مدیریت استفاده و رمزگذاری پیشینه‌ها به منظور انتقال آنها؛

ث- کفایت مدیریت ویرایش‌های پیشینه‌ها در طول زمان؛

چ- کفایت نگهداری از تاریخچه رویداد پیشینه‌ها، برای تخمین هدفمند بودن پیشینه‌ها در طول زمان؛

ج- قدمت سخت‌افزار و نرم‌افزار (از جمله تغییرات قالب) در ارتباط با فرایند و سامانه‌های پیشینه‌ها.

مثال: ویرایش‌های قدیمی پیشینه‌ها رقمی ممکن است از طریق نرم‌افزارهای فعلی یا ویرایش نرم‌افزارها قابل دسترسی نباشد.

۵-۵-۵ حوزه‌های عدم اطمینان: نظم پیشینه‌ها

حوزه‌های عدم اطمینان در فرایندهای نظم پیشینه‌ها عبارت‌اند از:

الف- مرتب‌سازی پیشینه‌ها هنگام طراحی و مستندسازی آن‌ها انجام می‌شود؛

ب- رویه‌های مرتب‌سازی شامل فراهم ساختن پیشینه‌هایی است که دوره نگهداری پیشنهادی آنها گذشته است؛

مثال- پیشینه‌های مورد نیاز برای امور حقوقی یا تحت قانون آزادی اطلاعات جزو این پیشینه‌ها هستند.

پ- اجرای مرتب‌سازی، مستند می‌شود؛

ت- انجام آزمون به‌عنوان اینکه آیا بهبود قانونی ممکن است از سخت‌افزار یا ابزار ذخیره‌سازی کنار گذاشته شده باشد لازم است.

مثال- کفایت قالب‌بندی دوباره لوح‌های فشرده سخت رایانه‌ها و چاپگرها یا ابزارهای ذخیره‌سازی مانند نوارهـای حافظـه بـرای پاک کردن تمام پیشینه‌ها.

۶ تحلیل ریسک‌های شناسایی‌شده

۶-۱ کلیات

ریسک با تعیین پیامدهای بالقوه و احتمال شناسایی دوباره آن تحلیل می‌شود.

در مورد فرایندها و سامانه‌های پیشینه‌ها، پیامدها بر حسب حوزه‌های عدم اطمینان شناسایی و طبق معیارهای ریسکی که طبق بند ۴ برای سازمان تدوین شده‌اند، درجه‌بندی می‌شوند.کنترل‌های موجود و کارآیی و اثربخشی آن‌ها را هم باید در نظر گرفت.

۶-۲ تجزیه‌وتحلیل احتمال و برآورد احتمال

احتمال، امکان(یا تکرار) بروز رویداد ریسک می‌باشد. احتمال شناسایی ریسک‌های تشخیص داده شده

طبق ماهیت، حوزه عدم اطمینان و داده‌های در دسترس در دوره زمانی کافی برای حمایت از ارزیابی معتبر تحلیل می‌شود. هر ریسکی باید با توجه به ترکیبی از احتمال بعضی رویداد و پیامدهای ناشی از آن رویداد واقعی تخمین زده شود.

احتمال را می‌توان طبق روش‌های متفاوت بیان کرد، ولی طبیعتاً به میزان ریسک مربوط است.

روش‌های کیفی می‌توانند پیامد، احتمال و میزان ریسک را با مقادیری معنادار همچون«زیاد»، « متوسط» و« کم»، بیان کند..

روش‌های نیمه کمی، از مقیاس‌های امتیازدهی عددی برای پیامدها و احتمالات استفاده می‌کند و برای سنجش و میزانی از ریسک با کمک فرمول، آنها را با هم ترکیب می‌کند. مقیاس‌ها، رابطه‌ای خطی، لگاریتمی و یا غیره دارند و فرمول‌های مورد استفاده نیز متفاوت است.

از روش‌های کاملاً کمی از اعداد برای پیامدها و احتمال آن‌ها استفاده می‌کند، می‌توان درهرجاکه داده‌های عملکرد (آماری) برای فرایندهای پیشینه‌ها و سامانه‌ها برای مدت زمانی معقول‌در دسترس باشند، استفاده کرد.

درجه‌بندی تعداد رویدادها روی محور زمان برای فرایندهای پیشینه‌ها و سامانه‌ها مناسب است. یک مثال از چگونگی درجه‌بندی احتمال در جدول ۱ نشان داده شده است.

جدول ۱- مثال برای درجه‌بندی احتمال

نمره احتمال	شرح
۱	احتمال نادرهر ده سال یک‌بار یا کمتر رخ می‌دهد
۲	احتمال کم، هر سه سال یک‌بار یا کمتر رخ می‌دهد.
۳	احتمال متوسط، یک‌بار در سال رخ می‌دهد
۴	احتمال زیاد، بیش از یک‌بار در هر ماه رخ می‌دهد

۶-۲-۱ بستر: عوامل بیرونی

برآورد احتمال رویداد ریسک در محیط سیاسی – اجتماعی، اقتصادی – کلان، کسب و کار و فیزیکی براساس اطلاعات پیشین و فعلی مقوله‌های زیر طبقه‌بندی می‌شود.

الف- تغییرات حکومتی اجرایی؛

ب- گزارش‌های آماری و دیگر گزارش‌های مربوط به داده‌های کسب و کار و اقتصاد کلان؛

پ- الگوهای تغییر سیاسی و اجتماعی در حوزه ملی و / یا بین‌المللی که در حوزه جغرافیایی سازمان اثرگذار است؛

ت- میزان تغییر فناوری و پذیرش اجتماعی آن؛

ث- آب‌وهوای نامتعادل یا دیگر وقایع فیزیکی، از جمله تخریب زیرساخت‌ها؛

برای رویداد آب‌وهوای غیرعادی شاید کمتر بتوان مصادیقی پیشین پیدا کرد (مانند تندباد)در مورد عوارض طبیعی دیگر (مانند آتش‌سوزی یا خرابی‌های زیاد برق) هم همین طوراست ولی نمی‌توان گفت چنین وقایعی رخ نمی‌دهد. با توجه به اثرات بسیار تخریبی این وقایع، باید این احتمالات را هم در برآورد ریسک در نظر گرفت

۶-۲-۲ بستر، عوامل درونی

برآورد احتمال رویداد ریسک در حین تغییر ساختار و فعالیت‌های سازمان و استفاده آن از فناوری و منابع مبتنی بر اطلاعات مأخوذ ازپیشینه کنونی ان در ذیل طبقه‌بندی می‌شود:

الف- تغییرات در مدیریت ارشد (از جمله خصوصی‌سازی، ادغام و انتصاب) و تغییرات متعاقب آن؛

ب- الگوی پاسخ‌گویی خود سازمان به تغییرات بیرونی مانند تغییر مقررات – توسعه فناورانه و شرایط مالی؛

پ- رقابت کارکنان سازمان و نظام آموزش داخلی؛

ت- تغییر تعداد کارکنان.

توصیه می شود، این پیشینه از تغییرات اخیر در بستر ماهیت فعالیت‌ها سازمان، اندازه و فرهنگ سازمانی قرار گیرد.

مثال- سازمان‌هایی که بر رقابت اقتصادی تأکید دارند و یا قبلاً فناوری‌های نوین را پذیرفته‌اند، با احتمال بیشتری فناوری جدید را در مقایسه با سازمان خدمات غیرانتفاعی دارای ساختاری قدیمی و سنتی اجرا می‌کند. تغییر در بودجه و سرمایه عاملی بسیار محتمل در القای تغییرات درونی برای سازمان‌های غیرانتفاعی است. برآورد میزان احتمال تغییر داخلی مبتنی بر اطلاعات خاص سازمان است.

۶-۲-۳ سامانه‌ها

برآورد احتمال رویدادهای ریسک در سامانه‌های مبتنی بر اطلاعات فراهم شده در خصوص امنیت، تداوم، تأمین منابع و قابلیت سازگاری و نگهداری است (که همه این مشکلات، خطاهای اجرایی، مسائل موجود و مسائل مورد توجه در تثبیت و برآورد تعداد را شناسایی می‌کند).

مسئله امنیت سامانه‌های پیشینه‌ها و قابلیت سازگاری و تأمین منابع عمومی در مرحله طراحی و بازنگری تعیین و مستند می‌شود، در حالی که طراحی تداوم پذیری، جنبه‌ای از برنامه مدیریت ریسک کسب و کار عمومی سازمان است.

فرایندهای درگیرشده در طراحی سامانه‌ها، در معرض رویدادهای ریسک هستندکه بر فرایندهای پیشینه‌ها سامانه اثر می‌گذارد. هنگام برآورد احتمال رویدادهای ریسک در مرحله طراحی سامانه باید این نکته را در نظر داشت.

تحلیل پیشینه‌های ایجاد شده از رویه‌های نگهداری، باید بتواند پایه درستی برای ارزیابی میزان احتمال رویدادهای معکوس را فراهم کنند. نگهداری سامانه هر دو جنبه‌های فناورانه و رویه‌ای را دربرمی‌گیرد.

توصیه می شود، اطلاعات حاصل از پایش کنترل کیفی برای شناسایی موارد عدم انطباق در رویه‌های نگهداری را به‌منظور برآورد فراوانی یا تعداد شناسایی الگوهایی که ممکن است بروز کنند، تحلیل شود. توصیه می شود، چنین الگوهایی از عدم انطباق را در مقابل ویژگی های طراحی سامانه تحلیل کرد.

