استاندارد ایران-ایزو-
آی ای سی-تی آر
۲۷۰۰۸
چاپ اول
دی ۱۳۹۱

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

INSO-
ISO/IEC-TR
27008
1st. Edition
Identical with
ISO/IEC TR
27008:2011
Jan.2013

فناوری اطلاعات- فنون امنیتی-

راهنماهایی برای ممیزان در کنترل‌های امنیت اطلاعات

Information technology _ Security techniques _ Guidelines for auditors on information security controls

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

موسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد 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.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و موسسات علمی، پژوهشی تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولید کنندگان، مصرف کنندگان، صادر کنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی 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 کمیته ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که موسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند در کمیته ملی طرح و بررسی و در صورت 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 شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که موسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

موسسه استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان بین‌المللی استاندارد ۳۴۰(ISO[1])، کمیسیون بین‌المللی الکترونیک (IEC[2]) و سازمان بین‌المللی 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 بهره-گیری می‌شود.

موسسه استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش‌بینی 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. موسسه 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 موسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، موسسه استاندارد این گونه سازمان‌ها و موسسات را بر اساس ضوابط نظام تایید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامه تایید صلاحیت به آنها اعطا و بر عملکرد آنها نظارت می‌کند. ترویج دستگاه بین‌المللی 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 for Legal Metrology (Organization International de Metrologie Legal)
4 - Contact Point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات- فنون امنیتی- راهنماهایی برای ممیزان در کنترل‌های امنیت اطلاعات»

رئیس:	**سمت و/یا نمایندگی**
قسمتی، سیمین (فوق لیسانس، فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (لیسانس، مهندسی کامپیوتر نرم‌افزار)	مدیر کل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات ایران
اعضا: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (لیسانس، مهندسی الکترونیک)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سعیدی، عذرا (فوق لیسانس، مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
طی‌نیا، رضا (فوق لیسانس، فناوری اطلاعات)	مدیر عامل شرکت کاسیس
عبداله پور، امید (لیسانس، کامپیوتر)	کارشناس سازمان ملی استاندارد
علیخانی، مجتبی (لیسانس، مهندسی برق مخابرات)	مدیر توسعه طرح‌ها و پروژه های شرکت امواج آینده صدرا

فرهاد شیخ احمد، لیلا (فوق لیسانس، مهندسی کامپیوتر نرم‌افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
فولادیان، مجید (فوق لیسانس، مهندسی مخابرات)	مشاور سازمان فناوری اطلاعات ایران
فیاضی، مهدی (لیسانس، مهندسی الکترونیک)	کارشناس مسئول تدوین استاندارد و امنیت شبکه سازمان فناوری اطلاعات ایران
میرزایی رضایی، طیبه (فوق لیسانس، فیزیک)	رییس اداره تدوین استاندارد سازمان فناوری اطلاعات ایران
یزدیان، علی (دکترا، مهندسی برق)	هیات علمی و رییس مرکز آپای دانشگاه تربیت مدرس
یوسف زاده، بهاره (لیسانس مهندسی برق)	کارشناس سازمان ملی استاندارد ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی- راهنماهایی برای ممیزان در کنترل‌های امنیت اطلاعات» که پیش نویس آن آگاهی کمیسیون‌های مربوط به وسیله سازمان فناوری اطلاعات ایران تهیه و تدوین شده و در صد و نود و هفتمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۷/۳ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان 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 زمینهٔ 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 تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC TR 27008:2011, Information technology — Security techniques — Guidelines for auditors on information security controls

فناوری اطلاعات- فنون امنیتی- راهنماهایی برای ممیزان

در کنترل‌های امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، فراهم آوردن راهنمایی برای بازنگری پیاده‌سازی و عملیات کنترل‌ها است که شامل وارسی[1] موارد انطباق فنی کنترل‌های سامانه‌های اطلاعاتی در مقایسه با استانداردهای امنیت اطلاعات برقرار شده در سازمان‌ها می‌باشد.

این استاندارد ملی در تمامی انواع و گستردگی سازمان‌ها شامل شرکت‌های دولتی و خصوصی، نهادهای دولتی و سازمان‌های غیرانتفاعی که بازنگری امنیت اطلاعات و وارسی انطباق فنی را هدایت می‌کنند، کاربردپذیر است. این گزارش فنی به منظور ممیزی سامانه‌های مدیریت نیست.

۲ مراجع الزامی

مدارکی که به عنوان منبع به آن‌ها در ادامه ارجاع داده می‌شود در متن استاندارد ملی ایران مورد استفاده قرار گرفته است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

در صورتی که به آگاهی با ذکر تاریخ انتشار آن ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نمی‌باشد، و در غیر این صورت همواره تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است :

2-1 ISO/IEC 27000:2009, Information technology — Security techniques — Information security management systems — Overview and vocabulary

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود:

1- Check

۱-۳

موضوع بازنگری[1]

موردی [2] ویژه که بازنگری می‌شود.

۲-۳

هدف بازنگری[3]

بیانیه‌ای[4] که دستاوردهای به دست آمده از یک بازنگری را توصیف می‌کند.

۳-۳

استاندارد پیاده‌سازی امنیت

مستندی که روش‌های مجاز برای تحقق بخشیدن امنیت را مشخص می‌کند.

۴ ساختار گزارش فنی حاضر

این گزارش فنی توصیف فرآیند بازنگری کنترل امنیت اطلاعات که شامل وارسی انطباق فنی می‌باشد را در بر می‌گیرد.

اطلاعات پیش‌زمینه در بند ۵ ارائه شده است.

بند ۶ کلیاتی از بازنگری‌های کنترل امنیت اطلاعات را ارائه می‌کند.

روش‌های بررسی در بند ۷ و فعالیت‌ها در بند ۸ ارائه شده‌اند.

وارسی انطباق فنی توسط پیوست الف و گردآوری اطلاعات اولیه توسط پیوست ب، پشتیبانی شده است.

۵ پیش‌زمینه

کنترل‌های امنیت اطلاعات سازمان باید بر اساس نتایج به دست آمده از ارزشیابی مخاطرات به عنوان قسمتی از فرآیند مدیریت مخاطرات امنیت اطلاعات به منظور کاهش مخاطره به سطح قابل قبول، انتخاب شوند. بنابراین سازمان‌هایی که تصمیم به پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS)[5]

1- Review object
2- Item
3- Review objective
4- Statement
5- Information system management system

ندارند ممکن است راه کارهای دیگری برای انتخاب، پیاده‌سازی و نگهداری کنترل‌های امنیت اطلاعات برگزینند.

معمولا کنترل‌های امنیت اطلاعات یک سازمان، با استفاده از پیاده‌سازی کنترل‌های فنی امنیت اطلاعات محقق می‌شود، به طور مثال هنگامی‌که دارایی‌های اطلاعاتی[1] شامل سامانه‌های اطلاعات شود.

کنترل‌های فنی امنیت یک سازمان باید بر اساس استانداردهای فنی امنیت اطلاعات[2] تعریف، مستند[3]، پیاده‌سازی و نگهداری شود. با گذر زمان، عوامل داخلی[4]، مانند اصلاحیه‌های[5] سامانه‌های اطلاعات، پیکربندی‌های کارکردهای امنیتی و تغییرات سامانه‌های اطلاعات پیرامونی[6] و عوامل خارجی مانند پیشرفت[7] در مهارت‌های حمله[8]، ممکن است اثراتی منفی بر اثر بخشی کنترل‌های امنیت اطلاعات و در نهایت استانداردهای امنیت اطلاعات سازمانی داشته باشد. سازمان‌ها باید برنامه کاملا دقیقی برای کنترل تغییرات امنیت اطلاعات داشته باشند. همچنین باید به طور منظم درستی پیاده‌سازی استانداردهای امنیتی و چگونگی عملیاتی شدن آن را بازنگری نمایند. وارسی انطباق فنی که در استاندارد ملی ایران به شماره ۲۷۰۰۲: سال ۱۳۸۷ آمده به عنوان یکی از کنترل‌هایی که به صورت دستی[9] و/یا به صورت خودکار به وسیله بازنگری‌های فنی با کمک ابزارهای خودکار صورت می‌گیرد، گنجانده شده است. این امر ممکن است به وسیله نقشی که در اجرای کنترل‌ها درگیر نمی‌باشد مانند صاحبان سامانه‌ها، مسئولین کنترل‌های ویژه یا متخصصان امنیت اطلاعات داخلی یا خارجی که شامل ممیزان فناوری اطلاعات می‌باشد، ایفا شود.

بازنگری خروجی وارسی انطباق فنی، نشان دهنده میزان واقعی انطباق فنی با استانداردهای پیاده‌سازی شده در امنیت اطلاعات سازمان است. این شواهد تضمینی را در هنگامی که وضعیت کنترل‌های فنی مطابق با استانداردهای امنیت اطلاعات باشد ارائه می‌کند یا در غیر این صورت مبنایی برای پیشرفت می‌گردد. زنجیره‌ی گزارش ممیزان، باید به طور واضح در آغاز بازنگری برقرار شود و از یکپارچگی فرآیند گزارش‌دهی اطمینان حاصل کرد. این قدم‌ها باید طی شود تا اطمینان حاصل نمود که:

1- Information asset
2- Technical information security standards
3- Documented
4- Internal factors
5- Amendment
6- Surrounding information systems
7- Advance of
8- Attack skills
9- Manually

- طرفین پاسخگو مرتبط به طور مستقیم از ممیزان بازنگری کنترل امنیت اطلاعات، نسخه بدون تغییرات گزارش را دریافت کنند.
- طرفین غیر پاسخگو یا غیر مجاز رونوشتی از گزارش ممیزی‌های صورت گرفته برای بازنگری کنترل امنیت اطلاعات را دریافت نکنند، و
- به ممیزان بازنگری برای بررسی کنترل امنیت اجازه داده شود تا بتوانند بدون مانع کار خود را انجام دهند.

بازنگری‌های کنترل امنیت اطلاعات و وارسی انطباق فنی به طور خاص، ممکن است به یک سازمان در موارد زیر کمک کند:

- شناسایی و شناخت میزان مشکلات بالقوه یا کمبود در پیاده‌سازی و عملیاتی کردن کنترل‌های امنیت اطلاعات سازمان، استانداردهای امنیت اطلاعات و در پی آن کنترل امنیت اطلاعات فنی،
- شناسایی و شناخت اثرات بالقوه سازمانی تهدیدها و آسیب‌پذیری‌ها ناشی از کاهش امنیت اطلاعات نامناسب سازمان،
- اولویت بندی در فعالیت‌های کاهش مخاطره امنیت اطلاعات،
- تایید بر اینکه قبلا به نقاط ضعف یا کمبودهای امنیت اطلاعات شناسایی شده یا پدیدارشده[1] به اندازه کافی پرداخته شده است، و/یا
- پشتیبانی از تصمیم‌های بودجه‌ای در فرآیند سرمایه‌گذاری و دیگر تصمیم گیری‌های مدیریتی مربوط به بهبود مدیریت امنیت اطلاعات سازمان.

این گزارش فنی بر بازنگری‌های کنترل‌های امنیت اطلاعات، شامل وارسی انطباق فنی در برابر استاندارد پیاده‌سازی امنیت اطلاعات که به وسیله سازمان برقرار شده است، تمرکز دارد.

این گزارش به منظور ارائه‌ی هر راهنمای خاص برای وارسی انطباق در رابطه با سنجش، ارزشیابی مخاطره یا ممیزی ISMS همانطور که به ترتیب ISO/IEC 27004، 27005،27007 مشخص شده، نیست.

استفاده از این مستند به عنوان نقطه شروعی در فرآیند تعریف روش‌های اجرایی برای بازنگری کنترل‌های امنیت اطلاعات، موجب ارتقا سطح سازگاری بیشتری از امنیت اطلاعات درون سازمانی می‌شود.

این امر نیاز به انعطاف پذیری برای سفارشی‌سازی[1] در بازنگری‌های صورت گرفته شده براساس ماموریت‌ها و اهداف کسب‌وکار، الزامات و خط‌مشی‌های سازمانی، تهدیدات شناخته‌شده و آسیب‌پذیری

1- Emergent

اطلاعات، ملاحظات عملیاتی، سامانه‌های اطلاعاتی و وابستگی‌ها به سکو[2] و میزان مخاطره‌پذیری[3] پیشنهاد می‌شود.

یادآوری- استاندارد ISO Guide 73 سطح مخاطره‌پذیری را تعریف می‌کند، به عنوان مقدار و نوع مخاطره‌ای که سازمان آماده است تا آن را دنبال، حفظ یا انجام دهد.

۶ مرور کلی بر بازنگری‌های کنترل امنیت اطلاعات

۶-۱ فرآیند بازنگری

زمانی که یک بازنگری مربوط به امنیت اطلاعات منحصر به فرد آغاز می‌شود، ممیزان مرتبط با این بازنگری، ممیزان بازنگری کنترل امنیت، به طور معمول توسط جمع آوری اطلاعات اولیه شروع می‌کنند، این محدوده طرح‌ریزی شده کاری را بازنگری می‌کنند، با مدیران و دیگر مخاطبین در قسمت‌های کاربرد پذیر این سازمان ارتباط برقرار می‌کنند و این ارزیابی مخاطره بازنگری را به منظور توسعه مستندسازی بازنگری برای راهنمایی این بازنگری واقعی، تعمیم می‌دهد. نیاز است ممیزان تعیین شده‌ی بازنگری کنترل امنیت اطلاعات، به منظور بازنگری موثر، برای هر دو موضوع کنترل و آزمون آماده شوند. (به عنوان مثال عملیاتی کردن ابزارهای کاربردپذیر، هدف فنی آزمون). همچنین در این سطح، ممکن است مولفه‌های بازنگری با توجه به مخاطرات شناخته شده اولویت بندی شده و به منظور پیروی از یک فرآیند یا سامانه‌ی کسب‌وکار ویژه، طرح‌ریزی شده یا برای تحت پوشش قراردادن محدوده بازنگری، به ترتیب به طور ساده طراحی شوند.

اطلاعات مقدماتی می‌تواند از منابع مختلفی به دست آمده باشد:

- کتاب‌ها، جستجوهای اینترنتی، دفترچه‌های راهنمای فنی، استانداردها و مرور ادبیات[4] مربوط به مخاطرات معمول و کنترل‌ها در این زمینه باشد، کنفرانس‌ها، کارگاه‌ها، سمینارها یا انجمن‌ها،
- نتایج بازنگری‌های اولیه، آزمون‌ها و ارزشیابی‌ها، صرف نظر از اینکه قسمتی یا کل آن، در راستای محدوده بازنگری‌های حاضر که به وسیله ممیزان بازنگری کنترل امنیت اطلاعات هدایت شده یا نشده باشد (به عنوان مثال، آزمون‌های امنیتی پیش از انتشار که به وسیله متخصصان امنیت اطلاعات انجام شده است، می‌تواند دانش با ارزشی را درباره امنیت سامانه‌های کاربردی اصلی ارائه کند)،

1- Customize
2 - Platform dependencies
3- Risk appetite
4- General background research

- اطلاعات مربوط به حوادث امنیت اطلاعات، مخاطرات پیش‌بینی نشده‌ای که منجر به آسیب نمی‌شود، مسائل مربوط به پشتیبانی و تغییرات که از محل کمک[1] فناوری اطلاعات و مدیریت تغییرات فناوری اطلاعات، فرآیندهای مدیریت حوادث و منابع مشابه گردآوری شده است، و
- چک‌لیست‌های عمومی بازنگری و مقالات ممیزان بازنگری کنترل امنیت اطلاعات یا متخصصان امنیت اطلاعات که در این زمینه تخصص دارند.

مرور حوزه بازنگری طرح‌ریزی شده در پرتو اطلاعات اولیه می‌تواند مناسب و مفید باشد. ، به خصوص اگر طرح بازنگری که در اصل نشان‌دهنده‌ی محدوده موضوع بازنگری است، از چند ماه پیش آماده شده باشد. به عنوان مثال، ممکن است بازنگری‌های دیگر دارای نگرانی‌های شناسایی نشده باشد که ارزش بررسی عمیق‌تری را داشته، یا برعکس باعث افزایش اطمینان در برخی از حوزه‌ها شود که اجازه می‌دهد تمرکز بر روی این کار را به جای دیگری معطوف کنیم.

ارتباط با مدیران و تماس‌های بازنگری ارتباطات در این مرحله اولیه، یک فعالیت مهم است. در پایان فرآیند بازنگری، این افراد نیاز دارند که از یافته‌های بازنگری آگاه شده تا بتوانند پاسخ مثبتی به گزارش بازنگری بدهند. همدلی، احترام متقابل و تلاش برای توضیح فرآیند بازنگری به طور قابل توجهی موجب بهبود کیفیت و تاثیر بر نتیجه شود.

در حالی که افراد با روش‌های گوناگون به مستندسازی کار خود می‌پردازند، بسیاری از کارکردهای بازنگری از فرآیندهای بازنگری از پیش استاندارد شده که با الگوهای مستند برای اوراق کار پشتیبانی می‌کنند، نظیر چک‌لیست‌های بازنگری، پرسشنامه‌های کنترل داخلی، زمان‌بندی آزمون، ماتریس‌های کنترل مخاطره و غیره استفاده می‌کنند.

چک‌لیست بازنگری (یا مشابه آن)، به چند دلیل یک مستند کلیدی است:

- حوزه‌های طرح‌ریزی شده کار بازنگری را احتمالا تا سطح جزئیات آزمون‌های بازنگری و یافته‌های پیش بینی شده/ایده‌آل منحصر به فرد ترسیم می‌کند،
- ساختار کار را فراهم کرده و کمک می‌کند تا اطمینان حاصل شود که محدوده طرح‌ریزی شده به اندازه کافی تحت پوشش قرار داده شده است،
- تحلیل لازم برای تولید چک‌لیست در مرحله اول ممیزان بازنگری کنترل امنیت اطلاعات را برای کار میدانی آماده می‌کند و در حین تکمیل چک‌لیست به عنوان مراحل پیشرفت بازنگری، فرآیند تحلیلی آغاز می‌شود که گزارش بازنگری از آن به دست می‌آید،

1- Help desk

- چارچوبی را فراهم می‌کند که در آن نتایج حاصل از بازنگری کارهای از پیش انجام‌شده و کار میدانی ثبت شود و به عنوان مثال، جایی برای ارجاع و اظهار نظر و بر شواهد بازنگری جمع آوری شده است،
- می‌توان آن را به وسیله مدیریت ممیزی یا دیگر ممیزان بازنگری کنترل امنیت اطلاعات به عنوان قسمتی از فرآیند تضمین کیفیت بازنگری، مورد بازنگری قرار داد، و
- هنگامی که تمامی مراحل آن تکمیل شد (همراه با بازنگری شواهد) به عنوان واقعه‌نگاری سابقه با جزییات قابل اثبات از بازنگری کار انجام شده محسوب و یافته‌هایی ایجاد می‌شوند که ممکن است برای اثبات یا پشتیبانی گزارش بازنگری، اطلاع‌رسانی به مدیریت و/یا با کمک بازنگری آینده طرح‌ریزی‌ها، لازم باشد.

ممیزان امنیت اطلاعات جدا از صرف زمان کمتر، باید مراقب استفاده از چک‌لیست بازنگری عمومی که به وسیله دیگران نوشته شده است، باشند، زیرا احتمالا بسیاری از مزایایی که در بالا یادآوری شده است را پوشش نداده‌اند. (این امر آنجا که الزاماتی که باید در نظر گرفته شود کاملا صریح و روشن هستند به طرح موضوعات کمتر با انطباق مستقیم یا بازنگری‌های گواهی گرایش دارد.)