بازبینه‌ای مربوط به ممیزی و پیشینه‌های امنیتی مشابه یا تناقضات محدودیت‌های دسترسی باید به‌طور مشابه برای شناسایی هر نوع الگوی عینی و برآورد تعداد علل آن‌ها، تجزیه‌وتحلیل شود. پیشینه‌هایی که نسخه‌های پشتیبان سامانه‌رایانه‌ای را تأیید می‌کند و مطابق با ویژگی‌های طراحی آن‌ها می‌باشد، اطلاعاتی را که نمایان‌گر هر نوع آسیب‌پذیری و تکرار بروز آن‌ها است، فراهم می‌کند. ارزیابی احتمال رویدادهای بعدی مرتبط با سامانه، باید اولویت اختصاص داده شده به سامانه پیشینه‌های متفاوت را در نظر بگیرد.

۶-۲-۴ فرایند

فرایندهای سامانه‌های پیشینه‌های تثبیت شده به واسطه پاسخ‌های عملی به نقایص با رویدادهای خرد پیش‌بینی‌ناپذیر که به مرور زمان در غیاب بررسی آگاهانه و مستندسازی دقیق، قابل گردآوری و تهیه باشند، تغییراتی اساسی را تجربه می‌کنند. تجمع این تغییرات افزایشی در فرایندهای پیشینه‌ها، حوزه عدم اطمینان

بسیار وسیعی را درست عین رویدادهای خارجی، اصلی و نامطلوب تشکیل می‌دهند. احتمال تخطی از خصیصه‌های طراحی با تجزیه‌وتحلیل عدم تطابق موارد و تغییرات غیرعادی برآورد می‌شود که در شرایطی ویژه تأییدشده‌اند.

برآورد احتمال رویدادهای ریسک حوزه فرایندهای پیشینه‌ها مبتنی بر اطلاعات گردآمده از کاربرد و کنترل پیشینه‌ها و ابزارهایی مانند طرح‌های رده‌بندی یا مستندهای نظم دهی است. منابع اطلاعات مربوط شامل موارد زیر می‌باشد:

الف- آمار پیشینه‌ها ایجاد شده و به‌کار رفته؛

ب- پیشینه‌های نامنطبق حاصل از پایش کنترل‌کیفی؛

پ- پیشینه‌های تغییرات در طرح‌های فرادادهای؛

ت- پیشینه‌های استفاده از مستندهای نظم‌دهی؛

ث- پیشینه‌های تغییرات در محدودیت و میزان دسترسی‌ها؛

تجزیه‌وتحلیل شکاف از اطلاعات متراکم می‌تواند برای شناسایی حوزه‌های فعالیت سازمان باشد که در آن ثبت پیشینه‌ها جدید، الزامات مشخص، نیازمندی‌های تغییر یافته یا حوزه‌های جدیدی از فعالیت رعایت نمی‌شود.

تحلیل شکاف و پیشینه‌های نامنطبق باید مبنای شناسایی هر الگوی از تغییرات را فراهم نماید که در آن، سامانه‌های پیشینه‌ها آسیب‌پذیری نشان داده شده را به اندازه کافی پاسخ نداده است.

۷ ارزیابی ریسک

۷-۱ کلیات

هدف از ارزیابی ریسک، کمک به تصمیم سازی، طبق برون داده‌ها و نتایج حاصل از تحلیل ریسک است که مشخص می‌کند کدام ریسک‌ها در اولویت هستند و کدام یک به تمهیدات نیاز دارند.

ارزیابی ریسک شامل مقایسه سطح و میزان ریسک یافت شده طی فرایند تجزیه‌وتحلیل با معیارهای ریسک تثبیت شده هنگام بررسی زمینه است. بر اساس این مقایسه، نیاز به تمهیدات می‌تواند در نظر گرفته شود.

مقایسه پیامد رویدادهای مغایر و کفایت کنترل‌گرهای موجود را که محور اصلی فعالیت‌ها، اقدامات و یا تمهیدات هستند، می‌توان با جدول احتمالات کنار هم قرار داد تا به شناسایی ریسک‌ها کمک کند.

تصمیمات شامل موارد زیر است:

الف– آیا ریسک نیازمند تمهیدات است؟

ب– اولویت برای این تمهیدات کدام است؟

پ– آیا یک فعالیت را باید انجام داد؟

ت- کدام تعداد گزینه‌ها را باید برگزید؟

اگر گمان می‌رود تأثیر ریسک بسیار وسیع است و به حل‌وفصل بحران کمک می‌کند، به ارزیابی ریسک در ارتباط با عواقب نامطلوب، باید چنان اهمیت داد که موارد نادر یا موارد دارای رویداد بسیار کم اهمیت هم درنظرگرفته شود.

همان‌طور که در مقدمه گفته شد، پیامدهای رویدادهای ریسک در حکم فقدان پیشینه‌ها یا صدمه رسیدن به آنهاست که باعث می‌شودآن‌ها دیگر قابل اعتماد، کاربر پذیر، معتبر، کامل و ثابت به حساب نیایید و نتوانند از اهداف سازمانی حمایت کنند.

یک رویداد می‌تواند دارای طیفی از اثرات با مقیاس‌های متفاوت باشد و طیفی از اهداف و ذی‌نفعان متفاوت را تحت‌الشعاع قرار دهد. انواع اثراتی که باید تحلیل شود و نیز ذی‌نفعان تحت تاثیر را هنگام تعیین و تأیید معیارهای ارزیابی ریسک سازمان، تعیین و شناسایی کند. اولویت‌های مرتبط با پیشینه‌ها، هنگام ارزیابی اثرات تغییر، عدم اطمینان و رویدادهای مغایر مرتبط با پیشینه‌ها، مدنظر قرار می‌گیرند. اولویت پیشینه‌ها روند ارزیابی اثرات و پیامدها را طوری تحت‌تأثیر قرار می‌دهد که رویداد مغایری که به لحاظ کمی ناچیز تلقی می‌شود، درصورتی‌که پیشینه‌های از بین رفته یا آسیب دیده در حل و فصل بحران مهم باشند یا پیشینه‌های اصلی کسب و کار باشند، در واقع بسیار کلان و اثرگذار به حساب می‌آیند.

۲-۷ ارزیابی اثر رویدادهای مغایر(معکوس)

عواملی که باید درنظرگرفت عبارت‌اند از:

الف- تعداد کاربران و دیگر ذی‌نفعان که تحت‌تأثیر قرار گرفته‌اند؛

ب- تأثیر آسیب یا از بین رفتن پیشینه‌ها بر عملکردهای فعلی سازمان؛

پ- سنجه‌های که برای حل و فصل مختل شدن دسترسی به پیشینه‌ها وجود دارد؛

ت- زمان و انرژی صرف شده برای بهبود و جایگذاری پیشینه‌های آسیب دیده؛

ث- تأثیر صدمه یا از بین رفتن پیشینه‌ها بر حقوق مالکیت سازمان؛

چ- تأثیر صدمه یا از بین رفتن پیشینه‌ها بر توانایی سازمان در انجام تعهداتش نسبت به تمامی ذی نفعان؛

ج- الزامات قانونی و حقوقی ناشی از حوزه اطلاعات درباره صدمه دیدن، از بین رفتن و دسترسی غیرمجاز به پیشینه‌ها؛

ح- تأثیر بر وجهه عمومی سازمان‌ها.

این فهرست جامع و کامل نیست. میزان و اندازه و ماهیت سازمان، انتخاب این عوامل را تحت‌تأثیر قرار می‌دهد.

تأثیر بالقوه رویدادهای مغایر را می‌توان طبق نمونه‌ای که در جدول ۲ مطرح شده، با استفاده از عواملی که از نظر اندازه و ماهیت فعالیت‌های سازمان بسیار مهم تلقی می‌شوند، طبقه‌بندی کرد.

جدول ۲- نمونه‌ای از رده‌بندی ارزیابی اثر رویدادهای مغایر

کم	متوسط	زیاد	شدید
اختلال در محدودیت دسترسی	دسترسی غیرمجاز به پیشینه‌ها	دسترسی غیرمجاز به پیشینه‌ها بایستی گزارش داده شود	از بین رفتن وسیع، دسترسی غیرمجاز و صدمه دیدن
صدمه به مقادیر کم پیشینه‌ها در حوزه کاری	صدمه به مقادیر نسبتاً زیاد پیشینه‌ها در یک حوزه کاری	صدمه به بخش مهم پیشینه‌های اصلی امور چند حوزه	صدمه به بخش مهم پیشینه‌های اصلی در چندین حوزه مهم
از بین رفتن محدود داده	از بین رفتن داده / آسیب به قابلیت اعتماد و درستی	از بین رفتن داده‌ها / آسیب به قابلیت اعتماد و درستی، آسیب رسیدن به اعتبار	از بین رفتن داده‌ها / از بین رفتن قابلیت اعتماد و درستی / از بین رفتن اعتماد عمومی
خسارت بازیافتنی	عملیاتی که آسیب ندیده و پیشینه‌ها با تلاش قابل‌برگشت	از بین رفتگی تأییدشده ف اختلال به بیش از یک حوزه کاری	عملیات خراب‌شده، برگشت‌پذیری هزینه بر است و به زمان و انرژی نیاز دارد. پیشینه‌ها برگشت‌ناپذیر است.

۳-۷ ارزیابی ریسک

مقیاس تأثیر رویدادهای مغایر را می‌توان با جدول احتمالات به کمک روند شناسایی رویدادهای مغایر که در اندازه‌گیری برآورد ریسک باید مورد توجه قرار داد، مانند رویه‌های پایش، کنترل و طرح‌های آماده‌سازی در کنار هم قرار داد. نمونه‌ای از شیوه درجه‌بندی تأثیر رویدادهای مغایر را می‌توان بر حسب برآوردی احتمالی و در قالب فهرستی طبق جدول ۳ ارائه می‌شود.

پس باید ارزیابی‌ریسک را برسامانه‌ها و فرآیندهای‌رکوردهای سازمانی طبق اولویت‌های تعیین‌شده اعمال کرد.

جدول ۳- مثالی برای ارزیابی ریسک

رویداد			احتمال		تأثیر		
زمینه	سامانه	فرایند	فراوانی	کم	متوسط	زیاد	بسیار زیاد
-	-	پیشینه‌ها درست طبقه‌بندی نشده است و وضعیت دسترسی با خطا مواجه است	بالا ماهانه یا بیشتر	قابل اصلاح تحت رویه‌های موجود			
تغییرات در قانون حفاظت حریم خصوصی			متوسط سالی یک‌بار		تأثیر بر محدودیت‌های دسترسی به سامانه‌های شخصی و سرایت آن به عملکردهای دیگر		
	آسیب به عملکرد نمایه‌سازی سامانه پیشینه‌ها		متوسط سالی یک‌بار	قابل بازگشت و اصلاح از طریق رویه‌های فعلی			
		شناسایی اشتباه پیشینه‌ها برای تخریب	متوسط سالی یک‌بار	قابل بازگشت و اصلاح از طریق رویه‌های فعلی			
		دسترسی غیرمجاز به پیشینه‌ها	پایین / کم سه سال یک‌بار		غیرقابل‌برگشت، عذرخواهی از کارکنان		
	آسیب به تأمین برق به مدت ۸ ساعت		پایین / کم سه سال یک‌بار		تأثیر بر تمامی پیشینه-های سامانه، تراکنش ناموفق یک‌روزه		
تخریب ساختمان سامانه پیشینه‌ها بر اثر آتش‌سوزی			نادر: ده سال یک‌بار				از بین رفتن پیشینه‌های مهم ،صدمه به کارکردها، از بین رفتن اعتماد عمومی

بدین منظور برای استفاده از جدول ۳، رویدادهای ریسک شناسایی‌شده در مقوله مناسب آن‌ها (در سمت چپ) در ردیفی در سطح فراوانی متناسب وارد می‌شود و تأثیر آن‌ها براساس مقیاس‌های سمت راست جدول ۳ تعیین می‌شود. سازمان‌هامی‌توانند تأثیر و احتمال رسیدن به عددی را که اولویت تعیین شده در پاسخ به رویدادهای ریسک را نشان می‌دهد، رتبه‌بندی کند.

۸ به اشتراک‌گذاری ریسک‌های شناخته شده

ریسک‌های ارزیابی شده را باید در ثبات ریسک ثبت کرد (برای مثال به پیوست«الف» نگاه کنید) ثبات پیشینه، وسیله‌ای است که ریسک‌ها را برای مدیریت سازمان در اختیار قرار می‌دهد. ریسک‌های ثبت شده واندازه‌گیری‌های پیشنهاد شده برای پاسخ به آنها باید به حوزه مسئولیت سازمانی برای برنامه‌ریزی مدیریت ریسک سازمانی اطلاع داده شود.

هدف اصلی از تجزیه‌وتحلیل و برقراری ارتباط ریسک، شناسایی و تعیین اولویت‌ها و اتحاد رویکردها مناسب است . برقراری ارتباط با ریسک بخشی‌از مدیریت کارآمد ریسک برای اطمینان از بازشناسی وسیع ریسک‌های سازمان است. به‌منظوراطمینان از اینکه کنترل‌گرهای برگزیده شده برای حل‌وفصل ریسک‌ها همچنان کارآمد باقی می‌ماند، روند ارزیابی ریسک را باید در بازده‌های زمانی منظم پایش و بازنگری کرد.

پیوست الف

(اطلاعاتی)

نمونه‌ای از ریسک های وارد شده مستند در ثبت ریسک

توصیف ریسک	
فیلدهای ثبت شده	**ورودی اقلام**
شناسگر ریسک	۴
نام ریسک	ناتوانی در شناسایی پدید آورنده یک مدرک
نوع یا گروه‌بندی ریسک	مدرک
مالک ریسک	متصدی سامانه EDRMS
زمان شناسایی	۲۰۱۳/۱۰/۱۲
زمان آخرین بروز رسانی داده	۲۰۱۳/۱۰/۱۵
توصیف	ناتوانی در تشخیص پدید آورنده پیشینه ثبت شده
نمود ریسک (شرایط اجرای ریسک)	عدم اطمینان از واحد کاری اصلی پیشینه‌ها
هزینه در صورت وقوع (مالی یا غیر آن)	کم
احتمال	متوسط
تأثیر	زیاد
روش پیشگیری	بازنگری و تثبیت قالب‌های مدرک در EDRMS
روش حل و فصل	بازنگری و تثبیت قالب‌های مدرک در EDRMS
تاریخ بازنگری	۲۰۱۴/۱/۳۱
ریسک‌های مرتبط با ارجاعات	۳:۱۲
وضعیت ریسک و وضعیت فعالیت ریسک	شروع عمل کاهش ریسک
تاریخ آخرین ارزیابی	۲۰۱۳/۱۰/۱۵

پیوست «ب»

(اطلاعاتی)

مثال: بازبینه‌ای ای برای شناسایی حوزه‌های عدم اطمینان

یادآوری – شناسایی حوزه‌های عدم اطمینان نمونه‌ای از سیاهه است که می‌توان از آن به‌طور مستمر در سازمان برای شناسایی تغییرات و حوزه‌های عدم اطمینان طی دوره زمانی معین، مانند دوره سالانه استفاده کرد.

ب- ۱ عوامل بیرونی

ب-۱-۱ بستر سیاسی – اجتماعی

آیا سازمان فرآیندی برای پایش تغییرات در محیط بیرونی دارد؟

آیا روند پایش سازمان تغییرات زیر را ثبت کرده است؟

الف- قوانین و مقررات اثرگذار بر الزامات رکوردها؟

ب- خط‌مشی‌های دولتی اثرگذار بر الزامات، فرایندها و سامانه‌های پیشینه‌ها ؟

پ- دستورگان جدید عمل یا تغییر در استانداردهای مرتبط با فرایندها پیشینه‌ها و سامانه‌ها؟

ت- درخواست برای خدمات پیشینه‌ها ؟

ث- انتظارات ذینفعان از پیشینه‌ها ؟

آیا رویدادها یا تغییراتی در شرایط بیرونی وجود داشته است که اعتبار یا وجهه عمومی سازمان را طی سال گذشته تحت‌الشعاع قرار دهد؟

ب-۱-۲ محیط کلان اقتصادی و فناوری

آیا تغییراتی در مالکیت، ساختار یا کارکرد سازمان طی سال گذشته وجود داشته است؟

آیا تغییراتی در امور مالی، اساس مشتری مداری یا دیگر تغییرات در محیط کسب و کار که الزامات پیشینه‌ها را تحت‌الشعاع قرار می‌دهد وجود داشته است؟

آیا تغییراتی در سازوکارهای قانونی و مقررات سازمان وجود داشته است؟

آیاتوسعه‌های فناورانه در اجتماع وجود داشته است که بر سازمان تأثیری بالقوه داشته باشد؟

ب- ۱-۳ زیرساخت و محیط فیزیکی

آیا رویدادهای آب‌وهوایی شدید محلی یا منطقه‌ای یا دیگر بلایای طبعی در روند برنامه‌ریزی لحاظ می‌شود؟

آیارویدادهای انسانی و عوامل غیرطبیعی (مثل جنگ، تروریسم و اتفاقات عمومی) در روند برنامه‌ریزی برای رویدادهای مغایر وجود دارد؟

آیا سازمان برای نقص موجود در خدمات که بر ذخیره و سامانه پیشینه‌ها اثرگذار باشد آمادگی داشته است؟

ب- ۱-۴ تهدیدات امنیتی بیرونی

آیا اقدامات امنیت اطلاعات برای پشتیبانی از سامانه‌های پیشینه‌ها در مقابل دسترسی غیرمجاز و/ یا آسیب‌رسان کافی هستند؟

آیا امنیت فیزیکی ذخیره پیشینه‌های سازمان (ذخیره در شکل‌های کاغذی و الکترونیکی)کافی هستند و به‌طور مرتب کنترل می‌شوند؟

آیا امنیت سامانه‌های فناوری اطلاعات سازمان به اندازه کافی و به‌صورت مرتب پایش و آزمون می‌شوند؟

آیا سازمان برای نقایص احتمالی خدمات شخص ثالث که سامانه‌های پیشینه‌ها به آن‌ها نیاز دارند، برنامه‌ریزی کرده است؟

ب- ۲ عوامل درونی

ب ۲-۱ تغییرات سازمانی

- آیا مالکیت بر پیشینه‌ها در تمامی طرف‌های سازمان تثبیت شده و مستند شده است؟

- آیا روندهای مدیریت انتقال و توزیع پیشینه‌ها یا ادغام سامانه‌ها بعد از تغییر سازمانی وجود دارند؟

- آیا بعد از انتقال یا تغییر در مالکیت، حقوق دسترسی توسط طرف‌های درگیر، مورد توافق و مستند شده است؟

- آیا سامانه پیشینه‌ها باید از تغییرات عمده سازمانی با دیگر سامانه‌ها به درستی و به معنای واقعی ادغام شده است؟

- آیاشرایط قراردادی مناسب برای مالکیت، ابقاء وکنترل پیشینه‌ها در مواقع برون‌سپاری، برون‌مرزی وتغییرات مبهم وجود دارد؟

- آیا سازمان می‌تواند با تغییر رویه‌ها در بخش قرار داد خدمات طرف سوم برای پشتیبانی / مدیریت سامانه‌های پیشینه‌ها کنار بیایید؟