قسمت عمده‌ای از کار میدانی بازنگری از یک سری آزمون‌های راهبردی به وسیله ممیزان یا به درخواست آن‌ها، به منظور جمع‌آوری شواهد بازنگری و بازنگری آن، که اغلب به وسیله مقایسه با نتایج پیش بینی شده یا مورد انتظار است، تشکیل شده است که از تعهدات انطباقی مربوط، استانداردها یا برداشت کلی از روش‌های مناسب به دست آمده است. به عنوان مثال، یک آزمون بازنگری امنیت اطلاعات که کنترل‌های بدافزار را مورد بررسی قرار می‌دهد ممکن است این موضوع را وارسی کند که آیا تمام سکوهای محاسباتی کاربردی دارای نرم‌افزار آنتی ویروس مناسب هستند. از آنجایی که به ندرت منابع بازنگری کافی برای جامعیت آزمون وجود دارد، آزمون‌های بازنگری مانند آن چه مطرح شد، اغلب از روش‌های نمونه برداری استفاده می‌کنند. روش‌های نمونه برداری بین ممیزان و وضعیت‌ها متفاوت است و می‌تواند شامل انتخاب تصادفی، انتخاب طبقه‌ای و فنون دیگر نمونه‌گیری آماری پیچیده‌تر (به عنوان مثال در نظر گرفتن نمونه‌های بیشتر به منظور اثبات میزان ضعف کنترل در صورتی که نتایج اولیه رضایت بخش نباشند) باشد. به عنوان یک قاعده کلی، آزمون‌های جامع‌تر این امکان را می‌دهند که در آن شواهد به دست آمده را به صورت الکترونیکی جمع آوری کرده و مورد آزمون قرار دهیم، به عنوان مثال با استفاده از پرس و جوی[1] پایگاه داده SQL به هنگام استفاده از یک پایگاه داده شواهد بازنگری که از سامانه یا پایگاه داده مدیریت دارایی گردآوری شده است. رویکرد نمونه برداری ممیزان باید حداقل در قسمتی با مخاطرات مرتبط با زمینه عملیات در حال ممیزی هدایت شود.

1- Query

شواهد جمع آوری شده در دوره بازنگری به طور معمول در بازنگری اوراق کار[1] باید، یادداشت، ارجاع یا نگهداری شود. همزمان با تحلیل بازنگری صورت گرفته، یافته‌ها، توصیه‌ها و گزارش‌ها، لازم است شواهد بازنگری به اندازه کافی به وسیله ممیزان بازنگری امنیت اطلاعات کنترل شود، به خصوص این که برخی از آن‌ها بسیار حساس و/یا ارزشمند هستند. داده‌های استخراج شده از پایگاه داده‌های محصول، برای بازنگری باید ایمن شوند. برای مثال، به همان میزان که پایگاه‌های داده‌ها به وسیله استفاده از کنترل‌های دسترسی، رمزنگاری و غیره باید ایمن گردند. ابزارهای بازنگری خودکار، پرس‌وجوها، برنامه‌های استخراج داده/کاربرد و غیره باید شدیدا کنترل شوند. به طور مشابه، نسخه‌های چاپی ایجاد شده به وسیله ممیزان بازنگری کنترل امنیت اطلاعات باید عموما به طور فیزیکی به وسیله قفل یا کلید ایمن شده و از افشاء یا تغییر غیرمجاز آن جلوگیری شود. در موضوع بازنگری‌های ویژه‌ی حساس، مخاطرات و در پی آن کنترل‌های امنیت اطلاعات لازم، باید در مراحل اولیه بازنگری، شناسایی و آماده شود.

پس از تکمیل چک‌لیست بازنگری، با انجام یک سری از آزمون‌های بازنگری و جمع‌آوری شواهد بازنگری کافی برای آن، ممیزان بازنگری کنترل امنیت اطلاعات باید در موقعیتی باشند که بتوانند با بررسی شواهد بازنگری، مشخص نمایند که کدام یک از مخاطرات امنیتی برطرف شده و اثر بالقوه هرگونه مخاطرات باقیمانده را بازنگری کند. در این مرحله، به طور معمول پیش نویسی از گزارش بازنگری تهیه می‌شود، به طور کیفی در کارکرد بازنگری شده و با مدیریت به ویژه مدیریت واحدهای کسب وکار، ادارات، کارگروه‌ها یا تیم‌ها به طور مستقیم یا احتمالا با دیگر قسمت‌های دخیل سازمان مورد بحث قرار می‌گیرد.

مدیران ممیزی باید شواهد را با بی طرفی بازنگری نمایند تا وارسی کنند که:

- شواهد کافی بازنگری شده برای ارائه مبنای واقعی به منظور پشتیبانی همه یافته‌های بازنگری وجود دارد، و
- تمام یافته‌ها و توصیه‌ها به محدوده بازنگری مرتبط هستند و مسائل غیر ضروری مستثنی شده است.

اگر کار بازنگری بیشتری برای یافته‌ها طرح‌ریزی شده باشد باید در گزارش مشخص شوند.

همان طور که طرح‌ریزی بازنگری صورت می‌گیرد، فرآیند تحلیل به طور اساسی مبتنی بر مخاطره است و بهتر است شواهد جمع آوری شده در طول کار میدانی بازنگری از نظر اطلاعاتی غنی شود. از آنجا که ایجاد بازنگری انطباق معمولا می‌تواند یک سری از نتایج نسبتا ساده شکست/پیروزی که با توصیه‌های بدیهی بزرگ نتیجه می‌شود، تولید کند. بازنگری امنیت اطلاعات اغلب موضوعاتی را ایجاد می‌کند که

1- Working papers

پیش از تصمیم‌گیری نسبت به اینکه چه اقداماتی (در صورت وجود) مناسب است، نیاز به تفکر مدیریتی و نیاز به بحث دارد. در بعضی از این موارد ممکن است مدیریت تصمیم به پذیرش برخی مخاطرات شناسایی شده به وسیله ممیزان امنیت اطلاعات گرفته باشد و در موارد دیگری ممکن است تصمیم بگیرند توصیه‌ها را آن طور که دقیقا وضع‌شده است، انجام ندهند: این حق مدیریت است، اما آن‌ها باید پاسخگوی تصمیمات خود نیز باشند. در این حالت ممیزان بازنگری کنترل امنیت اطلاعات صرفا توصیه ارائه می‌دهند و نقش غیر عملیاتی دارند گرچه آن‌ها دارای نفوذ قابل توجهی نیز هستند و به وسیله روش‌های بازنگری و شواهد مستند حمایت می‌شوند.

ممیزان بازنگری کنترل امنیت اطلاعات باید برای سازمان، فعالیت‌های امنیت اطلاعات (تمام فعالیت‌ها در سامانه مدیریت پیاده‌سازی نمی‌شود) را با تضمین مناسبی از دستیابی به مجموعه‌ای از اهداف مشخص شده فراهم کنند. بازنگری باید بیانیه‌ای از تفاوت بین واقعیت و مرجع را ارائه کند. وقتی خط‌مشی داخلی یک سازمان به عنوان مرجع در نظر گرفته می‌شود، این خط‌مشی باید به اندازه کافی روشن باشد تا بتواند به عنوان یک مرجع در نظر گرفته شود. معیارهای ذکر شده در پیوست ب ممکن است برای اطمینان از این موضوع در نظر گرفته شود. ممیزان بازنگری کنترل امنیت اطلاعات باید خط‌مشی‌های داخلی و روش‌های اجرایی مرتبط با محدوده‌ی بازنگری را در نظر بگیرند. معیارهای مرتبطی که دیگر مورد استفاده قرار نمی‌گیرند نیز ممکن است به صورت غیررسمی در درون سازمان‌ها استفاده شوند. عدم وجود معیارهای شناسایی شده به عنوان یک بحران ممکن است علت بالقوه ناهماهنگی‌های تطابق[1] باشند.

۶-۲ تامین منابع

بازنگری کنترل‌های امنیت اطلاعات نیاز به تحلیل هدف و مهارت‌های گزارش‌نویسی حرفه‌ای دارد. مهارت‌های تخصصی دیگری، در صورت ارتباط با وارسی انطباق فنی مورد نیاز هستند از جمله داشتن دانش فنی دقیق که چگونه خط‌مشی‌های امنیتی که در نرم‌افزار، سخت افزار، راه‌های ارتباطی و در فرآیندهای فنی مرتبط پیاده‌سازی شده‌اند. ممیزان بازنگری کنترل امنیت اطلاعات باید دارای مهارت‌های زیر باشند:

- آگاهی کلی از مخاطرات سامانه‌های اطلاعاتی و معماری‌های امنیت، مبتنی بر درک چارچوب‌های مفهومی زیر بنای سامانه‌های اطلاعاتی،
- دانش روش‌های امنیت اطلاعات مناسب از جمله کنترل‌های امنیت اطلاعات گسترش داده شده به وسیله استاندارد ISO/IEC ۲۷۰۰۲ یا سایر استانداردهای امنیتی،

1- Non-conformities

- توانایی بررسی اطلاعات پیچیده فنی با عمق کافی برای شناسایی هر گونه مخاطره قابل توجه و فرصت برای بهبود، و
- عملگرایی با آگاهی کاملی از محدودیت‌های عملی در هر دو جنبه امنیت اطلاعات و بازنگری‌های فناوری اطلاعات.

اکیدا توصیه می‌شود، هر کسی که وظیفه هدایت بازنگری کنترل‌های امنیت اطلاعات را به عهده داشته و از تجربه کافی در امر ممیزی برخوردار نیست، به طور رسمی با اصول حرفه‌ای ممیزی آشنا شود، که عبارتند از: اخلاق، استقلال، بی طرفی، محرمانگی، مسئولیت پذیری، اختیار، مجوز برای دسترسی به سوابق، کارکردها، مالکیت، کارکنان، اطلاعات، وظیفه مراقبت در اداره و حفاظت از آنچه به دست آمده است، یافته‌ها و توصیه‌ها، و فرآیند پیگیری.

برای رسیدن به هدف بازنگری، ممکن است یک تیم متشکل از ممیزان بازنگری کنترل امنیت اطلاعات با صلاحیت‌های تخصصی مرتبط متفاوت ایجاد شود. جایی که در آن مهارت‌ها یا صلاحیت در هنگام نیاز در دسترس نیست، مخاطرات و مزایا در تعامل با متخصصان موضوع باید چه به شکل درون سازمانی یا خارج از آن که برای انجام بازنگری در محدوده بررسی مورد نیاز است، در نظر گرفته شوند.

ممیزان بازنگری کنترل امنیت اطلاعات همچنین باید تایید کنند سازمان و کارکنان مسئول برای امنیت اطلاعات حضور دارند و به اندازه کافی در امنیت اطلاعات و ماموریت‌های خاص خود آگاهی داشته باشند و منابع لازم را در اختیار خود داشته باشند.

به عنوان قسمتی از برنامه مبارزه با تقلب‌های سازمان، ممیزان بازنگری کنترل امنیت اطلاعات ممکن است نیاز به همکاری نزدیک با ممیزان مالی در هر یک از مراحل طرح‌ریزی، اجرای ممیزی و گام‌های بازنگری ممیزی داشته باشند.

۷ روش‌های بازنگری

۷-۱ مرور کلی

مفهوم اساسی بازنگری کنترل‌ها به طور معمول عبارتند از: روش‌های اجرایی بازنگری، گزارش‌دهی بازنگری و پیگیری بازنگری. قالب و محتوای فرآیندهای بازنگری شامل اهداف بازنگری و روش‌های بازنگری است.

ممیزان بازنگری کنترل امنیت اطلاعات می‌توانند سه روش بازنگری را در بازنگری‌های کنترل امنیت اطلاعات استفاده کنند:

- بررسی[1]،
- مصاحبه، و
- آزمون[2].

قسمت‌های مربوطه عبارتند از: مجموعه‌ای از خصوصیات[3] و ارزش خصوصیت برای هر یک از روش‌های بازنگری. در مورد خصوصیت عمیق موارد زیر تعریف می‌شود، ارزش خصوصیت مورد نظر شامل دقت بازنگری و سطح جزئیات برای ارزش خصوصیت تعریف شده. ارزش خصوصیت تفصیلی شامل و ایجاد شده از بازنگری با دقت و سطح تعریف شده برای ارزش خصوصیت تخصصی (متمرکز) است. در مورد خصوصیت تحت پوشش موارد زیر تعریف می‌شود، ارزش یک خصوصیت خاص شامل و ایجاد شده از تعداد و نوع موضوعات بازنگری تعریف شده برای ارزش خصوصیت نمایش داده شده. ارزش خصوصیت جامع شامل و ایجاد شده از تعداد و نوع موضوعات بازنگری تعریف‌شده برای ارزش خصوصیت خاص است.

روش‌های «بررسی» و «آزمون» را می‌توان با استفاده از ابزارهای خودکار که به صورت گسترده‌ای مورد استفاده قرار گرفته است مورد پشتیبانی قرار داد. ممیزان بازنگری کنترل امنیت اطلاعات باید همچنین اثر عملکرد این نوع ابزار را بر عملکرد معمولی موضوع بازنگری، بازنگری کنند. هنگامی‌که قسمتی از این بازنگری متکی به چنین ابزاری باشد، ممیزان بازنگری کنترل امنیت اطلاعات باید آن را اعلام یا شواهدی مبنی بر این که ابزارها نتایج قابل اعتمادی دارند را ارائه کنند.

۷-۲ روش بازنگری: بررسی

۷-۲-۱ کلیات

فرآیند وارسی، بازرسی[4]، بازنگری، مشاهده، مطالعه یا تحلیل یک یا تعداد بیشتر از موضوعات بازنگری به منظور تسهیل در فهم، رسیدن به شفافیت یا به دست آوردن شواهدی که از نتایج آن برای پشتیبانی از مشخص کردن وجود، کارکرد، درستی، کامل بودن و پتانسیل بهبود یک کنترل در طول زمان استفاده شده است.

موضوعات بازنگری به طور معمول عبارتند از:

1- Examine
2- Test
3- Attributes
4- Inspecting

- ویژگی‌ها (به عنوان مثال، خط‌مشی‌ها، طرح‌ها، روش‌های اجرایی، الزامات سامانه، طراحی‌ها)،
- سازوکارها (به عنوان مثال، کارکردهای پیاده‌سازی شده توسط سخت افزار، نرم‌افزار، ثابت‌افزار[1]) و
- فرآیندها (به عنوان مثال، عملیات‌های سامانه، سرپرستی[2]، مدیریت، اجرایی[3])

اقدامات ممیز بازنگری کنترل امنیت اطلاعات ممکن است به عنوان نمونه شامل موارد زیر باشد:

- بازنگری خط‌مشی‌های امنیت اطلاعات، طرح‌ها، و روش‌های اجرایی،
- تحلیل مستندات طراحی سامانه و ویژگی‌های واسط،
- مشاهده عملیات‌های پشتیبان‌گیری از سامانه و بازنگری نتایج تمرینات طرح پیشامد رخ دهد،
- مشاهده فرآیند پاسخ به حادثه،
- مطالعه کتابچه‌های راهنمای فنی و راهنمایی‌های کاربر/مدیر،
- وارسی، مطالعه یا مشاهده عملیات سازوکار فناوری اطلاعات در سخت افزار/نرم‌افزار سامانه اطلاعاتی،
- وارسی، مطالعه و مشاهده مدیریت تغییرات و واقعه‌نگاری اقدامات مربوط به یک سامانه اطلاعاتی، و
- وارسی، مطالعه یا سنجش‌های امنیت فیزیکی مرتبط با عملیات یک سامانه اطلاعاتی.

۷-۲-۲ خصوصیات

۷-۲-۲-۱ بررسی عمومی

بررسی‌هایی که به طور معمول شامل بازنگری‌های سطح بالا، وارسی‌ها، مشاهدات یا بازرسی‌های موضوع بازنگری باشد. این نوع بررسی با استفاده از شواهد و مستندات محدود (به عنوان مثال، توصیف سطح کارکردی برای سازوکارها؛ توصیف فرآیند سطح بالا برای فرآیندها؛ و مستندات واقعی برای ویژگی‌ها) هدایت می‌شود. بررسی‌های عمومی سطحی از درک را نسبت به کنترل لازم برای تعیین اینکه آیا کنترل، پیاده‌سازی شده و خالی از اشکال است، را ارائه می‌کند.

۷-۲-۲-۲ بررسی تخصصی

بررسی‌هایی که به طور معمول شامل بازنگری‌های سطح بالا، وارسی‌ها، مشاهدات یا بازرسی و مطالعات/تحلیل‌های عمیق‌تر از موضوع بازنگری است. این نوع بررسی با استفاده از شواهد و مستندات قابل توجهی (به عنوان مثال، توصیف‌های سطح کارکردی و جایی که مناسب و در دسترس باشد، اطلاعات طراحی سطح بالا سازوکارها؛ توصیف‌های فرآیند سطح بالا و روش‌های اجرایی پیاده‌سازی فرآیندها؛ و مستندات حقیقی و مستندات مربوط به ویژگی‌ها) هدایت می‌شود. بررسی‌های تخصصی،

1- Firmware
2- Review
3- Exercise

سطحی از ادراک نسبت به کنترل امنیتی لازم برای تعیین اینکه آیا کنترل، پیاده‌سازی شده و خالی از اشکال است را فراهم می‌کند. همچنین زمینه‌های افزایش اعتماد را نسبت به اینکه کنترل درست پیاده‌سازی شده و همانطور که در نظر گرفته شده در حال کار است، ارائه می‌دهند.

۷-۲-۲-۳ بررسی تفصیلی

بررسی‌هایی که به طور معمول شامل بازنگری‌های سطح بالا، وارسی‌ها، مشاهدات یا بازرسی‌های عمیق‌تر، مفصل‌تر و به وسیله مطالعه/تجزیه و تحلیل موضوع بازنگری است. این نوع بررسی با استفاده از مستندات یا شواهد گسترده‌ای (به عنوان مثال، توصیف‌های سطح کارکردی جایی که مناسب و در دسترس باشد، اطلاعات طراحی در سطح بالا و سطح پایین و پیاده‌سازی اطلاعات برای سازوکارها؛ توصیف فرآیند سطح بالا و روش‌های اجرایی پیاده‌سازی تفصیلی فرآیندها؛ و مستندات حقیقی و مستندات مرتبط برای ویژگی‌ها) هدایت می‌شود. بررسی‌های تفصیلی سطحی از درک کنترل لازم را برای تعیین اینکه آیا کنترل، پیاده‌سازی شده و خالی از اشکال است، فراهم می‌کند. همچنین زمینه‌های افزایش اعتماد را نسبت به اینکه کنترل درست پیاده سازی شده و همانطور که در نظر گرفته شده در حال کار است و بهبود پایداری در اثر بخشی کنترل پشتیبانی می‌شود، را ارائه می‌کند.

۷-۲-۲-۴ بررسی نماینده[1]

بررسی‌ای که با استفاده از یک نمونه که نماینده‌ای از موضوعات بازنگری انجام می‌گیرند (بر اساس نوع و تعداد در نوع) تا سطح پوشش لازم برای تعیین اینکه آیا کنترل، پیاده‌سازی شده و خالی از اشکال است را ارائه دهد.

۷-۲-۲-۵ بررسی خاص

بررسی‌ای که از یک نمونه نماینده موضوعات بازنگری (بر اساس نوع و تعداد در نوع) و سایر موضوعات بازنگری ویژه برای دستیابی به اهداف بازنگری، مهم تلقی می‌شوند استفاده می‌کند. همچنین سطح پوشش لازم برای تعیین اینکه آیا کنترل پیاده‌سازی شده و خالی از اشکال است، را فراهم می‌کند. همچنین زمینه‌های افزایش اعتماد را نسبت به اینکه کنترل درست پیاده سازی شده و همانطور که در نظر گرفته شده‌اند در حال کار است، ارائه می‌کند.

1- Representative

۷-۲-۲-۶ بررسی جامع[1]

بررسی‌ای که از تعداد زیادی نمونه از موضوعات بازنگری (بر اساس نوع و تعداد در نوع) و سایر موضوعات بازنگری ویژه که برای دستیابی به هدف بازنگری، مهم تلقی می‌شوند استفاده می‌کند. همچنین سطح پوشش لازم برای تعیین اینکه آیا کنترل پیاده‌سازی شده و خالی از اشکال است، را فراهم می‌کند. همچنین زمینه های افزایش اعتماد را نسبت به اینکه کنترل درست پیاده سازی شده و همانطور که در نظر گرفته شده مداوم و مبتنی بر سازگاری در حال کار است و بهبود پایدار در اثر بخشی کنترل وجود دارد ارائه می‌کند.

۷-۳ روش بازنگری: مصاحبه

۷-۳-۱ کلیات

فرآیند هدایت گفتگوها با افراد یا گروه‌های درون سازمان به منظور آسان‌سازی درک، دستیابی به شفافیت یا رسیدن به محل شواهد است. نتایج به دست آمده برای پشتیبانی از تعیین میزان وجود کنترل امنیت، کارکرد، درستی، کامل بودن و پتانسیل بهبود در طول زمان استفاده شده است.

موضوعات بازنگری به طور معمول شامل افراد یا گروه‌ها می‌باشد.

اقدامات معمول ممیز بازنگری کنترل امنیت اطلاعات ممکن است شامل مصاحبه با افراد زیر باشد:

- مدیریت،
- صاحبان دارایی اطلاعاتی و مأموریت،
- کارشناسان امنیت اطلاعات،
- مدیران امنیت اطلاعات،
- کارشناسان کارکنان،
- مدیران منابع انسانی،
- مدیران تسهیلات،
- کارشناسان آموزش،
- کاربران سامانه اطلاعاتی،
- سرپرست‌های شبکه و سامانه،
- مدیران سایت،
- کارشناسان حفاظت فیزیکی، و

1- Comprehensive

- کاربران

۷-۳-۲ خصوصیات

۷-۳-۲-۱ مصاحبه کلی

مصاحبه‌ها، شامل گفتگوهای گسترده سطح بالا با افراد یا گروه‌ها است. این نوع از مصاحبه با استفاده از مجموعه‌ای از پرسش‌های کلی و سطح بالا هدایت می‌شود. مصاحبه‌های عمومی، سطحی از درک کنترل امنیتی لازم را برای تعیین اینکه آیا کنترل، درست پیاده‌سازی شده و خالی از اشکال است، ارائه می‌کند.

۷-۳-۲-۲ مصاحبه تخصصی

علاوه بر الزامات مصاحبه‌های عمومی، مصاحبه تخصصی شامل گفتگوهای عمیق در زمینه‌های خاص با افراد یا گروه‌هایی از افراد است. این نوع از مصاحبه، علاوه بر این از پرسش‌های عمیق در زمینه‌های خاص استفاده می‌کنند که در آن‌ها پاسخ‌ها نشان دهنده نیاز بیشتر به بررسی عمیق است. مصاحبه‌های تخصصی سطحی از درک را نسبت به کنترل امنیتی لازم برای تعیین اینکه آیا کنترل پیاده‌سازی شده و خالی از اشکال است، فراهم می‌کند و زمینه‌های افزایش اعتماد نسبت به اینکه کنترل درست پیاده‌سازی شده و همانطور که در نظر گرفته شده در حال کار است را ارائه می‌کند.

۷-۳-۲-۳ مصاحبه تفصیلی

علاوه بر الزامات مصاحبه‌های تخصصی، مصاحبه تفصیلی شامل پرسش‌های عمیق‌تر همراه با کاوش‌های مرتبط در زمینه‌های خاص است که در آن‌ها پاسخ‌ها نشان دهنده نیاز به بررسی عمیق‌تر یا جایی که با روش‌های اجرایی بازنگری فراخوانی شده، می‌باشند. مصاحبه‌های تفصیلی سطحی از درک نسبت به کنترل‌های امنیتی لازم را برای تعیین اینکه آیا کنترل پیاده‌سازی شده و خالی از اشکال است را فراهم می‌کند و زمینه‌های افزایش اعتماد نسبت به اینکه کنترل درست پیاده‌سازی شده و همانطور که در نظر گرفته شده به صورت مستمر در حال کار است و اینکه پشتیبانی برای بهبود مستمر در اثربخشی کنترل‌ها وجود دارد را ارائه می‌کند.

۷-۳-۳ خصوصیت پوشش

خصوصیت پوشش به محدوده یا گستره فرآیند مصاحبه پرداخته و شامل انواع مختلف افراد مصاحبه شونده (بر اساس نقش سازمانی و مسئولیت‌های مربوطه)، تعداد افراد مصاحبه شونده (بر اساس نوع) و افراد خاص مصاحبه شونده می‌باشد.

۷-۳-۳-۱ مصاحبه نماینده

مصاحبه‌ای که با استفاده از یک نمونه که نماینده‌ای از افراد در نقش‌های کلیدی سازمانی برای ارائه سطح پوشش لازم برای تعیین اینکه آیا کنترل پیاده‌سازی شده و بدون خطاهای آشکار است را ارائه می‌کند.

۷-۳-۳-۲ مصاحبه خاص

مصاحبه‌ای که با استفاده از یک نمونه‌ی نماینده‌ی افراد از نقش‌های کلیدی سازمان یا افراد خاص دیگر برای دستیابی به هدف بازنگری به منظور ارائه سطح پوشش لازم برای تعیین این که آیا کنترل امنیت پیاده‌سازی شده است و خالی از اشکال است، انجام می‌گیرند و زمینه‌های افزایش اعتماد را نسبت به اینکه کنترل به درستی پیاده‌سازی شده است و همچنین همانطور که انتظار می‌رود در حال کار است، ارائه می‌کند.

۷-۳-۳-۳ مصاحبه جامع

مصاحبه‌ای که از تعداد زیادی نمونه از افراد در نقش‌های کلیدی سازمانی و سایر افراد مهم برای دستیابی به هدف بازنگری به منظور ارائه سطح پوشش لازم برای تعیین اینکه آیا کنترل امنیت درست پیاده‌سازی شده و خالی از اشکال است، انجام می‌گیرند و زمینه‌های افزایش اعتماد که کنترل به درستی پیاده‌سازی شده است و همچنین همانطور که در نظر گرفته شده به صورت مداوم و مبتنی بر سازگاری کار می‌کند و پشتیبانی برای بهبود مستمر در اثربخشی کنترل وجود دارد، را ارائه می‌کند.

۷-۴ روش بازنگری: آزمون

۷-۴-۱ کلیات

فرآیند اعمال یک یا چند موضوع بازنگری در شرایطی مشخص برای مقایسه رفتار واقعی و پیش بینی شده است. نتایج، برای پشتیبانی از تعیین وجود کنترل، اثربخشی، کارکرد، درستی، کامل بودن و پتانسیل بهبود در طول زمان استفاده می‌شوند. آزمون باید با دقت بسیار زیادی به وسیله متخصصان توانمند انجام شده و اثرات احتمالی بر روی عملیات سازمانی به وسیله مدیریت مربوطه پیش از شروع آزمون در نظر گرفته شده و مورد تأیید قرار گیرد، همچنین گزینه‌های در حال اجرا برای آزمون در خارج از چارچوب‌های عملیاتی، برای کسانی که مسئولیت‌هایی در سطوح پایین دارند یا حتی در محیط آزمون، باید در نظر گرفته شود. شکست‌ها یا از دسترس خارج شدن سامانه اگر به علت آزمون باشد، می‌تواند تاثیر قابل توجهی در عملیات عادی کسب‌وکار سازمان داشته باشد. هر دو این‌ها ممکن است منجر به پیامدهای مالی شده و شهرت و اعتبار سازمان را تحت تأثیر قرار دهد به طوری که ملاحظات ویژه‌ای باید در طرح‌ریزی آزمون و قراردادی کردن آن (از جمله ملاحظات جنبه‌های حقوقی) در نظر گرفته شود.

نتایج مثبت-کاذب[1] و منفی-کاذب[1] آزمون‌ها قبل از هر گونه استنتاج، باید به دقت به وسیله ممیز بازنگری کنترل امنیت اطلاعات مورد بازنگری قرار گیرد.

1- False positive

موضوعات بازنگری معمول شامل سازوکارها (برای مثال سخت افزار، نرم‌افزار، ثابت افزار) و فرآیندها (برای مثال عملیات‌های سامانه، سرپرستی، مدیریت، تمرین‌ها) می‌باشد.

اقدامات معمول ممیز بازنگری کنترل امنیت اطلاعات ممکن است شامل موارد زیر باشد:

- آزمون کنترل دسترسی، شناسایی، احراز هویت و سازوکارهای بازنگری،
- آزمون تنظیمات پیکربندی امنیت،
- آزمون افزاره‌های کنترل دسترسی فیزیکی،
- هدایت آزمون تست نفوذ برای مولفه‌های کلیدی سامانه اطلاعات،
- آزمون عملیات‌های پشتیبان‌گیری سامانه اطلاعاتی،
- آزمون قابلیت پاسخگویی حادثه،
- تمرین قابلیت طرح‌ریزی پیشامد،
- آزمون پاسخ سامانه‌های امنیتی قادر به شناسایی، هشدار و پاسخ به نفوذ[2]،
- آزمون رمزنگاری و الگوریتم‌های سازوکار در هم آمیختگی[3] داده‌ها،
- آزمون شناسه کاربر و سازوکارهای مدیریت اختیارات ویژه[4]،
- آزمون سازوکار مجوز، و
- تایید انعطاف پذیری آبشاری[5] سنجش‌های امنیتی.

یادآوری- خصوصیات برای آزمون به کار برده نمی‌شوند.

۷-۴-۲ انواع آزمون

۷-۴-۲-۱ آزمون بدون دید[6]

ممیز بازنگری کنترل امنیت اطلاعات بدون داشتن هیچ گونه اطلاعات پیشین از ویژگی‌ها، به غیر از اطلاعاتی که در دسترس عموم می‌باشد، با موضوع بازنگری روبرو می‌شود. موضوع بازنگری با دانستن همه جزییات آماده بازنگری می‌شود. بازنگری بدون دید، در درجه اول مهارت‌های یک ممیز برای آزمون بازنگری کنترل امنیت اطلاعات است. وسعت و عمق بازنگری بدون دید تنها می‌تواند به گستردگی دانش کاربردی و کارآمدی ممیز بازنگری کنترل امنیت اطلاعات باشد. بنابراین استفاده از این آزمون در

1- False negative
2- Intrusion
3- Hash
4- Privilege
5- Cascade
6- Blind

بازنگری‌های امنیت محدود بوده و باید از آن اجتناب شود. به این گونه آزمون معمولا هک اخلاقی[1] گفته می‌شود.

۷-۴-۲-۲ آزمون بدون دید دوگانه

ممیز بازنگری کنترل امنیت اطلاعات بدون داشتن هیچ گونه اطلاعات پیشین از ویژگی‌ها، به غیر از اطلاعاتی که در دسترس عموم می‌باشد، با موضوع بازنگری روبرو می‌شود. موضوع بازنگری از محدوده بازنگری یا بردارهای آزمون مورد استفاده، آگاه نمی‌شود. آزمون‌های بازنگری بدون دید دوگانه، آمادگی موضوع بازنگری را نسبت به محرک‌های ناشناخته تحریک می‌سنجد.

۷-۴-۲-۳ آزمون جعبه خاکستری

ممیز بازنگری کنترل امنیت اطلاعات، با دانشی محدود درباره‌ی دفاع و دارایی‌ها اما با دانشی کامل نسبت به مولفه‌های آزمون در دسترس، با موضوع بازنگری روبرو می‌شود. موضوع بازنگری با دانستن جزییات برای بازنگری آماده می‌شود. بازنگری جعبه خاکستری مهارت‌های ممیز بازنگری کنترل امنیت اطلاعات را می‌آزماید. ماهیت این آزمون بر اساس کارایی است. گستردگی و عمق آن بستگی به کیفیت اطلاعات فراهم شده برای ممیز بازنگری کنترل امنیت اطلاعات پیش از بازنگری و همچنین دانش کاربردی ممیز بازنگری کنترل امنیت اطلاعات دارد. بنابراین این آزمون در بازنگری‌های امنیتی دارای محدودیت بوده و باید از آن اجتناب شود. به این نوع آزمون اغلب آزمون داوطلبانه گفته می‌شود و بیشتر به وسیله هدف به عنوان یک فعالیت خود-ارزشیابی پایه‌گذاری می‌شود.

۷-۴-۲-۴ آزمون جعبه خاکستری دوگانه

ممیز بازنگری کنترل امنیت اطلاعات، با دانشی محدود درباره‌ی دفاع و دارایی‌ها اما با دانشی کامل نسبت به مولفه‌های آزمون در دسترس، با موضوع بازنگری روبه‌رو می‌شود. موضوع بازنگری از پیش نسبت به محدوده و چارچوب زمانی موضوع بازنگری آگاه شده ولی اطلاعی نسبت به مولفه‌های آزمون ندارد. در آزمون‌های بازنگری جعبه خاکستری دوگانه، آمادگی هدف نسبت به متغیرهای ناشناخته تحریک مورد سنجش قرار می‌گیرد. گستردگی و عمق آن بستگی به کیفیت اطلاعات فراهم شده برای ممیز بازنگری کنترل امنیت اطلاعات و موضوع بازنگری پیش از آزمون به خوبی دانش کاربردی ممیز بازنگری کنترل امنیت اطلاعات دارد.

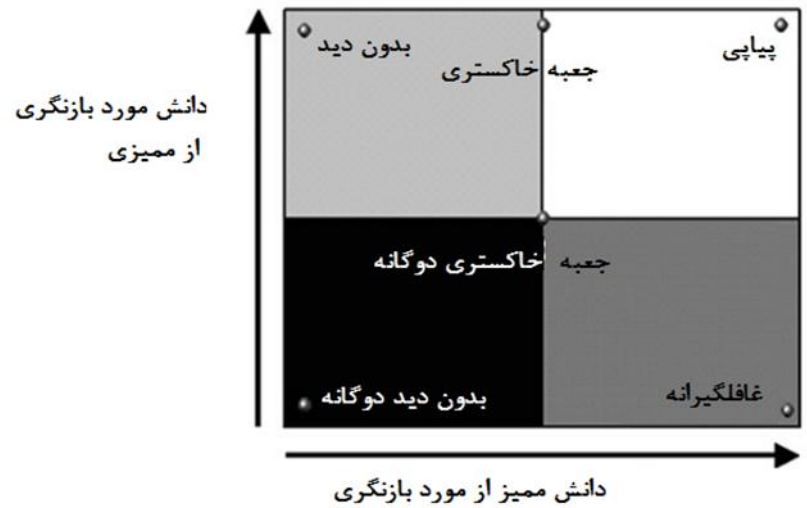
1- Ethical Hacking

۷-۴-۲-۵ آزمون پیاپی[1]

ممیز بازنگری کنترل امنیت اطلاعات و همچنین موضوع بازنگری هر دو با اطلاع پیشین نسبت به همه جزئیات بررسی برای بازنگری آماده می‌شوند. بازنگری‌های پیاپی حفاظت و کنترل‌های هدف را می‌آزماید. با این وجود، نمی‌تواند آمادگی هدف را در مقابل متغیرهای تحریک ناشناخته بیازماید. ماهیت واقعی این آزمون همه جانبه است چون ممیزان بازنگری کنترل امنیت اطلاعات دید کاملی از همه آزمون‌ها و پاسخ‌های آن ندارد. گستردگی و عمق آن به کیفیت اطلاعات فراهم شده برای ممیزان بازنگری کنترل امنیت اطلاعات پیش از آزمون و نیز دانش قابل کاربرد ممیزان بازنگری کنترل امنیت اطلاعات بستگی دارد. این آزمون اغلب به عنوان یک بازنگری داخل سازمان شناخته شده و ممیز بازنگری کنترل امنیت اطلاعات غالبا نقشی فعال در کل فرآیند امنیت دارد.

۷-۴-۲-۶ آزمون غافلگیرانه[2]

ممیزان بازنگری کنترل امنیت اطلاعات با دانشی کامل از فرآیندهای و عملیات امنیتی با موضوع بازنگری روبرو شده ولی موضوع بازنگری از اینکه چه، چگونه یا چه زمانی ممیز بازنگری کنترل امنیت اطلاعات، آزمون را انجام می‌دهد آگاهی ندارد. ماهیت واقعی این آزمون بازنگری آمادگی هدف به متغیرهای ناشناخته و بردارهای تحریک است. گستردگی و عمق آن به کیفیت اطلاعات فراهم شده برای ممیزان بازنگری کنترل امنیت اطلاعات پیش از آزمون و نیز دانش کاربردی آن‌ها بستگی دارد. به این نوع آزمون معمولا تمرین گروه قرمز گفته می‌شود.



شکل ۱- انواع آزمون

1- Tandem

۲- با توجه به مفهوم این آزمون، واژه غافلگیرانه برای آزمون Reversal انتخاب گردید.

۷-۴-۳ روش‌های اجرایی بازنگری توسعه یافته

علاوه بر روش‌های اجرایی بازنگری که در مورد کنترل فـردی اعمـال مـی‌شـوند، روش اجرایـی بـازنگری توسعه یافته را نیز می‌توان به عنوان یک امر کلی در بازنگری به کار برد. فرآیندهای بازنگری توسعه یافته برای انجام امور و تکمیل مراحل بازنگری آن به منظور کمک در زمینـه بـالا بـردن اعتمـاد در اثربخشـی کنترل‌ها طراحی شده است.

روش‌های اجرایی بازنگری توسعه یافته و اهداف مربوط به آن نیز با سطح مخاطره سامانه‌های اطلاعاتی در ارتباط هستند.

۸ فعالیت‌ها[1]

۸-۱ آماده‌سازی

برقراری و حفظ مجموعه‌ای مناسب از انتظارات در پیش از بازنگری، هنگام بـازنگری و پـس از بـازنگری، برای دستیابی به خروجی قابل قبول اهمیت زیادی دارد. این بدان معنا است که فراهم کـردن اطلاعـات، مدیریت را قادر می‌سازد که درباره چگونگی پیاده‌سازی و استفاده از سامانه‌های اطلاعاتی، تصمیماتی بـی نقص و بر پایه مخاطره اتخاذ کند. از آماده‌سازی کامل به وسیله سازمان و ممیزان بازنگری کنترل امنیـت اطلاعات، جنبه‌ای مهم از انجام یک بازنگری مؤثر، است. فعالیت‌های آماده سازی باید به طیف وسـیعی از مسائل مربوط به هزینه، زمان‌بندی، در دسترس بودن تخصص و عملکرد بازنگری‌ها بپردازد.