- آیا فرایندی برای بازنگری و به روز رسانی سیاست‌ها و رویه‌های مرتبط با سامانه پیشینه‌ها در دوره‌های زمانی منظم وجود دارد؟

- آیابرنامه‌ریزی در بردارنده هماهنگی‌ها برای پرداختن به موارد نقص در کارکنان کلیدی مسئول در امر فرایندها پیشینه‌ها و سامانه‌ها است؟

- آیارویه‌هایی برای سامانه‌های پیشینه‌ها در پاسخ به تغییر در کارکنان (مانند آموزش، بودجه‌ریزی و تعدیل نیرو) وجود دارد؟

- آیارویه‌ها برای بازنگری و بروز رسانی طرح‌های آمادگی برای موارد بحران متعاقب تغییر سازمانی وجود دارد؟

ب-۲-۲ تغییرات فناورانه

- آیا تغییر در فناوری بر قابلیت سازگاری بین سامانه پیشینه‌ها و دیگر سامانه‌ها تأثیر خواهد گذاشت؟

- آیا فناوری‌های در حال تغییر با سیستم عامل‌ها و سامانه‌های عملکردی سامانه‌های کنونی پیشینه‌ها سازگار است؟

- آیا رویه انجام نقل‌وانتقال سامانه‌های پیشینه‌ها به روز، مستند و کافی است؟

- آیا فرآیندهایی برای تضمین اینکه فراداده‌های پیشینه‌ها موقع معرفی فناوری جدید منتقل شده‌اند و نیز روند نقص و خرابی اطلاعات کنترل می‌شود وجود دارد؟

- آیا فرآیندهایی برای جلوگیری از جابه‌جائی غیرمجاز و نگهداری داده‌های غیرقابل استفاده هنگام نقل‌وانتقال و پیکربندی سامانه‌ها وجود دارد؟

- آیارویه‌ای برای مدیریت پیکربندی مجدد سامانه‌های پیشینه‌هاوفرایندها وجود دارد؟

- آیامسئولیت‌های لازم برای پیکربندی محدودسامانه‌ها، رویه‌ها وکنترل‌گرها، مستند و روزآمد شده‌اند؟

- آیا طرح به‌کارگیری تغییر در فناوری اثرگذار بر سامانه‌های پیشینه‌ها به اندازه کافی مدیریت شده است؟

- آیا خط و مشی‌های جاری به اندازه کافی فناوری‌های نوین را موقع به کارگیری در سازمان، تحت پوشش قرار می‌دهد؟

- آیا متخصصان و مدیریت فناوری اطلاعات از فواید آن در سامانه‌های پیشینه‌ها و مستندسازی پیشینه‌ها موقع معرفی فناوری جدید آگاه هستند؟

- آیا زیرساخت کنونی فناوری اطلاعات سازمان پشتیبان روند تغییر فناوری، در سامانه‌های پیشینه‌ها است؟

ب-۲-۳ منابع: افراد و رقابت‌ها

- آیا تعداد موجود کارکنان برای انجام فرایندهای پیشینه‌ها و مدیریت سامانه‌های پیشینه‌ها کافی است؟

- آیا کارکنان سازمان به اندازه کافی از خط و مشی‌های و فرایندهای مرتبط با پیشینه‌ها آگاهی دارند؟

- آیا مدیریت پیشینه‌ها را مدیریت ارشد سازمان پشتیبانی می‌کند؟

- آیا مدیریت ارشد، سازمان ریسک‌های فرایندهای پیشینه‌ها و سامانه‌ها را ریسک‌هایی تلقی می‌کند که باید رفع شوند؟

- آیا مسئولیت‌های پیشینه‌ها درصورت نیاز در تحلیل و شرح شغلی لحاظ شده است؟

- آیا ظرفیت‌های حاضر و قابلیت‌هایی در واکنش به تغییرات در محیط منظم بیرونی اثرگذار بر رویه‌ها ،خط مشی‌های پیشینه‌های سازمانی وجود داشته است؟

- آیا مسئولیت‌های متصدیان سامانه‌های پیشینه‌ها در ارتباط با کاربران سامانه‌ها تفهیم و مستند شده است؟

- آیا فرایندهایی برای تضمین روند انتقال مهارت‌های اساسی و دانش شیوه انجام کار، میان کارکنان مسئول پیشینه‌ها وجود دارد؟

- آیا برنامه آموزشی مداومی برای کارکنان مسئول رکوردها تدوین شده است؟

- آیا فرآیند پایش برای ارزیابی مهارت‌ها و شایستگی‌های کارکنان مسئول پیشینه‌ها وجود دارد؟

ب- ۲-۴ منابع: امورمالی و سرمایه‌ای

- آیا مدیریت پیشینه‌ها به اندازه کافی برای انجام اهداف وسیاست‌های مربوط به پیشینه‌ها و رویه‌های پیشینه‌ها در سازمان، تأمین مالی شده است؟

- آیاسامانه‌های پیشینه‌ها به‌اندازه کافی، به‌ویژه از نظر ارتقاء سامانه و نگهداری، بودجه‌بندی و حمایت شده‌اند؟

ب - ۳ سامانه پیشینه ها

ب-۳-۱ طراحی سامانه

- آیامستندسازی سامانه در بردارنده تعریف چیستی عناصر همه پیشینه‌ها است؟
- آیا فراداده و فرایندهای پیشینه‌ها به‌قدرکافی مستندسازی شده است؟
- آیا الزامات نگهداری توسط سامانه به‌اندازه‌کافی مدیریت و مستند شده است؟
- آیا تمامی فرایندهای پیشینه‌ها که سامانه مدیریت می‌کند شناسایی و مستند شده‌اند؟
- آیا فناوری انتخاب شده به شیوه‌ای مناسب با اندازه، پیچیدگی و فعالیت‌های سازمان انطباق دارد؟
- آیا فناوری به میزان مناسب از قابلیت عملکردی سامانه‌های پیشینه‌ها پشتیبانی می‌کند؟
- آیا سامانه وابسته به پشتیبانی کارگزاران است و قرار داد جاری خدمت به صورت مناسب تعریف شده است؟
- آیا مستندسازی کارگزاران به طرزی کافی در بردارنده تمامی عناصر لازم و طرح‌های کدگذاری است؟

ب - ۳-۲ نگهداری

- آیا تغییرات به‌طور مداوم در طراحی یا دیگر جنبه‌هایی همچون امنیت سامانه‌ها وجود دارد؟
- آیا سازمان به‌اندازه‌کافی رویه‌های مدیریت تغییر، برای اطمینان از اینکه تغییرات سامانه، تضمین، طراحی و کنترل شده است، دارد ؟
- آیا سطح مهارت‌های متصدیان سامانه و تلقی آنان از الزامات سامانه‌ها کافی و روزآمد است؟
- آیافراهم‌کنندگان سامانه‌ها توانایی خود را در به روز رسانی سامانه‌ها به طور منظم بررسی می‌کنند؟

- آیا مستندسازی شیوه‌های نگهداری از سامانه‌های پیشینه‌ها قابل دسترس است و به‌طور منظم بازنگری و روزآمد می‌شود؟
- آیا روند نقض و تخریب در فناوری که بر عملکردهای پیشینه‌ها تأثیر می‌گذارند پایش و مستند می‌شود؟
- آیا مستندسازی فنی سامانه‌ها قابل دسترس و روزآمد است؟
- آیا فرایندهای نسخه‌های پشتیبان و بازیابی برای سامانه‌های پیشینه‌ها به‌طور منظم آزمون، مستند و بازنگری می‌شود؟

ب -۳-۳ پایایی و دوام

- آیاسامانه‌های پیشینه‌ها طبق تغییرات دربستر بیرونی و درونی اثرگذار بر الزامات پیشینه‌های سازمان به‌طور منظم پایش و بازنگری می‌شود؟
- آیا پایش تضمین کیفیت سامانه‌های پیشینه‌ها برای شناسایی به روز دیگر تغییرات در سامانه‌ها بازنگری شده است؟
- آیا در مورد منابع مالی موردنیاز برای به‌کارگیری و حفظ سامانه‌های پیشینه‌ها و همچنین کارکنان شایسته مناسب برای این سامانه‌ها، ارزیابی کافی انجام می شود؟
- آیا سازمان تمامی سامانه‌هایی را که پیشینه‌ها ایجاد، نگهداری و مدیریت می‌کنند را شناسایی کرده است؟
- آیا ویژگی‌های سامانه‌های پیشینه‌ها به‌شیوه‌ای مناسب و کافی مستند و قابل دسترس شده است؟
- آیا رویه‌های نگهداری عملکردی تثبیت و مستند می‌شود؟
- آیا تصمیماتی که درباره اجرای سامانه‌های پیشینه‌ها گرفته می‌شود، برای تمامی کاربرانی که به آنها نیاز دارند، مستند، نگهداری و قابل دسترس می‌شود؟
- آیا قابلیت سامانه پیشینه‌ها برای حفظ قابلیت استفاده پیشینه‌ها مرتباً آزمون می‌شود؟
- آیا عملکرد سامانه‌های پیشینه‌ها بر حسب اهداف تعیین شده آن‌ها به‌طور منظم پایش و گزارش می‌شود؟
- آیا رویه‌های تثبیت شده برای مدیریت انتقال پیشینه‌ها به سامانه جدید پیشینه‌ها وجود دارد؟
- آیا ظرفیت معیار در سامانه‌های پیشینه‌ها برای وارد کردن آنها از سامانه‌های میرای دیگر سامانه‌های کسب و کار وجود دارد؟
- آیا تغییرات در دیگر سامانه‌هایی که سامانه‌های پیشینه‌ها به آنها وابسته یا به نوعی با آن‌ها در پیوند هستند، پایش و مدیریت می‌شود؟
- آیا جایی از فراهم آورندگان خدمات خارجی، مانند ذخیره، مبهم است؟
- آیا صدور پیشینه‌ها و یکپارچه‌سازی دوباره سامانه‌های پیشینه‌ها آزمون شده است؟
- آیا تاریخچه رویداد سامانه‌ها به اندازه کافی مدیریت می‌شود؟
- آیا برنامه‌ریزی سامانه کسب و کار به ویژه در بردارنده سامانه‌های پیشینه‌ها است؟
- آیا سامانه‌های پیشینه‌ها تداوم کسب و کار را با فراهم ساختن دسترسی به پیشینه‌ها در صورت رویداد و بحران، پشتیبانی می‌کند؟
- آیا طرح‌های پایایی در محل برای مدیریت نقص در خدمات‌دهی به سامانه‌های پیشینه‌ها وجود دارد؟