از دیدگاه سازمانی، آماده‌سازی برای بازنگری شامل فعالیت‌های کلیدی زیر است:

- اطمینان از اینکه خط‌مشی‌های مناسب برای پوشش‌دهی بازنگری‌ها مناسب بوده و به وسیله همه عناصر سازمانی قابل فهم هستند،
- اطمینان از این که همه مراحل طرح‌ریزی شده اجرای کنترل‌ها پیش از بازنگری با موفقیت تکمیل شده است و توسط مدیریت به صورت مناسبی بازنگری شده‌اند (این مورد فقط زمانی اعمال می‌شود که کنترل به طور کامل عملیاتی شده باشد نه در مرحله مقدماتی/ اجرایی)،
- اطمینان از اینکه کنترل‌های انتخاب شده به نهادهای مناسب سازمانی برای توسعه و پیاده‌سازی اجرا اختصاص داده شده‌اند.
- برقراری هدف و محدوده بازنگری (یعنی هدف بازنگری و آنچه که در دست بازنگری است، مشخص شده باشد.)

1- Activities

- متوجه نمودن مسئولین مهم سازمانی نسبت به در شرف بودن ممیزی‌ها و اختصاص منابع لازم برای انجام بازنگری،
- برقراری کانال‌های ارتباطی مناسب میان مقامات سازمانی که هنگام بازنگری‌ها دارای منافع هستند،
- برقراری محدوده‌های زمانی برای تکمیل بازنگری‌ها و نقاط کلیدی[1] تصمیم گیری مورد نیاز سازمان به منظور مدیریت مؤثر بازنگری‌ها،
- شناسایی و انتخاب ممیز بازنگری کنترل امنیت اطلاعات توانمند یا گروه ممیزی که هدایت بازنگری‌ها را با توجه به نبود وابستگی مسائل مربوط به ممیز بازنگری کنترل امنیت اطلاعات برعهده بگیرد.
- جمع‌آوری فراورده[2] برای ارائه به ممیزان جهت کنترل بازنگری امنیت اطلاعات (به عنوان مثال، مستندات کنترل‌ها امنیت اطلاعات از جمله نمودار سازمانی، خط‌مشی‌ها، روش‌های اجرایی، طرح‌ها، ویژگی‌ها، طراحی‌ها، سوابق، کتابچه راهنمای مدیر/کاربر، مستندات سامانه اطلاعاتی، توافق نامه‌های داخلی، نتایج بازنگری‌های پیشین) و
- برقراری یک سازوکار بین سازمان و ممیزان بازنگری کنترل امنیت اطلاعات برای به حداقل رساندن ابهامات یا سوء تفاهم‌ها در مورد پیاده‌سازی کنترل یا بازنگری کمبودها/ نقاط ضعف مشخص شده در طول بازنگری‌ها.
- علاوه بر طرح‌ریزی فعالیت‌های سازمانی صورت گرفته برای آماده‌سازی بازنگری‌ها، ممیزان کنترل امنیت اطلاعات نیز باید به وسیله روش‌های زیر آماده بازنگری گردند:
- به دست آوردن آگاهی کلی از عملیات‌های سازمانی (از جمله ماموریت، کارکردها، و فرآیندهای کسب‌وکار) و چگونگی پشتیبانی دارایی‌های اطلاعاتی در محدوده بازنگری از عملیات‌های سازمانی،
- به دست آوردن آگاهی از ساختار دارایی‌های اطلاعاتی (به عنوان مثال، معماری سامانه)
- به دست آوردن آگاهی کامل از تمام کنترل‌های در دست بازنگری،
- مطالعه منابع منتشر شده مربوطه که به عنوان مرجع به آن‌ها استناد می‌شود،
- شناسایی نهادهای سازمانی مسئول برای توسعه و اجرای کنترل‌های تحت نظر بازنگری که از امنیت اطلاعات پشتیبانی می‌کنند،
- برقراری نقاط تماس سازمانی مناسب مورد نیاز برای انجام بازنگری،
- به دست آوردن انواع مستندات مورد نیاز برای انجام بازنگری (به عنوان مثال خط‌مشی‌ها، روش‌های اجرایی، طرح‌ها، ویژگی‌ها، طراحی‌ها، سوابق، کتابچه راهنمای مدیر/کاربر، مستندات سامانه اطلاعاتی، توافق نامه‌های ارتباطات داخلی)،

1- Milestone
2- Artefacts

- به دست آوردن نتایج بازنگری‌های پیشین که ممکن است برای استفاده‌های مجدد در بازنگری‌ها مناسب باشد (به عنوان مثال گزارش‌ها، بازنگری‌ها، پویش‌های[1] آسیب‌پذیری، بازرسی امنیت فیزیکی، آزمون توسعه و ارزیابی)،
- برگزاری نشست با مقامات سازمانی مناسب برای اطمینان از رسیدن به یک درک مشترک برای اهداف بازنگری و میزان دقت پیشنهادی و محدوده بازنگری، و
- توسعه طرح بازنگری.

هنگام آماده سازی برای بازنگری کنترل‌های امنیت اطلاعات، اطلاعات پیش زمینه لازم باید گردآوری و در دسترس ممیزان بازنگری کنترل امنیت اطلاعات قرار گیرد. به میزانی که برای پشتیبانی از بازنگری‌های خاص لازم باشد، دسترسی‌ها به عناصر سازمانی مسئول (شامل افراد یا گروه‌ها) برای گسترش، مستندسازی، پخش، بازنگری، راه اندازی، نگهداری، به روز رسانی تمامی کنترل‌ها و خط‌مشی‌های امنیتی و روش‌های اجرایی مرتبط برای پیاده‌سازی ممیزی‌های خط‌مشی‌های سازگاری، باید شناسایی و کنترل شوند. همچنین لازم است ممیزان بازنگری کنترل امنیت اطلاعات به خط‌مشی‌های امنیتی سامانه‌های اطلاعاتی و تمامی روش‌های اجرایی مربوط به پیاده‌سازی، هر گونه مواد (به عنوان مثال، طرح‌های امنیت، سوابق، زمان‌بندی‌ها، گزارش‌های بازنگری، گزارش‌های پس از اقدام، توافق‌نامه‌ها، بسته‌های اعتبارگذاری) مرتبط با پیاده‌سازی و عملیات کنترل‌ها و موضوعات بازنگری، دسترسی داشته باشند.

در دسترس بودن مستندات و شواهد ضروری و همچنین دسترسی به کارکنان کلیدی سازمانی و سامانه اطلاعاتی موضوع بازنگری، به منظور بازنگری موفق کنترل‌های امنیت اطلاعات دارای اهمیت زیاد است.

۸-۲ توسعه یک طرح

۸-۲-۱ مرور کلی

ممیزان بازنگری کنترل امنیت اطلاعات که طرح‌های بازنگری کنترل را توسعه می‌دهند، باید نوع بازنگری کنترل (به عنوان مثال، بازنگری کامل یا جزئی) و این که کدام کنترل یا پیشرفت کنترل در بازنگری مبتنی بر هدف/محدوده باید در نظر گرفته شود را تعیین کنند. ممیزان بازنگری کنترل امنیت اطلاعات باید مخاطرات و اثرات بازنگری (در صورت وجود) را بر روی عملکرد معمول سازمان برآورد کرده و کاهش دهند و روش‌های بازنگری مناسبی را برای استفاده در مدت زمان بازنگری مبتنی بر کنترل و بهبود ممیزی‌هایی که در بازنگری در نظر گرفته شده و خصوصیات مربوط به عمق و پوشش آن را انتخاب کنند.

1- Scans

ممیزان بازنگری کنترل امنیت اطلاعات باید به دقت روش‌های اجرایی بازنگری را با سطح مخاطره سامانه اطلاعات انتخاب شده و محیط عملکرد واقعی سازمان هماهنگ نمایند. آن‌ها همچنین باید روش‌های اجرایی بازنگری بیشتری را در صورت لزوم برای نشان دادن کنترل‌های امنیتی ایجاد کنند و همچنین ایجاد بهبود در کنترل و نیازهای تضمین بیشتری که در این استاندارد تحت پوشش قرار نگرفته است، ایجاد نمایند.

طرح باید به گونه‌ای طراحی شود که شامل مراحلی برای تعیین چارچوب، ایجاد یک خط مبنای رفتار پیش‌بینی‌شده در زمینه‌های تعیین شده، ویژگی‌های آزمون‌ها/ارزیابی و روش‌های اعتبارسنجی یافته‌ها در زمینه ارزیابی باشد. طرح باید در برگیرنده‌ی گسترش یک راهبرد برای به کارگیری در روش اجرایی بازنگری توسعه یافته، بهینه سازی روش‌های اجرایی بازنگری به منظور کاهش انجام دوباره کاری امور و ارائه راه‌حل‌های بازنگری مقرون به صرفه باشد. ممیزان بازنگری کنترل امنیت اطلاعات باید طرح بازنگری را نهایی کرده و تأییدیه‌های لازم را برای اجرای این طرح اخذ نمایند.

۸-۲-۲ محدوده

مستندات باید مرور کلی از الزامات امنیتی دارایی‌های اطلاعاتی ارائه دهد و کنترل‌های موجود یا طرح‌ریزی شده برای برآوردن آن الزامات را شرح دهد. ممیز بازنگری کنترل امنیت اطلاعات باید با کنترل‌های از پیش شرح داده شده در مستندات امنیت اطلاعات را شروع کرده و همچنین هدف بازنگری را در نظر بگیرد. بازنگری می‌تواند بازنگری کاملی از همه کنترل‌های امنیت اطلاعات در یک سازمان یا بازنگری جزئی کنترل‌های حفاظت کننده دارایی‌های اطلاعاتی باشد (به عنوان مثال در پایش مستمر که در آن زیر مجموعه‌ای از کنترل‌های سرمایه‌گذاری در دارایی‌های مالی اطلاعات به صورت مداوم مورد بازنگری قرار می‌گیرد). برای بازنگری جزئی، صاحب دارایی‌های اطلاعاتی با مقامات سازمانی که علاقه‌مند به بازنگری هستند برای تعیین اینکه کدام کنترل باید مورد بازنگری قرار گیرد همکاری می‌کنند. انتخاب کنترل‌ها به زمان‌بندی برقرار شده‌ی پایش مداوم، مواردی بر طرح اقدام و نقاط کلیدی مهم بستگی دارد. کنترل‌ها برای دارایی‌هایی که دارای تغییرات گسترده‌ای می‌باشد، باید با تناوب بیشتر مورد بازنگری قرار گیرند.

۸-۲-۳ روش‌های اجرایی بازنگری

روش اجرایی بازنگری شامل مجموعه‌ای از اهداف است، که هر کدام دارای مجموعه ای مرتبط از روش‌های بازنگری بالقوه و موضوعات بازنگری می‌باشد. بیانیه‌های تصمیم[1] در هدف بازنگری، ارتباط نزدیکی با محتوای کنترل دارد (به عنوان مثال، کارکرد کنترل). این امر قابلیت ردیابی نتایج بازنگری را تا

1- Determination statement

دستیابی به الزامات اساسی کنترل، تضمین می‌کند. کاربرد روش اجرایی بازنگری در کنترل، باعث ایجاد یافته‌های بازنگری می‌شود. این یافته‌ها برای کمک به تعیین اثربخشی کلی کنترل مورد استفاده قرار می‌گیرد. موضوعات بازنگری موارد خاصی را که در دست بازنگری است شناسایی می‌کنند و مشخصات، سازوکارها، فرآیندها و افراد را در بر می‌گیرند.

پیوست الف مثال‌هایی از روش‌های اجرایی بازنگری برای وارسی انطباق فنی و بهبودهای کنترل را ارائه می‌کند. راهنمای عملی در پیوست الف به منظور تهیه شواهد برای تعیین اینکه آیا کنترل‌ها به درستی پیاده‌سازی شده است و همچنین همانطور که از پیش در نظر گرفته شده‌اند عمل می‌کنند و خروجی‌های مورد نظر را با توجه به الزامات امنیت اطلاعات و دارایی‌های مربوط به آن ایجاد می‌کنند، طراحی شده است. برای هر کنترل و ارتقاء آن که باید در این بازنگری گنجانده شود، ممیزان بازنگری کنترل امنیت اطلاعات، روش اجرایی مربوط را با مراجعه به پیوست الف توسعه می‌دهند. مجموعه روش‌های بازنگری انتخاب شده در بازنگری‌های مختلف، بر اساس هدف بازنگری تغییر خواهد کرد. (به عنوان مثال، بازنگری کنترل سالانه، پایش مستمر). پیوست الف، فرمی را برای برگزیدن روش‌های اجرایی بازنگری مناسب مبتنی بر تمرکز بر یک بازنگری خاص ارائه می‌کند.

فرآیندهای بازنگری را می‌توان متناسب با روش‌های اجرایی زیر انجام داد:

- انتخاب روش‌ها و موضوعات مورد نیاز بازنگری برای ایجاد موثرتر شیوه تعیین مناسب و برآوردن اهداف بازنگری،
- انتخاب روش عمیق و در برگیرنده مقادیر لازم خصوصیت در روش بازنگری برای برآورده کردن انتظارات مبتنی بر ویژگی‌های ویژگی‌های در حال بازنگری و تصمیم‌های خاص گرفته شده،
- از بین بردن روش‌های اجرایی بازنگری کنترل در صورتی که به وسیله فرآیند بازنگری مناسب دیگری، بازنگری شده باشند،
- توسعه سامانه اطلاعات/سکو خاص و روش اجرایی هماهنگی‌های ویژه سازمانی برای انجام موفقیت آمیز بازنگری‌ها،
- استفاده از نتایج بازنگری‌های از پیش صورت گرفته برای مواردی که کاربردپذیر تلقی می‌گردد،
- ایجاد سازگاری‌های مناسب در روش اجرایی بازنگری برای به دست آوردن شواهد لازم برای بازنگری ارائه‌کنندگان خدمات بیرون از سازمان در صورت وجود، و
- انتخاب شیوه‌های بازنگری با توجه به اثرات سازمانی خود و در عین حال اطمینان از اینکه اهداف ممیزی برآورده می‌شود.

۸-۲-۴ ملاحظات - مرتبط با موضوع[1]

سازمان‌ها می‌توانند به روش‌های مختلف دارایی‌های اطلاعاتی خود را مشخص، مستندسازی و پیکربندی کنند، محتوا و کاربرد این بازنگری شواهد ممکن است متفاوت باشند. این امر نیاز به اعمال روش‌های بازنگری گوناگون برای موضوعات بازنگری مختلف دارد تا شواهد مورد نیاز برای تعیین اینکه کنترل‌ها در کاربردشان مؤثر هستند، را ایجاد کند. بنابراین، فهرستی از شیوه‌ها و موضوعات بازنگری ارائه شده در روش بازنگری، دارای پتانسیل خوبی برای نشان دادن میزان نیاز به انتخاب مناسب‌ترین شیوه‌ها و اهداف برای یک بازنگری خاص است. روش‌ها و اهداف انتخاب شده برای ایجاد شواهد مورد نیاز برای بازنگری، ضروری تلقی می‌شوند و به صورت بالقوه برای روش‌های بازنگری به عنوان منبعی برای کمک به انتخاب این روش‌ها و اهداف مناسب ارائه شده است و هدف از ارائه آن‌ها محدود کردن انتخاب‌ها نیست. به این ترتیب، ممیزان بازنگری کنترل امنیت اطلاعات باید بر اساس قضاوت خود روش‌های بازنگری بالقوه و فهرست کلی از موضوعات بازنگری مرتبط با روش برگزیده شده را انتخاب کنند.

ممیزان بازنگری کنترل امنیت اطلاعات باید فقط روش‌ها و موضوعاتی را انتخاب کنند که بیشترین تاثیر را بر تصمیمات مرتبط با بازنگری دارند. سنجش کیفیت نتایج بازنگری مبتنی بر درستی دلایل ارائه شده است نه مجموعه‌ی خاصی از روش‌ها و موضوعات به کار گرفته شده. در بیشتر موارد لازم نیست که تمامی روش‌ها را برای همه اهداف بازنگری، به منظور به دست آوردن نتایج بازنگری‌های مطلوب مورد استفاده قرار داد و برای بازنگری‌های خاص و جامع، استفاده از روشی که در حال حاضر در مجموعه روش‌های بالقوه فهرست نشده است یا همان روش‌های پیشین کافی به نظر می‌رسد.

۸-۲-۵ یافته‌های پیشین

۸-۲-۵-۱ مرور کلی

ممیزان بازنگری کنترل امنیت اطلاعات باید از بازنگری‌های کنترل اطلاعات موجود برای آسان‌سازی بازنگری‌های موثر استفاده کنند. از نتایج بازنگری‌های قبلی مورد تایید، باید در بخش عمده‌ای از شواهدی که برای مشخص کردن میزان تعیین اثربخشی کلی کنترل در نظر گرفته شده، دوباره استفاده کرد.

هنگام استفاده مجدد از نتایج قبلی و میزان ارزش آن نتایج در بازنگری حاضر، ممیز بازنگری کنترل امنیت اطلاعات باید موارد زیر را تعیین کند:

- اعتبار شواهد،

1- Object-related

- تناسب و هماهنگی با تحلیل‌های پیشین، و
- کاربردپذیری شواهد با شرایط دارایی اطلاعاتی حاضر.

در وضعیت‌های خاص ممکن است تکمیل نتایج بازنگری‌های از پیش صورت گرفته برای استفاده مجدد در فعالیت‌های بازنگری بیشتر برای پرداختن کامل به اهداف بازنگری لازم باشد. برای مثال، اگر ارزیابی مستقل، طرف سوم از محصول فناوری اطلاعات، تنظیمات پیکربندی خاصی که به وسیله سازمان در سامانه اطلاعاتی استفاده شده رامورد آزمون قرار ندهد، آنگاه ممیزی بازنگری کنترل امنیت اطلاعات باید نتایج آزمون را با آزمون‌های بیشتری که برای تنظیمات پیکربندی محیط سامانه اطلاعاتی کنونی تحت پوشش قرار می‌گیرد، تکمیل کنند.

بخش‌های زیر باید هنگام اعتبارسنجی نتایج بازنگری‌های از قبل به دست آمده برای استفاده دوباره در بازنگری‌های جدید مورد بازنگری قرار گیرند.

۸-۲-۵-۲ تغییر شرایط

می‌توان کنترل‌هایی که در طول بازنگری‌های قبلی مفید بوده‌اند به دلیل تغییر شرایط مربوط به دارایی‌های اطلاعاتی یا محیط اطراف بی اثر باشند. بنابراین، نتایج بازنگری‌هایی که قبلا مورد تأیید بوده‌اند ممکن است شواهد قابل استنادی را برای تعیین میزان اثربخشی کنترل ارائه نکرده و به بازنگری‌های جدید نیاز باشد. کاربرد نتایج بازنگری‌های قبلی در بازنگری‌های حاضر نیازمند شناسایی تغییراتی که از زمان بازنگری قبلی تا کنون رخ داده و اثر این تغییرات در نتایج بازنگری‌های قبلی است. برای مثال استفاده دوباره از نتایج بازنگری‌های قبلی که شامل بررسی خط‌مشی‌ها و روش‌های اجرایی امنیتی یک سازمان بوده است در صورتی قابل قبول است که مشخص شود تغییرات قابل توجهی در خط‌مشی‌ها، روش‌های اجرایی و میزان مخاطره در محیط، رخ نداده است.