ب- ۳-۴ قابلیت سازگاری

- آیا سازمان قابلیت سازگاری که بین سامانه‌های کسب‌وکار و سامانه‌های نگه‌داشت پیشینه‌ها را شناسایی و مشخص می‌کند؟

- آیا وابستگی سامانه‌های پیشینه‌ها به منابع داده‌های بیرونی یا دیگر سامانه‌ها از جمله خدمات بیرونی مانند ذخیره ابری، شناسایی مستندسازی و به طرزی مناسب مدیریت می‌شوند؟

- آیا سازمان برای قابلیت سازگاری شناسایی‌شده از استانداردهای سازگار یا مشخصات تغییر تبادل پیشینه‌ها بین سامانه‌هایی که پایدارهستند استفاده می‌کند؟

- آیا تغییرات (مثل ارتقای نرم‌افزاری) در سامانه‌هایی که سامانه‌های پیشینه‌ها به آن‌ها وابسته هستند، یا نیاز به نگهداری قابلیت سازگاری آن‌ها وجود دارد، پایش و به صورت مناسب مدیریت می‌شود؟

- آیا تبادل پیشینه‌ها بین سامانه‌ها به شیوه‌ای مناسب در فراداده سامانه‌ها ثبت و به شیوه‌ای مناسب مدیریت می‌شود.

ب-۳-۵ امنیت

به پیوست «پ» که کنترل‌گرهای امنیت اطلاعات را در استاندارد ISO/IEC27001 را در مقایسه با موارد مطرح در اینجا ارائه می دهد، نیز مراجعه کنید.

یادآوری – در استاندارد ISO/IEC-27005، پیوست‌های «ب» تا «ت» نیز مثال‌هایی از حوزه‌های عدم اطمینان دارند که برای هر سامانه اطلاعاتی قابل کاربرد هستند.

- آیا خط مشی امنیت (اطلاعات) سازمان به اندازه کافی به امنیت پیشینه‌ها، فرایندهای پیشینه‌ها و سامانه‌ها می‌پردازد؟

- آیا محدودیت‌ها بر مجوزهای کاربران برای دسترسی، ایجاد و تغییر پیشینه‌ها قابل اجرا، عملی و مستند است؟

- آیا رویه‌های امنیتی برای تغییر حقوق دسترسی کاربران به سامانه‌ها هنگام تغییر نقش کارکنان یا انفصال آنان وجود دارد؟

- آیا خط مشی و رویه‌هایی برای کنترل شخص ثالث که به نیابت از سازمانی کار می‌کنند که به‌ویژه با مدیریت ذخیره‌سازی ایمن، دسترسی و فرایند پیشینه‌ها و سامانه‌های پیشینه‌ها سروکار دارد، وجود دارد؟

- آیا کارآیی خط‌مشی امنیت اطلاعات و کنترل‌گرها به شیوه‌ای منظم ارزیابی و اقدام اصلاحی می‌شود؟

ب- ۴ فرایند پیشینه‌ها

ب ۴-۱ طراحی پیشینه‌ها

- آیا تجزیه و تحلیل الزامات پیشینه‌های ثبت شده فعالیت‌های کسب و کار سازمان به‌شرح ذیل می‌باشد:

الف- مبتنی بر دانش کافی در باره کسب‌وکار سازمان است؛

ب- جامع است؛

پ- از نظر قوانین و مقررات مربوط کلی و منظم است؛

ت- دربرگیرنده تمامی طرف‌های موردنظر است؛

- آیا طراحی، تمامی کاربردهای مستند از پیشینه‌های موجود فعالیت ها را دربرمی‌گیرد؟

- آیا طراحی پیشینه‌ها برای هر سامانه مشخص، الزاماتی را در فراداده ها برای تعیین، توصیف، کاربرد، تاریخ رویداد و طراحی رویداد برآورده می کند؟

- آیا قواعد نامگذاری و طرح های رده بندی با اصطلاح شناسی سازمان تناسب دارد؟

ب-۴-۲ ایجاد پیشینه‌ها و اجرای سامانه‌های پیشینه‌ها

- آیا فرایند، خلق یا ایجاد پیشینه متناسب با سامانه و فرایند کسب و کار است. یعنی مبتنی بر فناوری مناسب، پایا، نظام یافته و به موقع می باشد؟

- آیا پیشینه‌ها به‌قدرکافی از نظر خلق یا ایجاد پیشینه‌ها قابل کنترل و شناسایی می باشد؟

- تاچه حد ممکن است فرایند ایجاد و خلق پیشینه‌ها با فرایند کسب وکار یکپارچه شوند یا ارتباطی نزدیک با تکمیل تراکنش داشته باشند؟

- آیا ایجادکننده پیشینه‌ها به‌قدر کفایت در این فرایند آموزش دیده اند؟

- آیا مسئولیت‌های ایجادوخلق پیشینه‌ها به قدر کافی مستند می شود و درصورت نیاز، از مسئولیت‌های کاربران سامانه کسب‌وکار قابل تمایز است؟

- آیا مسئولیت‌ها و فرایندهای ایجاد پیشینه‌ها از محیط بیرونی تعریف، تعیین و مستند شده است؟

- آیا دسترسی به پیشینه‌ها با الزامات قانونی/ حقوقی سازگار است و به‌صورت مناسب ثبت و پایش می‌شود.

ب-۴-۳ فراداده

- آیا ویژگی‌های خاص فراداده (از جمله موارد فنی آن) مستند شده و به منظور روزآمدسازی در دسترس قرار گرفته است؟

ب-۴-۴ کاربرد پیشینه‌ها و سامانه‌های پیشینه‌ها

- آیا کاربران موقع نیاز به پیشینه‌ها مدام به آنها دسترسی دارند؟
- آیا مجوزهای کاربران برای ایجادوخلق، دسترسی یا اصلاح پیشینه‌ها به شیوه‌ای مناسب در سامانه مدیریت می شود؟
- آیا مجوزها مبتنی بر نقش است نه شخص؟
- آیا پیشینه‌های قابل دسترس واصلاح پذیر برای پیشینه‌ها در سامانه در طول زمان نگهداری می شود؟

- آیا محدودیت‌های دسترسی در سامانه بیش از حد است و ثبت شده است و روش‌های مناسبی برای حل و فصل این تعارضات وجود دارد؟

- آیا کاربران پیشینه‌ها به اندازه کافی در فرایند سامانه ها آموزش می بینند؟

- آیا فرایندهایی برای جلوگیری از سوء استفاده و توزیع غیرمجاز پیشینه‌ها وجود دارد؟

ب-۴-۵ حفظ قابلیت استفاده

- آیا بستر ایجاد و کاربرد در پیشینه‌ها به‌قدر کافی مستند شده و در طول زمان در دسترس قرار می‌گیرد؟

- آیا روش‌هایی برای مدیریت وابستگی پیشینه‌ها به سامانه‌های خارجی (مانند داده ها یا دیگر پیوندها) برای حفظ جامعیت پیشینه‌ها وجود دارد؟

- آیا فرایندهای تضمین پایایی و اعتبار پیشینه‌ها در طول زمان (برای مثال: امنیت در برابر دسترسی غیرمجاز یا اصلاح) بررسی، مستندسازی و پایش می شود؟

- کدگذاری، موقع ذخیره سازی و انتقال پیشینه‌ها کجا استفاده می‌شود؟ آیا می‌توان آنها را رمزگشایی کرد؟

- آیا تجدیدنظرها، حاشیه نوشت‌ها و یادداشت‌ها و تاریخ تجدیدنظر پیشینه‌ها در طول زمان موردنیاز قابل دسترس است؟

- آیا تاریخ رویداد پیشینه‌ها را به اندازه کافی می توان برای اطمینان از تضمین جامعیت آنها در طول زمان نگهداری کرد؟

- آیا برای کنترل کاربردپذیری پیشینه‌های قدیمی برای مثال: وابستگی نرم افزاری و سخت افزاری، به اندازه کافی ذخیره فیزیکی برای پیشینه‌ها در قالب های مختلف وجود دارد؟

ب-۴-۶ استقرار پیشینه‌ها

- آیا مسئولین استقرار پیشینه‌ها ، مرتبط و در محل هستند؟

- آیا فرایندی برای بررسی مسئولیت‌های استقرار موجود هست؟

- آیا برای استقرار پیشینه‌ها رویه‌ای وجود دارد؟

- آیا نقش‌ها و مسئولیت‌های مربوط به استقرار، تعریف و مستند شده اند؟

- آیا استقرار بر پایه‌ای منظم و یکنواخت انجام می‌شود؟

الف- آیا فرایندی برای پرداختن به استثنائات وجود دارد؟

ب- آیا استقرار، از جمله تاییدپذیری به طرزی مناسب مستند شده است؟

پ- آیا روش آموزشی مناسبی برای اجرای خواست کارکنان مسئول پیشینه‌ها وجود دارد؟

ت- آیا روش‌های استقرار با سطح امنیتی موردنیاز متناسب است؟

با توجه به نیاز برای جلوگیری از بازسازی پیشینه‌ها از دستگاه‌های الکترونیکی و رسانه‌های ذخیره‌سازی کامل آیا فرایندهایی در محل وجود دارد تا اطمینان حاصل شود پیشینه‌ها به‌طورکامل تخریب شده است؟

پیوست پ

(اطلاعاتی)

راهنمای استفاده کنترل‌گرها از استاندارد

ISO/IEC27001، پیوست الف

متخصصان پیشینه‌ها باید حین شناسایی ریسک‌های مربوط به سامانه‌ها در سازمان‌هایی‌که از کنترل‌گرهای استاندارد ISO/IEC27001 استفاده می‌کنند به‌طرز عملکرد برخی از این کنترل‌گرها در حل‌وفصل ریسک‌ها ازبرخی حوزه‌های عدم اطمینان توجه کنند.