۸-۲-۵-۳ پذیرش استفاده مجدد بازنگری‌ها

مورد پذیرش بودن نتایج بازنگری‌ها در بازنگری کنترل باید با هماهنگی و تأیید کاربران نتایج قبلی باشد. لازم است مالک دارایی اطلاعات با مقامات مناسب سازمان (به عنوان مثال، کارشناس ارشد اطلاعات، کارشناس ارشد امنیت اطلاعات، مالک اطلاعات/ مأموریت) در تعیین قابل پذیرش بودن نتایج بازنگری‌های پیشین همکاری کند. تصمیم به استفاده مجدد از نتایج بازنگری باید در طرح بازنگری و گزارش نهایی مستند شود.

بازنگری‌های امنیت ممکن است دربرگیرنده یافته‌های بازنگری امنیت قبلی باشد تا زمانی که:

- در طرح‌های ممیزی به صراحت اجازه داده شده باشد،

- ممیزان بازنگری کنترل امنیت اطلاعات پشتوانه خوبی برای قبول باقی ماندن اعتبار این یافته‌ها داشته باشند.
- برای هر فناوری یا تغییرات در روش اجرایی در کنترل یا فرآیندهایی که در مورد آن‌ها به کار برده می‌شوند، ملاحظات امنیتی کافی در نظر گرفته شده باشد،
- استفاده‌های صورت گرفته و هماهنگی‌های انجام داده شده در پیامدهای بالقوه مدیریت مخاطره از پیش اتخاذ شده‌ی ممیزان قبلی به وضوح در گزارش‌های ممیزی عنوان شده باشد.

۸-۲-۵-۴ جنبه‌های زمانی

به طور کلی، با افزایش دوره زمانی بین بازنگری‌های قبلی و فعلی اعتبار/کارایی نتایج بازنگری‌های قبلی کاهش می‌یابد. اساسا این موضوع ناشی از این حقیقت است که دارایی‌های اطلاعاتی یا محیط بهره‌برداری با گذشت زمان تغییر کرده و احتمالا باعث نامعتبر شدن شرایط یا فرضیات اولیه‌ای می‌شود که بازنگری قبلی بر آن استوار بوده است.

۸-۲-۶ تخصیص کار

استقلال ممیز بازنگری کنترل امنیت اطلاعات یک عامل حیاتی در انواع خاصی از بازنگری‌ها، خصوصا برای دارایی‌های اطلاعاتی با سطح مخاطرات متوسط و بالا است. درجه استقلال مورد نیاز در بازنگری‌های مختلف باید ثابت باشد. به عنوان مثال، استفاده مجدد از نتایج خود- ارزشیابی قبلی جایی که نیاز به استقلال ممیز بازنگری کنترل امنیت اطلاعات نبوده است، در حالی که بازنگری‌های حاضر نیازمند میزان استقلال بیشتری است، مناسب به نظر نمی‌رسد.

۸-۲-۷ سامانه‌های بیرونی

روش‌ها[1] و روش‌های اجرایی[2] بازنگری که در پیوست الف آمده است باید برای لحاظ کردن بازنگری سامانه‌های اطلاعاتی بیرونی هماهنگ باشد. به دلیل این که سازمان بر روی کنترل‌های امنیتی که در سامانه‌های اطلاعاتی بیرونی استفاده می‌شود یا دید کافی در توسعه، پیاده‌سازی و بازنگری آن کنترل‌ها نیست، نظارت ندارد، ممکن است رویکردهای بازنگری جایگزین به کار گرفته شود. این موضوع باعث احساس نیاز به متناسب کردن روش‌های اجرایی بازنگری شرح داده شده در پیوست الف می‌شود. جایی که تضمین کنترل‌های توافق شده مورد نیاز برای سامانه‌های اطلاعاتی که در قراردادها یا توافق‌نامه‌های سطح خدمت بازنگری مستند شده‌اند. ممیز بازنگری کنترل امنیت اطلاعات باید این قراردادها را بازنگری کند و در جایی که مناسب است، روش‌های اجرایی بازنگری کنترل‌ها یا نتایج بازنگری کنترل فراهم شده

1- Methods
2- Procedures

به وسیله این قرارداد را بازنگری کند. علاوه بر آن، ممیـزان بـازنگری کنتـرل امنیـت اطلاعـات بایـد هـر بازنگری را که به وسیله سامانه‌های اطلاعاتی خارج از سازمان هدایت می‌شود یا در فرآیند هدایت است با توجه به حفاظت از دارایی‌های اطلاعاتی که مورد بازنگری قرار گرفته و می‌توان به آن تکیه کـرد در نظـر داشته باشند. در صورتی که اطلاعات کاربردی این بازنگری‌ها قابل اعتماد تلقی شود باید در گزارش اعمال شود.

۸-۲-۸ دارایی‌های اطلاعاتی و سازمان

روش‌های اجرایی بازنگری ممکن است به منظور نشان دادن وابستگی‌ها به یـک سـامانه/سـکو خـاص یـا سازمان خاص تطابق داده شود. این وضعیت ممکن است بارها در شیوه‌های اجرایـی ممیـزی مربـوط بـه کنترل‌های امنیتی از کنترل‌های فنی امنیت اطلاعات (از جمله کنترل دسترسی، ممیزی و پاسـخگویی، شناسایی و احراز هویت، سامانه و حفاظت ارتباطات) رخ دهد. اگر روش‌های آزمون ارائه شده دارای درجه بالایی از شفافیت باشند (یعنی آنچه که مورد آزمون قرار گرفته است، هم از نظر زمـانی و هـم چگـونگی آزمون) نتایج این آزمون ممکن است در بازنگری اخیر قابل کاربرد باشد. پروتکل‌هـای آزمـون مبتنـی بـر استاندارد ممکن است مثال‌هایی از چگونگی کمک به سازمان‌ها برای دستیابی به این سطح از شفافیت را ارائه کند.

۸-۲-۹ روش بازنگری توسعه یافته

سازمان‌ها انعطاف پذیری زیادی در دستیابی به الزامات تضمین کنترل امنیت اطلاعات دارند. بـرای مثـال در یک سازمان الزامی مانند تضمین در توجه به موقع به معایب، سازمان می‌تواند این الـزام را بـر اسـاس انجام ممیزی برای تمام کنترل‌ها به تفکیک، انواع کنترل، تمام سامانه‌ها بـه تفکیـک[1] یـا شـاید حتـی در سطح سازمان برآورده کند. هنگام در نظر گرفتن این انعطاف پذیری، شیوه اجرایی بازنگری توسعه یافتـه در بخش ۷-۵ بر اساس تمام بازنگری‌ها به تفکیک[2] که به طور معمول بـر اسـاس اینکـه سـازمان چگونـه تضمین را برای دارایی‌های اطلاعاتی مورد بازنگری به دست می‌آورد به کار برده می‌شود. عـلاوه بـر ایـن، سازمان اهداف بازنگری را از روش‌های اجرایی بازنگری مبتنی بر سطح مخاطره دارایی اطلاعـاتی انتخـاب می‌کند. کاربرد روش اجرایی بازنگری توسعه یافته با هدف تکمیـل سـایر روش‌هـا، بـرای افـزایش زمینـه اطمینان نسبت به اینکه کنترل‌ها به درستی پیاده‌سازی شده است و همانطور که در نظر گرفته شده عمل می‌کنند و خروجی مطلوب را با توجه به کاربرد پذیری آن در الزامات امنیت اطلاعـات ایجـاد مـی‌کننـد. می‌باشد.

1- System by system
2- Reviw by reviw

۸-۲-۱۰ بهینه‌سازی

ممیزان بازنگری کنترل امنیت اطلاعات می‌توانند دارای درجه‌ای از انعطاف پذیری در سازماندهی یک طرح بازنگری باشند که نیازهای سازمان را برآورده کند. بنابراین، این فرصتی را برای دستیابی به شواهد مورد نیاز به منظور تعیین میزان اثربخشی کنترل امنیت و در عین حال کاهش هزینه‌های کلی بازنگری‌ها فراهم می‌کند.

ترکیب و ادغام روش‌های اجرایی بازنگری زمینه‌ای است که در آن می‌توان این انعطاف پذیری را به کار برد. هنگام بازنگری، روش‌های بازنگری به دفعات در مورد موضوعات بازنگری برای یک زمینه خاص کنترل‌های امنیت اطلاعات به کار برده می‌شوند.

به منظور صرفه جویی در زمان، کاهش هزینه‌های بازنگری و افزایش سودمندی نتایج بازنگری، ممیزان بازنگری کنترل امنیت اطلاعات باید روش‌های اجرایی انتخاب شده بازنگری را برای زمینه‌های کنترل بازنگری کرده و روش‌های اجرایی (یا بخشی از روش‌های اجرایی) را تا آن جا که امکان پذیر و عملی باشد ترکیب یا ادغام کنند.

برای مثال، ممیزان بازنگری کنترل امنیت اطلاعات ممکن است تمایل به یکسان‌سازی مصاحبه‌ها داشته باشند که با مقامات کلیدی سازمان که با موضوعات گوناگون مرتبط با امنیت اطلاعات سروکار دارند، داشته باشند. ممیزان بازنگری کنترل امنیت اطلاعات ممکن است فرصت‌های دیگری برای ترکیب‌های که منجر به صرفه جویی بیشتر می‌شود را به وسیله بررسی خط‌مشی‌ها و روش‌های اجرایی امنیتی کاربردپذیر در یک زمان یا سازماندهی گروه‌های خط‌مشی‌ها و روش‌های اجرایی مربوط داشته باشند. دستیابی و بررسی تنظیمات پیکربندی اجزاء سخت افزاری و نرم افزاری مشابه در سامانه‌های اطلاعاتی مرتبط مثال دیگری از افزایش کارایی را ارائه می‌کند.

زمینه دیگری که می‌توان آن را برای بهینه سازی فرآیند بازنگری در نظر داشت، توالی است که در آن کنترل‌ها مورد بازنگری قرار می‌گیرند. بازنگری برخی از کنترل‌ها قبل از موارد دیگر ممکن است اطلاعاتی را فراهم کند که موجب آسان‌سازی میزان آگاهی و بازنگری سایر کنترل‌ها شود. برای مثال، حوزه‌های کنترلی ممکن است توضیحاتی را به صورت کلی از دارایی‌های اطلاعاتی ارائه کنند. بازنگری این کنترل‌های امنیتی در ابتدای فرآیند ممکن است درک اولیه‌ی بهتری را از دارایی‌های اطلاعاتی فراهم کرده که به بازنگری سایر فرآیندهای کنترل امنیتی کمک کند. راهنمای تکمیلی بسیاری از کنترل‌ها نیز باعث شناسایی بازنگری‌هایی مرتبطی می‌شود که اطلاعات مفیدی را برای سازماندهی روش‌های اجرایی بازنگری فراهم می‌کند. به بیان دیگر، ترتیبی که بر اساس آن بازنگری‌ها انجام می‌شوند می‌تواند موجب آسان‌تر شدن استفاده دوباره از اطلاعات بازنگری حاصل از کنترل در بازنگری دیگر کنترل‌های مرتبط شود.

۸-۲-۱۱ نهایی کردن

پس از انتخاب روش‌های اجرایی بازنگری (از جمله روش‌های اجرایی لازم برای توسعه که در این مستند به آن اشاره نشده است)، هماهنگ کردن این روش‌های اجرایی با شرایط ویژه دارایی مختص اطلاعاتی و سازمانی، بهینه‌سازی روش‌ها برای کارایی، کاربرد روش اجرایی بازنگری توسعه یافته در صورت لزوم و پرداختن به پتانسیل رویدادهای غیر منتظره که این بازنگری‌ها را تحت تأثیر قرار می‌دهد، طرح بازنگری نهایی شده و برنامه زمانبندی متشکل از نقاط کلیدی برای فرآیند بازنگری برقرار می‌گردد.

زمانی که طرح بازنگری تکمیل شد به وسیله مقامات سازمانی مناسب بازنگری و تأیید می‌شود تا از کامل بودن طرح و وجود هماهنگی با اهداف امنیت سازمان و بازنگری مخاطره سازمان با توجه به منابع اختصاص یافته برای بازنگری مقرون به صرفه اطمینان حاصل شود. در صورتی که احتمالا انجام این بازنگری موجب ایجاد وقفه در کارکرد عادی سازمان شود (به طور مثال با درگیر کردن پرسنل کلیدی یا نقص (موقت) در سامانه به دلیل آزمون نفوذ)، لازم است طرح بازنگری وسعت و چارچوب این وقفه‌ها را مشخص کند.

۸-۳ هدایت بازنگری‌ها

پس از اینکه طرح بازنگری به وسیله سازمان مورد تأیید قرار گرفت، ممیزان بازنگری کنترل امنیت اطلاعات، طرح را بر اساس نقاط کلیدی و برنامه زمان‌بندی توافق شده اجرا می‌کنند.

اهداف بازنگری به وسیله اعمال روش‌های بازنگری اختصاص یافته برای موضوعات بازنگری انتخاب‌شده و جمع آوری/ایجاد اطلاعات لازم برای تصمیمات مربوط به هریک از اهداف بازنگری به دست می‌آیند. هر گونه بیانیه که در هریک از روش اجرایی بازنگری گرفته شود به وسیله ممیزان بازنگری کنترل امنیت اطلاعات اجرایی شده و یکی از یافته‌های زیر را محقق می‌کند:

- رضایت بخشی[1] (S)
- رضایت بخشی نسبی(P)[2]، یا
- عدم رضایت بخشی (O)[3]

یافته‌هایی که مورد رضایت هستند، نشان دهنده‌ی آن بخش از کنترل‌های صورت گرفته هستند که به وسیله بیانیه‌ی تصمیم مورد اشاره قرار گرفته باشند، بازنگری اطلاعات به دست آمده (مثلا شواهد جمع

1- Satisfied
2- Partly satisfied
3- Other than satisfied

آوری شده) نشان می‌دهد که هدف بازنگری برای کنترل برآورده شده است و نتایج قابل قبولی را نیز ارائه کرده است. یک یافته رضایت بخشی نسبی نشان می‌دهد که بخشی از کنترل به هدف نپرداخته و در زمان بازنگری، پیاده‌سازی کنترل هنوز در حال انجام بوده و با تضمین منطقی کنترل به نتیجه رضایت بخش (S) خواهد رسید. یافته‌هایی که در آن عدم رضایت بخشی وجود دارد، نشان دهنده‌ی آن است برای آن بخش از کنترل‌ها که به وسیله بیانیه تصمیم مورد اشاره قرار گرفته و اطلاعات بازنگری به دست آمده نشان می‌دهد در عملیات و پیاده سازی کنترل نابهنجاری‌ها وجود داشته و لازم است که سازمان به این موضع بپردازد. یافته‌های عدم رضایت بخشی ، به دلایلی که ممکن است در گزارش بازنگری مشخص شده باشند، نشان می‌دهد که ممیزان کنترل امنیت اطلاعات توانایی دستیابی به اطلاعات کافی به منظور تصمیم ویژه برای بیانیه تصمیم را نداشته‌اند.

یافته‌های ممیزان بازنگری کنترل امنیت اطلاعات (به عنوان مثال تصمیم‌های گرفته شده) باید بدون غرض‌ورزی بوده و گزارش واقع بینانه‌ای از یافته‌های کنترل‌های بازنگری شده باشد. برای این دسته از یافته‌های عدم رضایت بخشی ، ممیزان بازنگری کنترل امنیت اطلاعات باید مشخص کنند که کدام بخش از کنترل امنیت مورد توجه قرار گرفته است (یعنی جنبه‌هایی از کنترل که رضایت بخش تلقی نشده یا قادر به بازنگری نبوده است) و توضیح دهند که چگونه نتایج کنترل از آن چه پیش از این طرح‌ریزی یا مورد انتظار بوده متفاوت است. ممیزان بازنگری کنترل امنیت اطلاعات همچنین باید خطرات بالقوه محرمانگی، یکپارچگی و دسترس‌پذیری را برای یافته‌هایی که رضایت بخشی را در پی نداشته است، ذکر کنند. اگر بازنگری، وجود ناهماهنگی زیادی را نشان دهد (یعنی یافته‌هایی که در آن رضایت بخشی نسبت به وضعیت طرح‌ریزی شده وجود ندارد و تا حد زیادی منحرف شده است)، ممکن است خطرات قابل توجهی را برای سازمان در پی داشته باشد، در این هنگام باید سریعا مدیریت و فرد مسئول این کنترل را آگاه کنند تا بتوان روش‌های اجرایی کاهش خطر را سریعا آغاز کرد.

۸-۴ تحلیل و نتایج گزارش شده

طرح بازنگری، اهداف بازنگری و نقشه راه را با جزییات و چگونگی هدایت آن ارائه می‌دهد. خروجی و نتایج نهایی بازنگری، گزارشی از بازنگری‌ها است که سطح تضمین اطلاعات را بر اساس کنترل‌های امنیت اطلاعات پیاده‌سازی شده، مستند می‌کند. لازم است گزارشی که شامل اطلاعات دریافتی از ممیزان بازنگری کنترل امنیت اطلاعات (به شکل یافته‌های بازنگری) است، میزان اثربخشی کنترل‌های به کار گرفته شده و اثر بخشی در کل سازمان برای پیاده‌سازی کنترل‌های انتخاب شده و مناسب، بر اساس یافته‌های ممیزان بازنگری کنترل امنیت اطلاعات را تعیین کند. گزارش یک عامل مهم در تعیین میزان مخاطرات امنیتی اطلاعات در عملیات‌ها (مثلا مأموریت، کارکردها) دارایی‌ها، افراد و سایر موارد سازمانی است.

نتایج بازنگری باید همراه با جزئیات مناسب برای بازنگری مطابق با قالب گزارش‌دهی مشخص شده توسط خط‌مشی سازمان، مستند شود. قالب گزارش باید همچنین برای نوع بازنگری کنترل هدایت شده (به عنوان مثال خود-ارزشیابی به وسیله دارندگان سامانه اطلاعاتی، درستی‌سنجی و اعتبارسنجی مستقل، بازنگری‌های کنترل مستقل به وسیله ممیزهای متفرقه) تناسب داشته باشد.

دارندگان سامانه اطلاعاتی به دانش فنی متخصصان امنیت اطلاعات اعتماد می‌کنند و به قضاوت فنی ممیزان بازنگری کنترل امنیت اطلاعات برای بازنگری کنترل‌های امنیتی تکیه دارند و همچنین توصیه های خاصی را در رابطه با چگونگی تصحیح نقاط ضعف و کاستی‌های موجود در کنترل ها و کاهش یا حذف آسیب‌پذیری‌های شناسایی شده ارائه می‌کنند.

اطلاعات بازنگری ایجاد شده به وسیله ممیزان بازنگری کنترل امنیت اطلاعات (یعنی یافته‌های رضایت بخش یا غیر رضایت بخش، شناسایی بخش‌های کنترل امنیت که نتایج رضایت بخشی در پی نداشته است و شرح خطرات بالقوه برای دارایی‌های اطلاعاتی) به مدیران در نسخه اولیه گزارش بازنگری امنیت ارائه می‌شود. مالکان این گونه دارایی‌ها ممکن است قبل از نهایی شدن گزارش به توصیه‌های ممیزان بازنگری کنترل امنیت اطلاعات اقدام نمایند تا فرصت‌های خاصی برای تصحیح نقاط ضعف یا کاستی‌ها در کنترل‌ها یا تصحیح یا شفاف‌سازی سوء تفاهم‌ها یا تفاسیر غلط در رابطه با نتایج بازنگری را فراهم کنند. ممیزان بازنگری کنترل امنیت اطلاعات باید کنترل‌هایی را که در آن موجب تغییر و بهبود می‌شود یا به آن اضافه شده است را در طول این فرآیند قبل از ایجاد گزارش نهایی مجددا بازنگری نمایند. تحویل گزارش پایانی به مدیریت، نشان رسمی به پایان رسیدن بازنگری کنترل امنیت اطلاعات است.

از آنجایی که نتایج بازنگری در نهایت بر محتوای کنترل‌های امنیت اطلاعات و طرح اقدام نقاط کلیدی اثر می‌گذارد، مالکین دارایی‌های اطلاعاتی، یافته‌های ممیزان بازنگری کنترل امنیت اطلاعات را باید مورد بازنگری خود قرار دهند و با موافقت مدیریت مراحل مناسب و لازم را برای تصحیح ضعف‌ها و کمبودهای شناسایی شده طی بازنگری صورت گرفته، تعیین کنند. استفاده از برچسب‌هایی که وجود یا عدم وجود رضایت را مشخص می‌کند، قالب گزارش‌دهی برای یافته‌های بازنگری‌های مشاهده شده و برای مدیران نسبت به ضعف‌ها و کاستی‌های امنیت اطلاعات را فراهم کرده و رویکردی ساخت یافته و نظام‌مند را برای کاهش مخاطره، بر اساس فرآیند مدیریت مخاطره امنیت اطلاعات، فراهم می‌کند. برای مثال، مالک دارایی اطلاعاتی هنگام مشورت با مدیران ممکن است تصمیم بگیرد که برخی از یافته‌های بازنگری که نشانه‌هایی از عدم رضایت در آن است را دارای ماهیتی غیر منطقی بیابند و بدانند که هیچ مخاطره قابل توجهی برای سازمان ایجاد نمی‌کند. از طرف دیگر شاید آن‌ها این نشانه‌ها را مهم تلقی کرده و خواستار اقدامات جبرانی سریع باشند. در همه موارد، سازمان هریک از یافته‌های ممیزان بازنگری کنترل امنیت اطلاعات را بازنگری کرده و قضاوت خود را با توجه به اهمیت آن یافته (یعنی اثر معکوس بالقوه بر روی عملیات، دارایی‌ها، افراد سازمان) صرف نظر از اینکه آن یافته آن قدر مهم است که ارزش بررسی یا اقدام

جبرانی را داشته باشد یا نه، اعمال می‌کند. درگیر نمودن مدیران ارشد در فرآیند کاهش ممکن است به منظور اطمینان از اینکه منابع سازمان به درستی مطابق با اولویت‌های سازمانی اختصاص یافته و منابع در ابتدا برای دارایی‌های اطلاعاتی که از بیشتر فرآیندهای مهم کسب وکار پشتیبانی می‌کنند یا کاستی‌ها را جبران می‌کنند، فراهم شود. در نهایت، یافته‌های بازنگری و هر اقدام جبرانی دیگر که به وسیله مالک دارایی اطلاعاتی با همکاری مقامات سازمانی آغاز می‌شود، آغازکننده فرآیند به روز رسانی در مدیریت مخاطره امنیت اطلاعات و کنترل‌های امنیت اطلاعات است. بنابراین، مستندات کلیدی استفاده شده به وسیله مدیران به منظور تعیین وضعیت امنیت اطلاعات دارایی‌های اطلاعاتی به روز رسانی می‌شود تا منعکس کننده نتایج بازنگری باشد.

طی نقاط کلیدی از پیش تعیین شده یا دوره های ثابت بازنگری، به عنوان مثال سه ماه پس از گزارش نهایی، یک بازنگری پیگیری با تمرکز بر مسائل باقی‌مانده یا «بسته‌نشده» به طور معمول انجام می‌گیرد. این مراحل شامل اعتبارسنجی راه‌حل‌های پیاده‌سازی شده در یافته‌های قبلی نیز می‌باشد. ممکن است سازمان‌ها تصمیم به هدایت فعالیت‌های پیگیری در بازنگری‌های بعدی بگیرند، خصوصا برای مسائلی که غیر بحرانی یا غیر اضطراری هستند.

پیوست الف

(اطلاعاتی)

راهنمای عملی وارسی انطباق فنی

این پیوست با استفاده از کنترل‌های فنی معمول برگرفته از ISO/IEC ۲۷۰۰۲ برای وارسی انطباق فنی، مجموعه‌ای از راهنماهای عملی را ارائه می‌کند. هر کنترل در پیوست الف بر اساس ساختار بیانیه و راهنمایی زیر سازماندهی شده است.

«کنترل فنی» (همراه با «اطلاعات فنی اضافی»)

۱- استاندارد پیاده‌سازی امنیت (همراه با «نکات فنی درباره استاندارد پیاده‌سازی امنیت»)
۱-۱ راهنمای عملی، شواهد مفروض، روش
۱-۲ راهنمای عملی، شواهد مفروض، روش
۲- استاندارد پیاده‌سازی امنیت (همراه با «نکات فنی درباره استاندارد پیاده‌سازی امنیت»)
۲-۱ راهنمای عملی، شواهد مفروض، روش
۲-۲ راهنمای عملی، شواهد مفروض، روش

هر کنترل فنی، دارای اطلاعات فنی اضافی، برای پشتیبانی بیشتر، از ممیزان بازنگری کنترل امنیت اطلاعات است. این کنترل، به طور کلی شامل تعدادی از «استانداردهای پیاده‌سازی امنیت» است که باید مرتب به وسیله سازمان بازنگری شوند تا تعیین شود که استانداردهای کاربردپذیر، به درستی پیاده‌سازی و راه‌اندازی شده است.

هر «استاندارد پیاده‌سازی امنیت»، دارای یک «نکته فنی اضافی درباره استاندارد پیاده‌سازی امنیت» است که اطلاعات فنی بیشتری را برای فرآیند بازنگری در اختیار قرار می‌دهد. همچنین تعدادی از «راهنماهای عملی»، «شواهد مفروض» و «روش» را نیز ارائه می‌کند.

«راهنمای عملی»، روش اجرایی وارسی انطباق را به منظور اعمال برای استاندارد پیاده‌سازی امنیت فراهم می‌کند. شواهد مفروض، برخی از مثال‌هایی از سامانه‌ها، فایل‌ها، مستندات یا سایر مواردی را ارائه می‌دهد که می‌توان آن‌ها را به عنوان «شواهد» در روش اجرایی وارسی انطباق پذیرفت. لطفا توجه کنید که اسامی شواهد ممکن است در سازمان‌های مختلف متفاوت باشند. با این وجود، اسامی استفاده شده در این پیوست را می‌توان به عنوان اسامی عمومی پذیرفته شده در زمینه وارسی انطباق فنی در نظر گرفت. «روش»، رویکردی مناسب را برای وارسی انطباق فنی بر اساس راهنمای عملی در بالا فراهم می‌کند.

این پیوست راهنماهای عملی جامعی را برای وارسی انطباق فنی ارائه نمی‌کند، بلکه تا حد زیادی به سازمان‌ها کمک می‌کند بازنگری نمایند که آیا استانداردهای پیاده‌سازی امنیت به درستی پیاده‌سازی و راه‌اندازی شده است.

الف-۱ وارسی فنی کنترل در مقابل کدهای مخرب

کنترل	**بند ۱۰-۴-۱ ISO/IEC ۲۷۰۰۲ کنترل‌ها در مقابل کدهای مخرب** تشخیص، جلوگیری و بازیابی کنترل‌ها به منظور حفاظت در برابر کد مخرب و روش‌های مناسب آگاهی کاربر باید پیاده‌سازی شود.
اطلاعات فنی اضافی	کد مخرب (بدافزار[1]) یک اصطلاح کلی است که برای اشاره به کدهای قرار داده شده در نرم‌افزار، برنامه، اسکریپت استفاده شده که به منظور آسیب به سامانه رایانه‌ای به وسیله سرقت اطلاعات، تقلب، جاسوسی، خرابکاری و تخریب طراحی شده است به کار می‌رود. زمانی که بدافزار وارد یک سامانه رایانه‌ی می‌شود، سامانه ممکن است دچار آسیب شده یا ممکن است اطلاعات سامانه به سرقت رود، همچنین این احتمال وجود دارد که رفتار آن سبب ایجاد آسیب به سایر سامانه‌ها شود. کدهای مخرب شامل ویروس‌های رایانه‌ی، کرم‌ها، تروجان‌ها، روبات‌ها، نرم‌افزارهای جاسوسی[2]، تبلیغات متقلبانه، و سایر نرم‌افزارهای مخرب و ناخواسته باشد. در شرایطی که شبکه سازمان به اینترنت متصل است، ممیزان بازنگری کنترل امنیت اطلاعات باید بازنگری کنند که کارکردهای تشخیص/جلوگیری بدافزارها در مرز اینترنت به صورت کارآمد و موثر نصب شده و وظایف خود را به درستی انجام می‌دهند. خصوصا، به منظور بازنگری این که کارکرد تشخیص/جلوگیری به درستی عمل می‌کند، ممیزان بازنگری کنترل امنیت اطلاعات باید تأیید کنند که الگوهای فایل‌ها یا امضاهای استفاده شده برای تشخیص بدافزار به روز رسانی شده‌اند. برخی از سامانه‌های تشخیص/جلوگیری به گونه‌ای طراحی شده‌اند که بدافزار را با استفاده از الگوی امضاء فایل تشخیص داده و برخی دیگر به گونه‌ای طراحی شده‌اند که رفتار غیرطبیعی سامانه رایانه‌ی را بدون استفاده از فایل‌های الگو یا امضاها تشخیص دهند. از آنجایی که برخی از الگوهای اتصال به اینترنت نظیر اتصال شبکه سازمان به وسیله گذرگاه یا اتصال هر رایانه به طور جداگانه مستقیما به اینترنت وجود دارد، ممیزان بازنگری کنترل امنیت اطلاعات باید اطمینان حاصل کنند که سامانه تشخیص/جلوگیری به درستی

1- Malware
2- Spyware

			تحت هر شرایطی عمل می‌کند. **یادآوری**- ممیزان بازنگری کنترل امنیت اطلاعات باید مطلع باشند که توانایی سامانه تشخیص/جلوگیری برای بدافزارهای ناشناخته چون حمله روز صفر[1] محدود می‌باشد.
۱	استاندارد پیاده‌سازی امنیت		نصب و به‌روزرسانی منظم تشخیص کد مخرب و تعمیر نرم‌افزار جهت پویش رایانه‌ها و رسانه به عنوان یک کنترل پیشگیرانه، یا به طور منظم. وارسی‌های انجام شده باید شامل موارد زیر باشد: ۱- وارسی هر یک از فایل‌های رسانه الکترونیکی یا نوری و فایل‌های دریافت شده به وسیله شبکه برای کد مخرب قبل از استفاده؛ ۲- وارسی پیوست‌های رایانامه و دانلودها برای کد مخرب قبل از استفاده؛ این وارسی باید در مکان‌های مختلفی نظیر کارساز[2]های رایانامه، رایانه‌های رومیزی و هنگام ورود به شبکه سازمان انجام شود؛ ۳- وارسی صفحات وب برای کد مخرب.
	نکات فنی مربوط به اجرای استاندارد امنیتی		در درگاه، ورودی شبکه سازمان، سامانه تشخیص/جلوگیری نرم افزارهای مخرب باید به درستی برای خدمات یا پروتکل های شبکه‌ای نظیر WWW، رایانامه (Mail) و FTP کار کند.
	۱-۱	راهنماهای عملی	راهنماهای عملی ذیل که برای «استاندارد پیاده‌سازی امنیت» به کار برده می‌شود به ترتیب عبارتند از ۱-، ۲- و ۳-. ۱- وارسی کنید که تشخیص کد مخرب و سامانه مرمت به طور جامع و موثر برای همه فایل‌های رسانه‌های الکترونیکی یا نوری و فایل‌های دریافت شده از شبکه توسط بازنگری ویژگی‌های سامانه یا نمودارهای شبکه قرار داده شده‌اند. ممیزان بازنگری کنترل امنیت اطلاعات وارسی می‌کنند که سامانه تشخیص/جلوگیری به طور جامع و به طور موثر توسط بازنگری ویژگی‌های سیستم یا نمودارهای شبکه قرار گرفته شده است. ۲- وارسی کنید که تشخیص کد مخرب و سامانه مرمت به طور جامع و

1- Zero day attack
2- Server

			موثر برای هر فایل الصاقی و بارگیری‌شده رایانامه توسط بازنگری ویژگی سامانه یا نمودارهای شبکه که شامل کارساز رایانامه، رایانه‌های رومیزی و درگاه شبکه قرار داده شده‌اند. تشخیص کد مخرب و سامانه مرمت گاهی اوقات به روشنی در مشخصات سامانه به عنوان یک افزاره انحصاری شرح داده شده است، با این وجود، ممیزان بازنگری کنترل امنیت اطلاعات باید توجه داشته باشند که در کارسازهای که برای ارائه کارکردها و خدمات دیگر (www، رایانامه و FTP) قرار داده شده و بنابراین ذاتاً در مشخصات سامانه بدون توضیح روشن قرار داده شده‌اند. برای رایانه‌های رومیزی، ممیزان بازنگری کنترل امنیت اطلاعات باید توجه داشته باشند که تشخیص کد مخرب و سامانه مرمت بدون توضیح روشن در مشخصات سامانه قرار داده شده است. ۳- وارسی کنید که تشخیص کد مخرب و سامانه مرمت به طور جامع و موثر برای صفحات وب توسط بازنگری ویژگی‌های سیستم و نمودارهای شبکه که شامل کارساز وب است قرار داده شده‌اند. برای رایانه‌های رومیزی که برای بازنگری صفحات وب استفاده می‌شوند، ممیزان بازنگری کنترل امنیت اطلاعات باید توجه داشته باشند که تشخیص کد مخرب و سامانه مرمت به طور ذاتی در مشخصات سامانه بدون توضیح روشن قرار داده شده است. در این مورد، تشخیص کد مخرب و سامانه مرمت ممکن است به طور ذاتی در مرورگر واقع شده باشد. برای کارساز وب، تشخیص کد مخرب و سامانه مرمت گاهی اوقات به روشنی در مشخصات سامانه به عنوان یک افزاره انحصاری شرح داده شده است، با این وجود، ممیزان بازنگری کنترل امنیت اطلاعات باید توجه داشته باشند که به طور ذاتی در مشخصات سامانه بدون توضیح روشن واقع شده است.
		شواهد مفروض	مشخصات سامانه، نمودارهای شبکه
		روش	بررسی/بازنگری
	۲-۱	راهنمای عملی	راهنماهای عملی ذیل که برای «استاندارد پیاده‌سازی امنیت» به کار برده می‌شود به ترتیب عبارتند از ۱-، ۲- و ۳-. ۱- وارسی کنید که تشخیص کد مخرب و سامانه مرمت قرار داده شده‌اند و به درستی برای همه فایل‌های رسانه‌های الکترونیکی و نوری و فایل‌های دریافت شده از شبکه به وسیله مشاهده تسهیلات پردازش اطلاعات کار

			می‌کند. وارسی کنید که آیا نرم‌افزار مدیریت در سامانه یکپارچه تحت شرایطی که تشخیص کد مخرب و سامانه مرمت در یک سامانه یکپارچه مدیریت می‌شود به درستی کار می‌کند. ۲- وارسی کنید که تشخیص کد مخرب و سامانه مرمت قرار داده شده‌اند و به درستی برای تشخیص هر الصاق رایانامه و فایل‌های بارگیری شده در کارساز رایانامه، رایانه‌های رومیزی نمونه و درگاه شبکه با مشاهده تسهیلات پردازش اطلاعات کار می‌کنند. برای پست‌های الکترونیک، وارسی کنید که سامانه تشخیص هم برای فایل‌های پیوست شده و هم کد مخرب در متن رایانامه html عمل می‌کند. ۳- وارسی کنید که تشخیص کد مخرب و سامانه مرمت قرار داده شده‌اند و به درستی برای تشخیص صفحات وب به وسیله مشاهده تسهیلات پردازش اطلاعات کار می‌کند. برای رایانه‌های رومیزی که برای بازنگری و مرور صفحات وب استفاده می شوند، وارسی کنید که سامانه تشخیص برای Active x control و اسکریپت‌ها و غیره به درستی کار می‌کند. وارسی کنید که برای کارساز وب، مانند apache، IIS[1] و غیره سامانه تشخیص هم برای فایل‌های html و هم کد مخرب در خدمات تحت وب۲ به درستی عمل می‌کند.
		شـــــــواهد مفروض	تسهیلات تشخیص کد مخرب و سـامانه مرمـت قـرار داده شـده اسـت: بـه عنوان مثال: • کارساز فایل • کارساز رایانامه • رایانه‌های رومیزی نمونه • رایانه‌های با قابلیت جابجایی • تشخیص ویژه کد مخرب و سامانه مرمت قرار داده شده در درگاه شبکه (مرز بین شبکه سازمان و اینترنت) • کارساز وب • پیشکار[3] • مرورگر وب • سایر (افزاره‌ی مسدود کردن USB که به طور فیزیکی وارد می‌شود)

1- Internet Information Services
2- Web service
3 - Proxy server

		روش	بررسی/ مشاهده
	۳-۱	راهنمـــــای عملی	فایل‌های واقعه‌نگاری[1] را از سامانه تشـخیص و تعمیـر جمـع آوری کـرده و وارسی کنید که سوابق واقعه‌نگاری نشان دهنده در حال اجرا بـودن سـامانه می‌باشد و اقدام لازم هنگام تشخیص بدافزار انجام شده است. **یادآوری**- برای رایانه‌های رومیزی، خروجـی معمـولی واقعـه‌نگـاری از سامانه تشخیص و تعمیر در رایانه‌هـا ذخیـره مـی‌شـوند. بـرای کارسـازها و افزاره‌های خارجی، این واقعه‌نگاری گاهی به سامانه‌های دیگری بـه وسـیله پروتکل‌های انتقالی نظیر syslog منتقل و در آنجا ذخیره می‌شوند. • برای رایانه‌های رومیزی که برای بازدید و مرور صفحات وب استفاده می‌شوند، عمل تشخیص در مرورگر وب ممکن است سوابق واقعه‌نگاری که نشان می‌دهد تابع در حال اجرا است را تولید نکند. در عوض بیشتر مرورگرها پیغامی را در مواقعی که اسکریپت‌های غیرمجاز تشخیص داده می‌شوند نمایش می‌دهند.
		شـــــــواهد مفروض	• سامانه تشخیص در خدمت • خروجی فایل واقعه‌نگاری از سامانه تشخیص • سوابق هشدار سامانه تشخیص • پیغام از سامانه تشخیص در مرورگر وب
		روش	بررسی/ مشاهده
	استـــــاندارد پیاده سـازی امنیت	نرم‌افزار تشخیص و مرمت کد مخرب، به منظور پویش[2] رایانه‌ها و رسانه‌هـا بـه عنـوان یـک کنترل پیشگیرانه باید به طور منظم یا به طور معمول به روز رسانی شود.	
	نکـات فنـی مربـوط بـه پیاده سـازی اسـتاندارد امنیتی	در بیشتر موارد، کارکردهایی برای به روز رسانی فایل‌های الگو یا امضاها بـه طـور خودکـار وجود دارد.	
	۲-۱	راهنمـــــای	وارسی کنید که طراحی نرم‌افزار تشخیص و مرمت کد مخرب را بـه منظـور