در سازمان هایی که در آنها از استاندارد ISO/IEC27001 استفاده می شود، کار ارزیابی ریسک برای فرایندها و سامانه‌های پیشینه‌ها که متخصصان پیشینه‌ها انجام می‌دهند از دانش وسیع و انطباق مناسب با استانداردISO/IEC27001 بهتر اجرا می شود

در سازمان‌هایی‌که از استاندارد فوق استفاده نمی‌کنند، کنترل‌گرهای‌آن را می‌توان درحکم منبعی برای فعالیت های حل و فصل موارد استفاده کرد. مطالعه بیشتر این استاندارد توصیه می‌شود.

جدول زیر حوزه های عدم اطمینانی را که در بخش ۵-۴ در کنترل‌گرهای استانداردهای فوق معرفی شده‌اند را ترسیم می‌کند.

در صورت امکان در ستون سمت چپ با عنوان «مشاهدات» ، نکاتی برای کمک به فهم بهتر کنترل‌گرهای امنیت اطلاعات استاندارد ISO/IEC27001 از نقطه نظر سامانه‌های پیشینه‌ها ارائه شده است.

جدول پ-۱ حوزه های عدم اطمینان

	حوزه های عدم اطمینان سامانه‌های پیشینه‌ها در ISO/TR18128	کنترل‌گرهای پیوست الف در ISO/IEC27001-2013	مشاهدات
حوزه های عدم اطمینان: طراحی سامانه‌ها			
۱	تعریف پیشینه‌ها به‌گونه‌ای که سامانه پیشینه‌ها را طبق اهداف سامانه ایجاد و مدیریت می‌کند.	بدون کنترل‌گر مرتبط با ISO/1EC27001	
۲	شناسایی کافی الزامات حفظ و نگهداری	بدون کنترل‌گر مرتبط با ISO/IEC27001	جابه جایی هدف اصلی امنیت اطلاعات نیست ولی از نظر سامانه پیشینه‌ها حوزه عدم اطمینان مهمی است به‌ویژه اگر سامانه هایی که پیشینه‌ها را ایجاد و کنترل کند در اجرای تصمیمات جابه‌جایی ناتوان باشند.
۳	شناسایی و مستندسازی کلیه فرایندهای پیشینه‌های لازمی را که سامانه باید مدیریت کند	بدون کنترل‌گرهای مرتبط با ISO/IEC27001	-
۴	کارآیی طراحی سامانه پیشینه هایی‌که مناسب فناوری و کارکنان سازمان باشد	**الف- ۱۰-۳-۱ طراحی و انطباق سامانه** : کاربرد منابع بایستی نظارت و تنظیم شود و طرح‌هایی از الزامات آتی ظرفیتها برای تضمین عملکرد موردنیاز سامانه استخراج شود.	الزامات ظرفیت‌ها و کاربرد منابع فقط دو جنبه از ارزیابی کارآمدی سامانه‌های رکرودهاست که باید طبق الزامات عملکردی به طور اساسی آزمون کرد
۵	مدیریت وابستگی به حمایت کارگزار	**الف- ۱۲-۵-۵- برون سپاری**: توسعه نرم افزار بایستی بوسیله سازمان تحت نظارت و نگهداری باشد.	اگر سامانه‌های پیشینه‌ها مبتنی بر نرم افزار تجاری تهیه شده توسط فراهم آوردندگان خارجی باشد، قابلیت اعتماد فراهم آورندگان خارجی را حین شناسایی ریسک ها باید مورد توجه قرار داد کنترل‌گرها ISO/IEC27001 می تواند از نظر سامانه-های پیشینه‌ها تحت نظر باشد.
۶	دسترسی به مستندات کارگزار	**الف-۱۰-۱-۱ رویه های کارکردی مستندسازی شده**: رویه های کارکردی مستندسازی شده، نگهداری شده و در اختیار تمامی کاربرانی که به آنها نیاز دارند، قرار می‌گیرد.	ISO/IEC27001 باید برای سامانه‌های پیشینه‌های نرم افزار مستندی به کار ببرد که مشتمل بر رویه های داخلی برای نگهداری آنها باشد.

حوزه‌های عدم اطمینان: نگهداری

۱	تغییرات در سامانه‌های کارکردی و کسب‌وکار که در سامانه‌های پیشینه‌ها تاثیرگذار است	**الف-۱۰-۱-۲ مدیریت تغییر:** تغییر در تسهیلات فرایند اطلاعات و سامانه‌هایی که بایستی کنترل شود. **الف-۱۰-۱۰-۴ گزارش‌های متصدی و اپراتور:** فعالیت‌های متصدیان و اپراتورها باید گزارش شود. **الف-۱۰-۱۰-۵ گزارش صدمات:** موارد نقض، گزارش‌دهی، تحلیل به طرزی مناسب چاره جویی شود.	کنترل‌گرهای ISO/IEC27001 را باید با الزامات ارتباطی و اشتراک‌گذاری برای اطمینان از آگاهی متخصصان پیشینه‌ها همراه کرد.
۲	سطح مهارت مدیران سامانه و فهم آنان از الزامات مدیریت پیشینه‌ها در سامانه	**الف-۱۰-۳-۱ مدیریت ظرفیت:** استفاده از منابع باید پایش و بررسی شده و الزامات ظرفیت آتی برای تضمین عملکرد مناسب سامانه پیش بینی شود. **الف-۱۰-۳-۲ پذیرش سامانه:** معیار پذیرش برای سامانه‌های اطلاعاتی جدید، بهینه‌سازی، و ویرایش‌های جدید باید تثبیت شود و آزمون‌هایی مناسب از سامانه(ها) طی دوره توسعه و قبل از پذیرش انجام شود.	کنترل‌گرها ISO/IEC27001 برای انتقال موارد عدم اطمینان درباره سطح مهارتی مدیران از نظر الزامات پیشینه‌ها کافی نمی-باشد. باید توجه ویژه‌ای به این حوزه داشت.
۳	اعتبار فراهم‌آورندگان سامانه‌ها و توانایی آنان در حفظ به روز نگهداشتن فنآوری سامانه	**الف-۱۲-۵-۵ توسعه برون-سپاری نرم افزار:** توسعه برون سپاری نرم افزار بایستی سرپرستی و پایش شود.	اگر سامانه‌های پیشینه براساس نرم افزار تهیه شده توسط فراهم آورندگان خارجی باشد، هنگام شناسایی ریسک‌ها لازم است توانایی فراهم‌آورندگان را هم در نظر گرفت. کنترل‌گرهای ISO/IEC27001 می تواند از نقطه نظر سامانه‌های پیشینه‌ها خیلی کلی باشد
۴	کفایت مستندسازی رویه ها برای نگهداری کارکردها	**الف- ۱۰-۱-۱ رویه های عملیاتی مستند:** رویه‌های عملیاتی بایستی مستند و پایش شده و قابل دسترس برای کلیه کاربران و کسانی که به آن نیاز	مستندسازی سامانه (فنی و رویه ای) را باید جزء پیشینه‌ها دانست و به طور مناسب از آنها نگهداری کرد.

		دارند باشد.	
۵	کفایت فنی مستندسازی سامانه	**الف- ۱۰-۱-۱ رویه‌های عملیاتی مستند:** رویه‌های عملیاتی بایستی مستند و پایش شده و قابل دسترس برای کلیه کاربران و کسانی که به آن نیاز دارند باشد.	مستندسازی سامانه (فنی و رویه ای) را باید جزء پیشینه‌ها دانست و به طور مناسب از آنها نگهداری کرد.
۶	کفایت رویه های نسخه‌های پشتیبان مستند برای سامانه های پیشینه‌ها	**الف-۱۰-۵-۱ نسخه‌های پشتیبان اطلاعاتی:** نسخه‌های پشتیبان اطلاعاتی و نرم افزار بایستی به طور منظم و طبق خط‌مشی توافق شده نسخه‌های پشتیبان، در نظر گرفته و آزمون شود.	کنترل‌گرهای ISO/IEC27001 نسخه پشتیبان تمام موارد عدم اطمینان مرتبط با نگهداری کاربردپذیری یا انتقال پیشینه ها را دربر نمی‌گیرد.
۷	کفایت بازپس‌گیری (ترمیم) از نسخه‌ها پشتیبان	**الف-۱۰-۵-۱ نسخه‌های پشتیبان اطلاعاتی:** نسخه‌های پشتیبان و نرم افزار بایستی به طور منظم و طبق خط مشی توافق شده نسخه‌های پشتیبان در نظر گرفته و آزمون شود.	کنترل‌گرهای ISO/IEC27001 نسخه پشتیبان تمام موارد عدم اطمینان مرتبط با نگهداری کاربردپذیری یا انتقال پیشینه‌ها را دربر نمی گیرد.