1- Log
2- Scan

		عملی	به روز رسانی خودکار فایل‌های الگو یا امضاها به طور خودکار یا بـر اسـاس یک روال مشخص هستند.
		شـــــــواهد مفروض	طراحی یا مشخصات سامانه تشخیص
		روش	بررسی/بازنگری
	۲-۲	راهنمـــــای عملی	وارسی کنید که تنظیمات نرم‌افزار تشخیص و مرمت کد مخرب بـه منظـور به روز رسانی خودکار فایل‌های الگو یا امضاها به طور خودکار یا بـر اسـاس یک روال مشخص هستند.
		شـــــــواهد مفروض	• تنظیمات سامانه تشخیص
		روش	بررسی/مشاهده
	۳-۲	راهنمـــــای عملی	وارسی کنید فایل‌های الگو یا امضاها از طریق مشاهده نام محصول، نسـخه و واقعه‌نگاری فایل‌های الگو یا امضا به روز رسانی شده‌اند.
		شـــــــواهد مفروض	اطلاعات سامانه تشخیص/تعمیر یعنی: • نام محصول • نسخه محصول • نسخه فایل الگو یا امضا
		روش	بررسی/مشاهده

الف-۲ وارسی فنی کنترل مربوط به واقعه‌نگاری ممیزی	
کنترل	**بند ۱۰-۱۰-۱ ISO/IEC ۲۷۰۰۲ واقعه‌نگاری ممیزی** واقعه‌نگاری ممیزی فعالیت‌های کاربران، استثنائات و رویدادهای امنیت اطلاعات که باید برای دوره زمانی توافق شده به منظور کمک به بررسی‌ها و بازنگری کنترل دسترسی ایجاد و نگهداری شوند را ثبت می‌کند.
اطلاعات فنی اضافی	به منظور تشخیص فعالیت های پردازش اطلاعات غیر مجاز، مهم است که واقعه‌نگاری ممیزی که به منظور دنبال کردن فعالیت‌های کاربران، عملیات سامانه، رویدادهای امنیت و سامانه‌ها است، ثبت شود. واقعه‌نگاری ممیزی به منظور تحلیل فعالیت‌های تصدیق نشده، رویدادهای امنیتی رخ داده باید شامل موارد زیر باشند: • شناسه‌های کاربر • تاریخ‌ها، زمان،رویدادهای کلیدی همچون ورود یا خروج سامانه • شناسایی پایانه • نشانی‌های شبکه و پروتکل‌ها به منظور ایجاد سوابق لازم شامل اطلاعات بالا، تجهیزاتی که واقعه نگاری‌ها را ایجاد می‌کنند باید تنظیم شوند یا برخی قواعد برای آن‌ها به کار برده شود. روش واقعه‌نگاری وابسته به ساختار سامانه، معماری و کاربردهای پیاده‌سازی شده است. ممیزان بازنگری کنترل امنیت اطلاعات باید تفاوت روش واقعه‌نگاری برای معماری سامانه متفاوت همچون کارسازها و رایانه‌های رومیزی در نظر قرار دهند. **یادآوری-** • مثال‌هایی از ساختار سامانه که باید مد نظر قرار گیرند عبارتند از: • سامانه کارساز کلاینت[1]؛ • سامانه مبتنی بر وب[2]؛ • سامانه کلاینت نازک[3]؛ • مجازی‌سازی؛

1- Client server system
2- Web based system
3- Thin client system

			• به کارگیری ASP[1] (فراهم کننده خدمت کاربرد)، SaaS[2] (نرم‌افزار به عنوان خدمت) یا رایانش ابری. • مثال‌هایی از معماری سامانه که باید مد نظر قرار گیرند عبارتند از: • یونیکس؛ لینوکس؛ • ویندوز؛ • سامانه بزرگ رایانه[3]. • مثال‌هایی از انواع واقعه‌نگاری که باید مد نظر قرار گیرند عبارتند از: • فایل واقعه‌نگاری سامانه • فایل واقعه‌نگاری کاربرد
۱	استاندارد پیاده‌سازی امنیت		فعالیت‌های کاربر واقعه‌نگار ممیز، استثنائات و رویدادهای امنیت اطلاعات باید ایجاد شود. سوابق ممیزی باید شامل موارد زیر باشند: الف- شناسه‌های کاربر؛ ب- تاریخ‌ها، زمان‌ها و جزئیات رویدادهای کلیدی نظیر ورود و خروج؛ پ- شناسه پایانه یا مکان احتمالی؛
	اطلاعات فنی بر استاندارد پیاده‌سازی امنیت		ت- سوابق تلاش موفق یا ناموفق دسترسی به سامانه؛ ث- سوابق تلاش موفق یا ناموفق دسترسی به داده‌ها یا دیگر منابع؛ ج- تغییرات در پیکربندی سامانه؛ چ- استفاده از کاربردهای سامانه؛ ح- دسترسی به فایل‌ها و نوع دسترسی؛ خ- نشانی‌های شبکه و پروتکل‌ها؛ د- هشدارهای ایجاد شده به وسیله سامانه کنترل دسترسی؛ ذ- فعالسازی و غیر فعالسازی سامانه‌های حفاظتی، نظیر سامانه‌های آنتی ویروس و سامانه‌های تشخیص نفوذ.
	اطلاعات فنی بر استاندارد پیاده‌سازی امنیت		به منظور پیدا کردن رویدادهای امنیتی و دلایل آن، ممیزان بازنگری کنترل امنیت، وضعیت عملیات سامانه، استفاده و تغییر از سوابق واقعه‌نگاری را تحلیل می‌کنند. به منظور وارسی رویدادها، علت رویدادها، سوابق ممیزی از سامانه‌های مختلف باید با یکدیگر ترکیب شوند. به این منظور، درک موقعیت و نوع فایل واقعه نگاری ممیزی با توجه به، ساختار/معماری/پیکربندی مهم است.
	۱-۱	راهنمای عملی	وارسی کنید که طراحی سامانه واقعه‌نگاری مبتنی بر استاندارد پیاده‌سازی امنیت می‌باشد.

1- Application service provider
2- Software as a service
3- Mainframe

		شـــــواهد مفروض	• مستند مشخصات • مستند تعریف الزامات • مستند طراحی نرم‌افزار
		روش	بررسی/بازنگری
	۲-۱	راهنمـــای عملی	وارسی کنید که تنظیمات فایل‌های پیکربندی سامانه واقعه‌نگاری مطابق بـا مستندات طراحی سامانه است.
		شـــــواهد مفروض	• مستند طراحی نرم‌افزار • فایل پیکربندی سامانه
		روش	بررسی/مشاهده
	۳-۱	راهنمـــای عملی	وارسی کنید که سوابق فایل‌های واقعه‌نگاری ممیـزی مطـابق بـا مسـتندات طراحی سامانه باشند. **یادآوری**- در واقعه نگاری ممیزی، برخی سـوابق وجـود دارد کـه ثابـت هستند و برخی سوابق مانند سوابق خطا اینگونه نیستند. به منظـور وارسـی اینکه آیا سامانه، سوابقی که تنها در برخی حالات خاص ظاهر مـی‌شـوند را ثبت می‌کند. ممیزان بازنگری کنترل امنیت اطلاعات ممکن اسـت نیـاز بـه استفاده از سنجش‌های متفاوتی شامل ایجاد حالت آزمون، وارسی مستندات طراحی سامانه داشته باشند.
		شـــــواهد مفروض	• فایل واقعه‌نگاری
		روش	بررسی/مشاهده
	۴-۱		راهنمای عملی وارسی کنید که یکپارچگی سـوابق در واقعـه‌نگـاری ممیـزی بـرای تعیـین واقعه‌نگاری مناسب است. **یادآوری**- برخی سوابق که باید در واقعه‌نگاری ممیـزی ثبـت شـود بـه دلیل کمبود کارایی قابلیت سامانه یا به دلایل دیگر از دست رفته‌اند، گرچـه تنظیمات واقعه‌نگاری مناسب باشد.
		شـــــواهد	• فایل واقعه‌نگاری

		مفروض	
		• روش	بررسی/مشاهده
۲	استاندارد پیاده‌سازی امنیت	واقعه‌نگاری ممیزی باید به مدت توافق شده‌ای برای کمک به بررسی‌ها و پایش کنترل دسترسی نگه داشته شوند.	
	نکات فنی مربوط به استاندارد پیاده‌سازی امنیتی	در برخی موارد، دوره‌های نگهداری واقعه‌نگاری ممیزی بر اساس هدف کسب‌وکار، قرارداد یا قوانین/مقررات تعریف می‌شود. برای مثال، واقعه‌نگاری ممیزی که شامل هشدارهای ایجاد شده به وسیله دسترسی به سامانه کنترل هستند، باید تا زمان بررسی رویدادها، و تکمیل علت رویدادها نگهداری شوند. **یادآوری**- سامانه تازه به کار گرفته‌شده مرتبط عملیات آغاز شده و واقعه‌نگاری ممیزی آن در زمان توافق ذخیره نشده است. در چنین حالتی به منظور دستیابی راهنمای عملی ۲-۳، ۲-۱ و ۲-۲ که در ذیل آمده لازم است وارسی شوند.	
	۲-۱	راهنمای عملی	وارسی کنید دوره ذخیره واقعه نگاری ممیزی مطابق با مستندات طراحی سامانه باشد.
		شواهد مفروض	• فایل واقعه‌نگاری • مستند طراحی سامانه
		روش	بررسی/مشاهده
	۲-۲	راهنمای عملی	تنظیمات دوره ذخیره واقعه‌نگاری ممیزی در سامانه را وارسی کنید تا مطابق با مستندات طراحی سامانه یا تنظیمات بازنویسی یا پاک کردن واقعه‌نگاری ممیزی، قبل از زمان ذخیره‌سازی به کار گرفته نشده باشند.
		شواهد مفروض	• فایل واقعه‌نگاری • مستندات طراحی سامانه
		• روش	بررسی/مشاهده
	۲-۳	راهنمای عملی	وارسی کنید که دوره ذخیره واقعه‌نگاری ممیزی طولانی‌تر از دوره توافق شده مشاهده فایل‌های واقعه‌نگاری یا برنامه زمانی[1] واقعه‌نگاری باشد.

1- Timestamp

		شـــــواهد مفروض	• فایل واقعه‌نگاری • مستندات طراحی سامانه
		روش	بررسی/مشاهده

الف- ۳ وارسی فنی کنترل مدیریت با اختیارات ویژه	
کنترل	**بند ۱۱-۲-۲ ISO/IEC ۲۷۰۰۲ اختیارات ویژه** اختصاص و استفاده از اختیارات ویژه باید محدود شده و کنترل شده باشد.
اطلاعـــات فنـــی اضافی	مدیریت اختیارات ویژه مهم است چون استفاده نامناسب از اختیارات ویژه سبب اثرات قابـل توجه بر روی سامانه‌ها می‌شود. وضعیت اختصاص اختیارات ویژه باید در مستندات شـرح داده شـده کـه اختیـارات ویـژه را تعریف کند (مستند تعریف اختیارات ویژه). چون دسترسی اختیـارات ویـژه مربـوط بـه هـر محصول (سامانه عملیاتی، سامانه مدیریت پایگاه داده، و کـاربرد هـر کـدام) متفـاوت اسـت. مثال‌های انواع اختیارات ویژه عبارتند از: • root (یونیکس، لینوکس) • سرپرست (ویندوز) • کاربر پشتیبان (ویندوز) • کاربر توان[1] (ویندوز) • sa (DBMS)[2] و • DB admin (DBMS) . اختصاص اختیارات ویژه باید بر اساس کمترین نیـاز باشـد. همچنـین اختصـاص مـداوم آن ضروری نیست. روش مدیریت اختیارات ویژه در سامانه هـای مختلـف اسـت. مثـال‌هـایی از مدیریت اختیارات ویژه در سامانه‌ها عبارتند از: • در سیستم عامل، ACL[3] (فهرست کنترل دسترسی) اختیارات ویژه را تعریف می‌کند. • در DBMS تنوع اختیارات ویژه پیش فرض را تعریف می‌کند. • در کاربردها ممکن است طیف وسیعی از اختیارات ویژه پیش فرض را برای کارکرد

1- Power user
2- Database management system
3- Access Control List

			مدیریت کاربرد تعریف کرده تا ممیز بازنگری کنترل امنیت اطلاعات سطح بازنگری را از قبل وارسی کند، و • در OS امن، دارای کارکرد اجباری کنترل دسترسی است.
۱	استاندارد پیاده سازی امنیت		اختیارات ویژه دسترسی مربوط به هر محصول سامانه از جمله سیستم عامل، سامانه مدیریت پایگاه و هر نرم افزار کاربردی و کاربرانی که نیاز به تخصیص دارند باید شناسایی شود. نکات فنی مربوط به استاندارد پیاده‌سازی امنیت فعالیت کاربران دارای اختیارات ویژه باید مورد بازنگری قرار گیرد، چون استفاده نامناسب از اختیارات ویژه باعث ایجاد اثرات قابل توجه بر سامانه می‌شود. روش های تشخیص استفاده نامناسب در معماری‌های مختلف متفاوت هستند. **یادآوری-** معماری‌های سامانه نماینده عبارتند از: • سامانه اصلی[1] • ویندوز • یونیکس، لینوکس • سیستم عامل امن
	۱-۱	راهنمای عملی	وارسی کنید که اختصاص اختیارات ویژه در مستند تعریف اختیارات ویژه شرح داده شده باشد.
		شواهد مفروض	• مستند تعریف اختیارات ویژه
		روش	بررسی/مشاهده
	۲-۱	راهنمای عملی	وارسی کنید که تنظیمات پیکربندی سامانه مطابق با مستندات توصیف شده اختیارات ویژه باشد. روش وارسی عملیات اختیارات ویژه در معماری‌های مختلف متفاوت است. مثال‌های از روش وارسی عملیات اختیارات ویژه عبارتند از: ۱- (در مورد سامانه اصلی) وارسی کنید وضعیت استفاده از اختیارات ویژه به وسیله وارسی گزارش RACF[2] (تسهیل کنترل دسترسی منابع) مناسب باشد.

1- Mainframe
2- Resource access control facility

			۲- (در مورد یونیکس، لینوکس یا ویندوز) وارسی کنید که وضعیت استفاده از اختیارات ویژه به وسیله بررسی واقعه‌نگاری که استفاده از اختیارات ویژه را نشان می‌دهند مناسب باشد. **یادآوری-** • RACF (تسهیل کنترل دسترسی منابع) در سامانه اصلی میان‌افزار مدیریت امنیت است. • در یونیکس یا لینوکس، خطرناک است که فقط ورود توسط root به منظور وارسی نا مناسب استفاده از root بررسی شود. دلیل این امر این است که کاربران عادی ممکن است توسط استفاده از دستور su بعد از ورود به یونیکس یا لینوکس root شوند.
		شواهد مفروض	• مستند تعریف اختیارات ویژه • فهرست کنترل دسترسی • گزارش RACF
		روش	بررسی/ مشاهده
۲	استاندارد پیاده سازی امنیت	اختیارات ویژه باید به شناسه کاربر متفاوتی که برای استفاده معمول کسب‌وکار است اختصاص یابد.	
	نکات فنی مربوط به استاندارد پیاده سازی امنیت	در صورت دسترسی به وسیله اختیارات ویژه، امکان عملیات غیر مجاز وجود داشته و وضعیت استفاده از اختیارات ویژه تبدیل به زمینه‌ای برای دسترسی‌های غیرمجاز می‌شود. اگر این عملیات نیاز به اختیارات ویژه ندارد کاربران باید شناسه عادی را استفاده کنند. اگر ورود به وسیله اختیارات ویژه root مجاز باشد، غیرممکن است فردی را که وارد سامانه شده است شناسایی کرد.	
	۲-۱	راهنمای عملی	به وسیله مشاهده ACLهای سامانه وارسی کنیدکه آیا کاربران با اختیارات ویژه دارای شناسه کاربری علاوه بر شناسه اختیارات ویژه هستند.
		شواهد مفروض	• فهرست کنترل دسترسی
		روش	بررسی/مشاهده

	۲-۲		راهنمای عملی وارسی کنید که اختیارات ویژه از شناسه متفاوتی نسبت به شناسه معمول کسب‌وکار استفاده می‌کند. درمورد یونیکس یا لینوکس، وارسی کنید که پیکربندی سامانه مانع ورود به سامانه به وسیله root می‌شود. **یادآوری**- ممیزان بازنگری کنترل امنیت اطلاعات باید برای وارسی اختیارات ویژه با استفاده از شناسه‌های مختلف کاربران برای استفاده از کسب‌وکار عادی هنگام ورود مصاحبه کنند که نشان می‌دهد که اختیارات ویژه تنها از شناسه اختیارات ویژه استفاده می‌کند.
		شواهد مفروض	• فایل واقعه‌نگاری • پیکربندی سامانه ورود بر اساس root
		روش	بررسی/مشاهده

الف-۴ وارسی فنی کنترل پشتیبان‌گیری	
کنترل	**بند ۱۰-۵-۱ ISO/IEC ۲۷۰۰۲ پشتیبان‌گیری اطلاعات** نسخه‌های پشتیبان اطلاعات و نرم‌افزار باید تهیه شده و به طور منظم مطابق با خط‌مشی پشتیبان‌گیری توافق شده مورد آزمون قرار گیرد.
اطلاعات فنی اضافی درباره کنترل	برای تهیه پشتیبان مناسب، استاندارد سازمان باید مطابق با خط‌مشی پشتیبان تعریف شده و باید در مستند طراحی پشتیبان منعکس شده باشد. پشتیبان‌ها برای بازیابی اطلاعات ضروری یا نرم‌افزار در هنگام وقوع از دست دادن داده‌ها مانند یک حادثه یا نقص در رسانه‌ها استفاده می‌شوند. هنگامی که از طرح سازمان پشتیبان تهیه می‌شود، سایت‌های پشتیبان، مسیر پشتیبان و روش پشتیبان‌گیری باید مطابق با خط‌مشی انتخاب شده سازمان باشد. در مورد مکان پشتیبان، سازمان باید محلی بر روی سایت یا خارج از سایت را انتخاب کند. پشتیبان در سایت بسیار سریع‌تر از پشتیبان خارج از سایت در نظر گرفته می‌شود. پشتیبان خارج از سایت اغلب به منظور جلوگیری از اثرات حوادث در محل از قبیل آتش سوزی، سیل یا زلزله در نظر گرفته می‌شود. در مورد مسیر پشتیبان، آنلاین یا آفلاین باید انتخاب شود. پشتیبان آنلاین به این

			معناست که داده ها به وسیله شبکه یا خط ارتباطی پشتیبان‌گیری می‌شوند. پشتیبان گیری آفلاین بدان معنی است که داده‌های مورد حفاظت، به صورت فیزیکی به وسیله رسانه‌های برداشتنی[1] مانند DLTs یا سی دی/ دی وی دی انتقال پیدا می‌کنند. روش پشتیبان‌گیری به طبقه بندی گزینه‌های مختلف از جمله پشتیبان کامل، پشتیبان افزایشی و پشتیبان تفاضلی اتلاق می‌گردد. پشتیبان کامل به معنای پشتیبان‌گیری از تمام داده‌های انتخاب شده می‌باشد. نسبت به روش‌های دیگر به زمان بیشتر و ظرفیت داده بیشتری نیاز دارد، اما ساده‌ترین روش برای پشتیبان‌گیری است. پشتیبان افزایشی به این معنی است پشتیبان از آخرین تغییرات تهیه می‌شود. نیازمند زمان کمتر و ظرفیت داده کمتر است اما پیچیده‌ترین روش برای بازگرداندن اطلاعات است. پشتیبان تفاضلی به معنی پشتیبان‌گیری از داده هایی است که از زمان آخرین پشتیبان گیری به طور کامل تغییر کرده است. نیاز به زمان و ظرفیت داده کمتری نسبت به پشتیبان کامل داشته و نسبت به پشتیبان افزایشی روش ساده‌تر و آسان‌تری برای بازگرداندن اطلاعات محسوب می‌شود.
۱	استاندارد پیاده‌سازی امنیت		وسعت (به عنوان مثال پشتیبان کامل یا تفاضلی) و دفعات پشتیبان‌گیری باید منعکس کننده الزامات کسب‌وکار سازمان، الزامات امنیتی اطلاعات مربوطه، و اهمیت برای ادامه عملیات سازمان باشد.
	نکات فنی مربوط به استانداردهای پیاده‌سازی امنیت		مطابق با الزامات کسب‌وکار، سازمان باید زمان و ظرفیت داده‌ای مناسب را برای پشتیبان گیری و بازیابی انتخاب کند. ارزیاب‌ها باید ارزیابی کنند که روش پشتیبان‌گیری برای رسیدن به نیازهای کسب‌وکار انتخاب شده، مناسب می‌باشد. نمونه‌هایی از تناوب تهیه پشتیبان عبارتند از: • همانندسازی[2] یا تکثیر به هنگام (زمانی که اهمیت اطلاعات در بالاترین سطح است) • روزانه (هنگامی که بازسازی داده‌ها حداقل یکبار در روز مورد نیاز است)؛ • هفتگی • ماهانه
	۱-۱	راهنمای عملی	وارسی کنید که پشتیبان‌گیری بر اساس استاندارد پیاده‌سازی امنیت طراحی شده باشد.