حوزه های عدم اطمینان: ثبات و تداوم

۱	تغییر در بستر درونی و بیرونی اثرگذار بر الزامات پیشینه‌های سازمان	بدون کنترل‌گر ISO/IEC27001	
۲	کفایت نظارت بر تخمین کیفیت برای شناسایی تغییرات در الزامات پیشینه‌ها	**الف- ۱۰-۱۰-۱ گزارش حسابرسی:** گزارش‌های حسابرسی برای ثبت فعالیت‌های کاربران، موارد استثناء رویدادهای امنیت اطلاعات تولید شده و نگه داشتن دوره مورد توافق برای کمک به تحقیقات آینده و نظارت بر کنترل دسترسی. **الف-۱۰-۱۰-۱ نظام پایش:** رویه های استفاده برای پایش، استفاده از تسهیلات فرایند اطلاعات که باید برآورد شود و نتایج آن باید به صورت منظم بازنگری شود.	کنترل‌گرهای ISO/IEC27001 یک جنبه از پایش نظام را شناسایی می کند اما سامانه‌های پیشینه‌ها به پایش تضمین کیفیت بسیار وسیعی نیازمند است.

۳	کیفیت ارزیابی هزینه‌های واقعی، اجرا و نگهداری سامانه‌های پیشینه ها از جمله منابع انسانی	**الف-۶-۱-۳ تخصیص مسئولیت های امنیت اطلاعات:** تمامی مسئولیت‌های امنیت اطلاعات به-صورت روشن تعیین می شود. **الف- ۱۰-۳-۱ طراحی و پذیرش سامانه:** استفاده از منابع باید بررسی و تنظیم شود و الزامات ظرفیتی برای تضمین عملکرد موردنیاز سامانه تعیین و طراحی شود.	کنترل‌گرهای ISO/IEC27001 جنبه های اقتصادی سامانه‌ها بجز کنترل‌گرهای مربوط به مسئولیت های داخلی سازمان در امنیت اطلاعات را تحت پوشش قرار نمی دهد. جنبه های اقتصادی سامانه‌های پیشینه‌ها می توانند حوزه مهمی از عدم اطمینان در سازمانی باشند که خط مشی کاهش هزینه ها را اجرا می کنند.
۴	کفایت شناسایی و مستندسازی سامانه‌های پیشینه‌ها	**الف- ۷-۱-۲ مالکیت بر دارایی ها:** تمامی اطلاعات و دارایی‌های مرتبط با تسهیلات فرایند اطلاعات باید با بخش تعیین شده از سازمان تحت مالکیت قرار گیرند.	کنترل‌گرهای ISO/IEC27001 نیاز به مستندسازی مالکیت بر سامانه‌ها را شناسایی می‌کنند اما شناسایی و مستندسازی کافی سامانه های پیشینه ها موردنیاز است.
۵	حفظ و دسترسی به اختصاصات و مستندات سامانه‌ها	**الف-۱۰-۷-۴ امنیت مستندسازی سامانه:** مستندسازی سامانه در مقابل دسترسی‌های غیرمجاز حفظ و حراست می شود	کنترل‌گرهای ISO/IEC27001 بر حفظ مستندات برای جلوگیری از ریسک‌ها بر امنیت اطلاعات تمرکز دارد. از نقطه نظر سامانه‌های کنونی پیشینه‌ها، نقطه دسترس در حفظ اطلاعات مهم است.
۶	مستندسازی کافی تصمیمات اخذ شده درباره اجرای سامانه‌های پیشینه‌های قابل دسترس برای کلیه کاربرانی که در آن نیازمند است	الف-۱۰-۷-**۴ امنیت مستندسازی سامانه:** مستندسازی سامانه در مقابل دسترسی‌های غیرمجاز حفظ و حراست می شود	به مورد بالا نگاه کنید.
۷	توانایی سامانه پیشینه‌ها در نگهداری از کاربردپذیری پیشینه‌ها	بدون کنترل‌گرهای مرتبط با ISO/IEC27001	کاربردپذیری بر امنیت اطلاعات تمرکز ندارد اما حوزه عدم اطمینان مهمی از نقطه نظر پیشینه‌هاست
۸	قابلیت تاثیر بر پیشینه‌ها از نقطه نظر سامانه‌های قانونی و دیگر سامانه های کسب و کار	بدون کنترل‌گرهای مرتبط با ISO/IEC27001	
۹	انتقال پیشینه‌ها به سامانه پیشینه های جدید به علت تغییر در الزامات پیشینه‌ها فنآوری	**الف-۱۲-۵-۲ بررسی فنی کاربردها بعد از تغییر سیستم‌های عامل:** وقتی سیستم‌های عامل تغییر می کند کارکردهای عمده کسب و کار برای تضمین عدم تاثیر سوء بر	انتقال از یک سامانه به سامانه دیگر را باید با توجه به حفظ محدودیت های پیشینه‌ها در طول زمان، در حکم حوزه ی عدم اطمینان شناسایی کرد.

		کارکردهای امنیت سازمانی بررسی و آزمون می شود	
۱۰	تغییر سامانه‌های دیگرکه سامانه پیشینه‌ها به آن وابسته است	بدون کنترل گرهای مرتبط با ISO/IEC27001	
۱۱	توانایی سامانه های ابری برای صدور پیشینه‌ها موقع نیاز و ادغام دوباره آن ها با سامانه های سازمانی	بدون کنترل گرهای مرتبط با ISO/IEC27001	
۱۲	کفایت تاریخچه رویداد سامانه های پیشینه‌ها، از جمله نگهداری برای طول عمر سامانه و مدیریت وابستگی به دیگر سامانه‌ها برای تضمین مناسب آن در طول زمان	**الف-۱۰-۱۰-۱ گزارش وضعیت:** گزارش وضعیت موجود مطابق با فعالیت و استثنائات و رویدادهای امنیت اطلاعاتی باشد که باید در یک دوره مورد توافق برای کمک به تحقیقات آینده و نظارت بر کنترل دسترسی تولید و نگه‌داری شود.	گزارش وضعیت موجود در ISO/IEC27001 در مورد فعالیت های کاربران از نظر پیشینه‌ها محدود است و باید در کنار دیگر فعالیت‌ها مرتبط با پیشینه‌ها برای تشکیل تاریخچه آن فراهم کرد.

۱۳	توانایی سامانه پیشینه‌ها در پشتیبانی از تداوم کسب و کار با فراهم ساختن دسترسی به پیشینه‌ها در رویدادهای بد	**الف- ۱۴-۱-۳ ایجاد و اجرای طرح‌های تداوم: از جمله طرح‌های امنیت اطلاعات**، برای حفظ و ذخیره کارکردها و تضمین اطلاعات قابل دسترس در سطح موردنیاز و در مقیاس‌های زمانی موردنیاز متعاقب نقص یا تخریب فرایندهای اصلی کسب و کار، طرح هایی توسعه و اجرا شود. **الف-۱۴-۱-۴ چارچوب طرح تداوم کسب‌وکار:** یک چارچوب واحد از طرح‌های تداوم کسب و کار برای تضمین اینکه همه طرح‌ها همساز هستند و به صورت همساز امنیت اطلاعات را در بر دارند و الویت‌های آزمون و نگهداری را شناسایی می کنند نگهداری می‌شوند. **الف-۱۴-۱-۵ آزمون، نگهداری وارزیابی طرح‌های تداوم کسب وکار:** طرح‌های تداوم کسب وکار به صورت مرتب برای تضمین به روز و کارآمد بودن آزمون و به روز می شوند.	کنترل‌گرهای ISO/IEC27001 درباره مدیریت تداوم کسب‌وکار بر الزامات امنیت اطلاعات تمرکز دارد این کنترل‌گرها از نقطه نظر پیشینه ها با الزامات پیشینه‌ها که عمدتاً بر پیشینه های کارکردی اصلی متمرکزند تکمیل می شوند.

		الف-۱۵-۱-۳ پشتیبانی از پیشینه های سازمانی: از پیشینه‌های مهم در مقابل تخریب، تکذیب و امحاء طبق الزامات کسب وکار منظم، قراردادی و مشروط پشتیبانی می‌شود.	
۱۴	طرح همگرا برای موارد تخریب خدمات	**الف- ۱۴-۱-۳ ایجاد و اجرای طرح‌های تداوم: از جمله طرح های امنیت اطلاعات،** برای حفظ و ذخیره کارکردها و تضمین اطلاعات قابل دسترس در سطح موردنیاز و در مقیاس‌های زمانی موردنیاز متعاقب نقص یا تخریب فرایندهای اصلی کسب و کار، طرح هایی توسعه و اجرا شود	کنترل‌گرهای ISO/IEC27001 درباره مدیریت تداوم کسب و کار بر الزامات امنیت اطلاعات تمرکز دارد، این کنترل‌گرها از نقطه نظر پیشینه-ها با الزامات پیشینه‌هایی که عمدتاً بر دغدغه های تداوم کسب و کار متمرکزند، تکمیل می‌شوند.

حوزه عدم اطمینان- قابلیت سازگاری

۱	کفایت شناسایی و تخصیص قابلیت سازگاری موردنیاز بین سامانه‌های پیشینه‌ها و دیگر سامانه‌های کسب و کار	**الف-۱۰-۸-۱ رویه ها و خط مشی های تبادل اطلاعات:** خط مشی تبادلات رسمی، رویه ها و کنترل گرها باید برای پشتیبانی از تبادل اطلاعات از طریق استفاده از کلیه تسهیلات ارتباطی وجود داشته باشد. **الف-۱۰-۸-۲ موافقت نامه‌های تبادل:** برای تبادل اطلاعات و نرم افزار بین سازمان و طرف‌های خارجی باید توافقاتی صورت گیرد. **الف- ۱۰-۸-۵ سامانه اطلاعات کسب‌وکار:** برای پشتیبانی از اطلاعات مرتبط با روابط متقابل بین سامانه‌های اطلاعات کسب‌وکار، خط مشی‌ها و رویه‌های ایجاد شده و به کار می‌روند.	کنترل‌گرهای ISO/IEC27001 بر مستندسازی رسمی امنیت اطلاعات برای تبادل اطلاعات بین سامانه ها تمرکز دارد. از نظر پیشینه‌ها، قابلیت سازگاری بین سامانه‌های پیشینه‌ها و دیگر سامانه‌ها می تواند موضوعی معمول و عملیاتی باشد و از این رو، حوزه عدم اطمینان تلقی می شود. شکست در قابلیت سازگاری سامانه دسترسی به پیشینه‌ها و کاربردپذیری آنها را تحت تاثیر قرار می‌دهد.
۲	وابستگی سامانه‌های پیشینه‌ها بر منابع داده های خارج از سامانه پیشینه‌ها و ظرفیت تبادل داده ها با این سامانه ها (مانند خدمات ذخیره ای مبهم یا دیگر خدمات خارجی)	**الف-۶-۲-۱ شناسایی ریسک‌های مرتبط با طرف های خارجی:** ریسک های اطلاعات و تسهیلات فرایند اطلاعات از فرایندهای کسب و کار مشتمل بر طرف های خارجی، باید شناسایی و کنترل‌گرها مناسب	امنیت داده ها در فراهم آورندگان خدمات طرف سوم تنها مورد قابل توجه از نظر سامانه پیشینه‌ها نیست اما کنترل‌گرها مناسب هستند.

		قبل از تائید دسترسی اعمال شود. **الف-۶-۲-۳ پرداختن به امنیت در توافقات طرف سوم:** توافقات با طرف های سوم شامل دسترسی، فرایند، به اشتراک گذاری یا مدیریت اطلاعات سازمانی و تسهیلات فرایند اطلاعات یا افزودن محصولات یا خدمات به تسهیلات فرایند اطلاعات، کلیه الزامات امنیتی مرتبط را دربر می گیرد.	
۳	سازگاری استانداردها یا ویژگی‌های تبادل پیشینه‌ها یا قابلیت سازگاری بین سامانه ها	**الف-۱۵-۲-۲ کنترل سازگاری حتی اطلاعات:** سامانه ها برای سازگاری با استانداردهای اجرای امنیت به صورت منظم کنترل می شوند.	کنترل گرهای ISO/IEC27001 براستانداردهای اجرای امنیت تمرکز دارند، از نقطه نظر پیشینه ها، کاربرد این استاندارد بین المللی، در سامانه پیشینه‌ها می تواند نوعی حوزه عدم اطمینان یاشد. این امر باعث تقویت استانداردهای قابلیت سازگاری می شود.
۴	قابلیت سازگاری موثر سامانه بعد از تغییر یا ارتقای فناورانه یک یا هر دو سامانه یکپارچه	**الف-۱۰-۳-۲ طراحی و پذیرش سامانه:** معیارهای پذیرش برای سامانه های اطلاعاتی جدید، موارد ارتقاء و ویرایش‌های جدید، تثبیت می‌شود و آزمون‌هایی مناسب از سامانه ها طی روند توسعه و قبل از پذیرش انجام می‌شود.	
۵	مدیریت فراداده مرتبط با کنترل گرهای بین سامانه ها برای به کارگیری و معنابخشی مداوم به پیشینه‌ها	بدون کنترل‌گرها مرتبط با ISO/IEC27001	توانایی سامانه‌های پیشینه‌ها در پشتیبانی از الزامات فراداده‌ها می تواند حوزه عدم اطمینان مهمی باشد. وقتی سامانه های پیشینه‌ها نتواند فراداده هایی از فرایندهای پیشینه‌ها را مدیریت کند معنا و کاربرپذیری پیشینه‌ها آسیب می بیند.

حوزه عدم اطمینان: امنیت (تمامی این حوزه عدم اطمینان را باید کنترل‌گرهای ISO/IEC27001 تحت پوشش قرار دهند). موارد زیر درباره کنترل گرهای بسیار معروف هستند.

۱	کفایت خط مشی سازمان با توجه به پیشینه ها، فرایندهای پیشینه‌ها و سامانه های پیشینه‌ها	**الف-۵-۱-۱ مدرک خط مشی امنیت اطلاعات:** مستندات خط مشی امنیت اطلاعات توسط مدیریت تصویب می‌شود و	موقع شناسایی ریسک‌ها در این حوزه، متخصصان پیشینه ها باید اطمینان یابند که خط مشی امنیت اطلاعات

		در اختیار تمامی کارکنان و طرفهای خارجی قرار می گیرد. **الف-۵-۱-۲ بازنگری خط مشی امنیت اطلاعات :** خط مشی امنیت اطلاعات بایستی در فواصل زمانی برنامه ریزی شده یا در صورت ایجاد تغییرات مهم برای اطمینان از تداوم شایستگی کفایت و اثربخشی بازنگری شود.	سازمان مشتمل بر نیازهای خاص پیشینه‌ها و سامانه های پیشینه‌ها است و نیز باید مطمئن شوند خط مشی ها و رویه ها هماهنگ با خط مشی امنیت اطلاعات است.
۲	توانایی محافظت و اجرای مقررات دسترسی و مجوزهای مرتبط با پیشینه، فرایند های پیشینه‌ها و سامانه‌های پیشینه‌ها	**الف-۱۱-۱-۱ خط مشی کنترل دسترسی:** خط مشی‌کنترل دسترسی براساس الزامات کسب و کار و امنیت برای دسترسی ایجاد، مستندسازی و بازنگری می شود. **الف-۱۱-۲-۱ ثبت نام کاربر**: برای تایید و لغو دسترسی به تمامی خدمات و سامانه‌های اطلاعات فرایند ثبت نام رسمی کاربران و انصراف از آن بایستی وجود وجود داشته باشد. **الف-۱۱-۲-۲ مدیریت امتیازها** تخصیص و کاربرد امتیارها محدود و کنترل شده است. **الف-۱۱-۲-۳ مدیریت گذر واژه کاربر:** اختصاص گذر واژه باید از طریق فرایند مدیریتی رسمی کنترل شود. **الف-۱۱-۲-۴ بازنگری حقوق دسترسی کاربران:** مدیریت، حقوق دسترسی کاربران را مرتباً با فرایند های رسمی بازنگری می کند. **الف-۱۱-۶-۱ محدودیت دسترسی به اطلاعات:** دسترسی به اطلاعات وسامانه کاری توسط کاربران و کارکنان پشتیبانی براساس خط مشی کنترل دسترسی مشخص محدود می شود.	زمانی که متخصصان ریسک ها را در این حوزه شناسایی می‌کنند. باید محدودیت مجوزها برای دسترسی، ایجاد و تغییر پیشینه‌ها را در نظر بگیرند. مجوزها باید براساس خط مشی کنترل دسترسی تعریف شده در خط مشی امنیت اطلاعات باشد.
۳	خط مشی و کنترل طرف های سوم که به نیابت از سازمان کار می کند که بر ذخیره، دسترسی و فرایند پیشینه‌ها و سامانه‌های پیشینه‌ها اثرگذار است.	**الف-۶-۲-۳ لحاظ کردن امنیت در توافقات طرف سوم:** توافق با طرف‌های سوم از جمله دسترسی، فرایند، به اشتراک گذاری یا مدیریت امنیت اطلاعات سازمان در خدمات اطلاعاتی، تمامی الزامات امنیتی را در	

		بر می گیرد. **الف-۱۰-۲-۱ ارائه خدمات:** تضمین می شود که کنترل‌گرهای خدمات، تعریف خدمات و سطوح ارائه گنجانده شده در توافقات طرف سوم توسط طرف سوم اجرا، عملیاتی و ابقا می‌شود. **الف- ۱۰-۲-۲ پایش و بازنگری خدمات طرف سوم:** خدمات، گزارش و پیشینه های فراهم شده توسط شخص ثالث به صورت مرتب پایش و بازنگری شده و موارد حسابرسی به طور مرتب اعمال می شود. **الف- ۱۰-۲-۳ مدیریت تغییر در خدمات طرف سوم:** تغییر در تامین خدمات از جمله نگهداری و بهبود خط مشی امنیت اطلاعات موجود، رویه ها و کنترل‌گرهای کنونی در امنیت اطلاعات بایستی با در نظر گرفتن منتقدانه فرایند و سامانه‌های کسب‌وکار درگیر وارزیابی مجدد ریسک‌ها مدیریت شود.	

کتاب‌نامه

1- ISO 15489‑1:2001, Information and documentation — Records management — Part 1: General
2- ISO/TR 15489‑2:2001, Information and documentation — Records management — Part 2: Guidelines
3- ISO 23081‑1:2006, Information and documentation — Records management processes — Metadata
for records — Part 1: Principles
4- ISO 23081‑2:2009, Information and documentation — Managing metadata for records — Part 2: Conceptual and implementation issues
5- ISO/TR 23081‑3:2011, Information and documentation — Managing metadata for records —
Part 3: Self-assessment method
6- ISO 27001, Information technology — Security techniques — Information security management
systems — Requirements
7- ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk
management
8- ISO 31000:2009, Risk management — Principles and guidelines
9- IEC 31010:2009, Risk management — Risk assessment techniques