1- Removable
2- Mirroring

		شواهد مفروض	مستند مشخصات پشتیبان‌گیری مستند تعریف کسب‌وکار و الزامات امنیتی مستند طراحی تنظیمات پشتیبان‌گیری
		روش	بررسی/بازنگری
	۲-۱	راهنمای عملی	وارسی کنید فایل‌های پیکربندی سامانه پشتیبان‌گیری در مستند طراحی پشتیبان‌گیری شرح داده شده باشد.
		شواهد مفروض	• مستند مشخصات پشتیبان‌گیری • مستند تعریف کسب‌وکار و الزامات امنیتی • مستند طراحی تنظیمات پشتیبان‌گیری
		روش	بررسی/بازنگری
	۳-۱	راهنمای عملی	وارسی کنید پشتیبان‌گیری همانطور که در مستند طراحی پشتیبان‌گیری شرح داده شده است انجام گیرد.
		شواهد مفروض	• مستند طراحی پشتیبان • فایل‌های واقعه‌نگاری • رسانه پشتیبان‌گیری
		روش	بررسی/مشاهده
۲	استاندارد پیاده‌سازی امنیت	روش اجرایی بازیابی باید به طور منظم وارسی و آزمون شده تا اطمینان حاصل شود که موثر بوده و می‌توان آن‌ها را در زمان اختصاص داده شده در روش‌های عملیاتی برای بهبود تکمیل کرد.	
	نکات فنی مربوط به استاندارد پیاده‌سازی امنیت	پیچیدگی و مدت زمان لازم برای بازیابی به روش صورت گرفته، مانند پشتیبان کامل یا تفاضلی با یکدیگر متفاوت هستند. طرح آزمون و وارسی روش اجرایی بازیابی باید آماده شده و مستند باشد.	
	۱-۲	راهنمای عملی	وارسی کنید طرح وارسی مرتبا وارسی شود.
		شواهد مفروض	• سوابق وارسی طرح آزمون و وارسی
		روش	بررسی/بازنگری

	۲-۲	راهنمای عملی	وارسی کنید طرح آزمون و وارسی مرتبا برای اطمینان از اثر بخش بودن و تکمیل شدن در زمان اختصاص داده شده در روش های اجرایی عملیاتی بازیابی بازدید شده باشند.
		شواهد مفروض	• سوابق بازنگری آزمون بازیابی • طرح آزمون و وارسی
		روش	بررسی/بازنگری

الف-۵ وارسی فنی کنترل مدیریت امنیت شبکه		
کنترل		**بند ۱۰-۶-۲ ISO/IEC ۲۷۰۰۲ امنیت خدمات شبکه** ویژگی‌های امنیتی، سطح خدمات و الزامات مدیریت خدمات شبکه‌ای همگی باید شناسایی شده و در توافقنامه خدمات شبکه گنجانده شود صرف نظر از اینکه این خدمات در سازمان انجام شده یا برون سپاری شده باشند.
اطلاعات فنی اضافی درباره کنترل		خدمت شبکه، خدمتی است که در محیط محاسبات شبکه‌ای در سازمان یا خارج از آن ارائه شده است. وقتی که یک سازمان از خدمات شبکه استفاده می‌کند، اطلاعات محرمانه سازمان ممکن است در مسیر برون سپاری خدمات شبکه منتقل شود. بنابراین، یا باید کارکردهای امنیتی لازم مانند رمزگذاری را در نظر گرفت و/یا تأیید اعتبار به وسیله ارائه دهنده خدمات شبکه برون سپاری شده ارائه شود. نمونه ای از سامانه‌های مورد استفاده برای خدمات شبکه عبارتند از: • DNS • DHCP • فایروال (دیوار آتش) / VPN • آشکارساز آنتی ویروس • IPS / IDS
۱	استاندارد پیاده‌سازی امنیت	تمهیدات امنیتی لازم برای ارائه خدمات خاص از قبیل ویژگی‌های امنیتی، سطح خدمات و الزامات مدیریت باید شناخته شده باشد سازمان باید اطمینان حاصل کند که ارائه دهندگان خدمات شبکه این اقدامات را اجرا کنند.
	نکات فنی مربوط به	برای استفاده از خدمات شبکه، تمهیدات امنیتی برای محافظت از اطلاعات در هنگام انتقال مهم است.

	اجـــــــرای اســـــــتاندارد امنیت	الزامات مربوط در مورد ویژگی‌های امنیتی به طور معمول در شرایط کسب‌وکار گنجانـده شده‌اند. نمونه‌هایی از ویژگی‌های مربوط به خدمات شبکه به شرح زیر است. • رمزنگاری در برابر استراق سمع • کنترل دسترسی به شبکه در مقابل دسترسی‌های غیر مجاز • IPS / IDS در برابر فعالیت‌های مخرب، • فیلتر کردن URL در برابر دسترسی به وب غیر مجاز، و • پاسخ به رخداد غیر منتظره برای رویدادهای امنیتی	
	۱-۱	راهنمای عملی	وارسی کنید که مستند قرارداد شامل SLA (توافق سـطح خـدمت) کـه بـه وسـیله ارائـه دهنـده خـدمت فـراهم شـده اسـت الزامـات کسب‌وکار، حقوقی و امنیتی سازمان را برآورده سازد.
		شواهد مفروض	• مستند قرارداد • مستند تعریف نیازمندی‌ها
		روش	بررسی/بازنگری
	۲-۱		راهنمای عملی در مورد داخل سازمانی، وارسی کنید کـه تنظیمـات اسـتفاده شـده برای خدمت شبکه همانطور که در مستند طراحی خـدمت توصـیف شده، باشد.
		شواهد مفروض	• پیکربندی سامانه • مستند طراحی خدمت شبکه
		روش	بررسی/بازنگری
	۳-۱	راهنمای عملی	در مورد داخل سازمانی، وارسی کنید که سـوابق فایـل‌هـای واقعـی واقعه‌نگاری سامانه‌های خـدمت شـبکه همـانطور کـه در مسـتندات طراحی خدمت شبکه توصیف شده، باشد. نمونه ای از سوابق خدمات شبکه: • احراز هویت؛ • رمزنگاری؛ • کنترل‌های ارتباط شبکه؛

			• سرعت مدار؛ • پاسخ (در مورد سامانه آنلاین)؛ • طول مدت خرابی.
		شواهد مفروض	• فایل واقعه‌نگاری • پیام هشدار • مستند طراحی خدمت شبکه
		روش	بررسی/مشاهده

الف-۶ وارسی فنی کنترل مسئولیت‌های کاربر		
کنترل		کاربران باید به دنبال تدابیر امنیتی در انتخاب و استفاده از کلمه عبور باشند.
اطلاعات فنی اضافی درباره کنترل		به منظور جلوگیری از دسترسی غیرمجاز به منابع رایانه، کلمه عبور ایجاد شده و دسترسی به آن‌ها باید مخفی نگه داشته شود. تأیید هویت رمز عبور، روش تأیید هویت کاربر است که به وسیله منابع مختلف از جمله سامانه‌های عامل، برنامه‌ها، پایگاه‌های داده، شبکه‌ها یا وب مورد استفاده قرار گرفته است. کیفیت رمز عبور بستگی به طول و نوع حروف الفبا و علامت‌ها دارد. ممکن است برای کاربران امکان پیکربندی پارامترهای خط‌مشی رمز عبور در برخی از سامانه های عامل مانند ویندوز وجود داشته باشد. از سوی دیگر، توسعه دهندگان برنامه‌های کاربردی ممکن است تابع اعتبار را برای تنظیم خط‌مشی رمز عبور توسعه دهند. ارزیاب‌ها باید ارزیابی کنند که کارکرد مجوز با کلمه عبور در منابع رایانه به طور موثر قرار گرفته و آن دسته از توابع به طور مناسب عمل می‌کنند.
۱	استاندارد پیاده‌سازی امنیت	رمزهای عبور با کیفیت با حداقل طول کافی انتخاب کنید که دارای مشخصات زیر باشد: ۱- به خاطر سپاری آن آسان باشد؛ ۲- بر اساس چیزی که فرد دیگری به راحتی بتواند آن را حدس زده یا با استفاده از اطلاعات شخصی به دست آورد، نباشد. به عنوان مثال نام، شماره تلفن، تاریخ تولد و غیره؛ ۳- نسبت به حملات لغت‌نامه آسیب پذیر نباشد (به عنوان مثال ازکلمات موجود درلغت‌نامه نباشد)؛ ۴- بدون حروف مشابه، فقط عددی یا الفبایی باشد.

	نکات فنی مربوط به استاندارد پیاده‌سازی امنیت	کلمات عبوری که یادآوری آن برای کاربر دیگری آسان باشد به طور کلی آسیب پذیر هستند.	
	۱-۱	راهنمای عملی	وارسی کنید که قانون انتخاب کلمه عبور در خط‌مشی کلمه عبور سازمان شرح داده شده باشد.
		شواهد مفروض	• خط‌مشی کلمه عبور سازمان
		روش	بررسی/مشاهده
	۲-۱	راهنمای عملی	وارسی کنید که تنظیمات پیکربندی سامانه (خط‌مشی کلمه عبور سامانه) در خط‌مشی کلمه عبور سازمان مشخص شده باشد.
		شواهد مفروض	• پیکربندی سامانه (خط‌مشی کلمه عبور سامانه) • خط‌مشی کلمه عبور سازمان
		روش	بررسی/مشاهده
	۳-۱	راهنمای عملی	وارسی کنید که فایل واقعه‌نگاری نشان دهنده تغییر کلمات عبور به وسیله کاربران باشد.
		شواهد مفروض	• فایل واقعه‌نگاری
		روش	بررسی/مشاهده

پیوست ب

(اطلاعاتی)

جمع آوری اطلاعات اولیه (به غیر از IT)

سرممیز بازنگری کنترل امنیت اطلاعات، برای هر زمینه از امنیت اطلاعات، باید یک ممیز بازنگری کنترل امنیت اطلاعات که دانش و تجربه کافی آن زمینه را دارد، اختصاص دهد.

ممکن است برای همکاران مربوطه پرسش‌هایی ابتدایی، شامل زمینه‌ها و فهرست‌های غیر جامع باشد، که در زیر ارائه شده است.

ب-۱ منابع انسانی و امنیت

الف- آیا کارکنان احساس مسئولیت کرده و/یا نسبت به اقدامات خود پاسخگو هستند؟
ب- آیا دانش امنیت و امنیت اطلاعات، به منظور پاسخ به سوالات، ایجاد انگیزه در کارکنان و ارائه راهنمایی مورد نیاز، در سایت وجود دارد؟
پ- آیا خط‌مشی‌های قابل اجرا و روش‌های اجرایی، واضح و SMART[1] (اختصاصی، قابل سنجش، قابل قبول، واقع گرایانه و وابسته به زمان) هستند؟
ت- آیا کارکنان، مطابق با دانش عملیاتی مورد انتظار استخدام شده‌اند؟
ث- آیا کارکنان، برای رسیدگی و دسترسی[2] به اطلاعات حساس و سامانه‌های حیاتی سازمان، قابل اعتماد هستند؟
ج- آیا کارکنان، به طور موثر، قابل اعتماد هستند؟
چ- میزان این اعتماد چگونه تعریف و سنجش می‌شود؟

ب-۲ خط‌مشی‌ها

الف- سلسله مراتب:
۱- آیا خط‌مشی‌های امنیت اطلاعات، از اهداف کسب‌وکار، و به طور کلی از خط‌مشی‌های امنیتی برگرفته شده‌اند؟

1- Specific, Measurable, Acceptable, Realistic, Time-related
2- Handle

۲- چگونه پیوند با IT، HR و خط‌مشی‌های اکتسابی و غیره، ایجاد شده است؟

ب- جامعیت:

۱- آیا خط‌مشی‌ها در همه قسمت‌های فعالیت‌های کسب‌وکار (منابع انسانی، فیزیکی، IT، فروش، تولید، R & D، مخابرات، و غیره) امنیت اطلاعات را در نظر دارد؟

۲- آیاخط‌مشی‌ها، بر اساس راهبرد طراحی‌شان، تاکتیک و عملیات تکمیل شده‌اند؟

پ- فرمول‌بندی

۱- آیا خط‌مشی‌ها عینا موارد استاندارد ایران به شماره ۲۷۰۰۲: ۱۳۸۷ است، یا اهداف کنترل وکنترل‌هایی متناسب با محتوایی خاص هستند؟

۲- آیا خط‌مشی‌ها، به گونه‌ای نوشته شده‌اند که فرد مسئول، به وضوح، قابل شناسایی باشد؟

۳- هر اقدام پیش بینی شده بر اساس خط‌مشی یا روش اجرا، باید سوالات اساسی چه کسی، چه وقت، چرا، چه، کجا، چگونه را در بر بگیرد:

- اگر فرد مسئول، برای انجام اقدامی تعریف نشده است، چه کسی به مجموعه اهداف دست می‌یابد؟
- اگر زمان معین برای انجام اقدامی تعریف نشده است، آیا اقدام در زمان معین آغاز و به پایان خواهد رسید؟
- اگر هدف یا مقصود اقدامی تعریف نشده است، آیا اقدام به خوبی آگاهی شده و اهمیت آن در نظر گرفته خواهد شد؟
- اگر خود اقدام تعریف نشده است، چگونه ممکن است آن را انجام داد؟
- اگر یک اقدام مواردی چون موضوع، مکان، فرآیند، دارایی اطلاعاتی یا «کنترلی» را که بر آن اثر دارد، تعریف نمی‌کند، چگونه می‌تواند موثر باشد (کجا)؟
- اگر یک اقدام در یک روش اجرایی به وضوح تعریف نشده باشد که کارها چگونه باید انجام شود، چگونه می‌توان آن را به درستی انجام داد (چگونه)؟
- اگر اقدامی، شاخص‌ها و کنترل‌های تایید درستی رسیدن به اهداف را تعریف نمی‌کند، چگونه یک سازمان می‌تواند مطمئن شود که به اهداف خود رسیده یا می‌تواند برسد؟

۴- آیا کنترل‌ها و محیط وارسی در محل برای تعیین اینکه آیا بیانیه‌های خط‌مشی، اجرا، پیاده‌سازی و اهداف محقق شده‌اند، وجود دارد؟

۵- اهداف بیانیه خط‌مشی باید معیارهای SMART را در نظر بگیرند. اگر نه:

- تشخیص اهداف نامشخص آسان نبوده و فرد مسئول برای دستیابی به آن، به طور کلی تعریف نشده است.
- اگر هدف قابل سنجش نباشد، شانس کمی وجود دارد که سازمان توانایی رسیدن یا نرسیدن به آن را بررسی کند.

- اگر هدف برای کارکنانی که باید از عهده‌اش برآیند، به خوبی تبیین نشده و قابل قبول نباشد، شانس زیادی در اشتباه گرفته شدن، دور شدن یا قطع شدن کنترل، وجود خواهد داشت.
- اگر هدف در رابطه با توانایی واقعی سازمان، واقع بینانه نباشد، شانس کمی برای رسیدن به آن وجود خواهد داشت، و
- اگر هدف در ارتباط با زمان (زمانی که باید آن را به دست آورد، زمانی که این اقدام قرار است شروع شود، و غیره) تعریف نشده باشد، احتمال آن زیاد است که هیچ اقدامی انجام نشده و هدف برآورده نگردد.

ب-۳ سازمان

الف- آیا مجموعه‌ای از نقش‌ها و مسئولیت‌های تعریف شده و اختصاص داده شده، که برای رسیدن به اهداف کسب‌وکار لازم و کافی هستند در مفاد خاص و محدودیت در نظر گرفته شده‌اند؟

ب- آیا ارتباط با افراد بیرونی دارای اختیار تعریف شده است؟

پ- آیا مسئولیت‌های امنیتی در صورتی که سازمان توانایی داخلی نداشته باشد، برون سپاری شده‌اند؟

ت- آیا به امنیت اطلاعات در قرارداد اشاره شده است؟

ب-۴ امنیت فیزیکی و امنیت محیطی

ب-۴-۱ آیا اماکن برای اطلاعات امن هستند؟

الف- مناطق

۱-آیا نواحی عمومی از فضاهای مرتبط با کسب‌وکار جدا شده‌اند؟
۲- آیا مناطقی تعریف شده که در آن اطلاعات مهم‌تری که به کار گرفته می‌شود (توسط افراد یا سامانه ICT) مدیریت شوند؟
۳- آیا این «مناطق امن» برای جلوگیری از تبادل اطلاعات تفکیک شده‌اند؟

ب- محل‌ها

۱- آیا مناطق مختلف به وضوح مشخص شده و در جای مناسب واقع شده‌اند؟
۲- آیا «مرزها» (دیوار، سقف، کف و غیره) به وضوح تعریف شده و استحکام آن‌ها برای حفاظت از دارایی‌های در بر گرفته شده، مناسب است؟
۳- آیا محل‌های مهم به درستی برای از دسترس خارج ساختن افراد خارجی نشان‌گذاری شده‌اند؟

پ- درگاه‌ها[1] - نقاط دسترسی

۱- آیا درها و پنجره‌ها و نقاط ارتباطی در مرزها در زمان باز بودن مشابه زمان بسته بودن حفاظت می‌شوند؟
۲- آیا کنترل دسترسی مناسب در محل ورود و خروج مکان‌ها وجود دارد؟
۳- آیا یک سامانه ضد نفوذ وجود دارد؟
۴- آیا خروجی‌های اضطراری وجود دارد که به انتقال کافی اطلاعات، افراد و تجهیزات کمک کند؟

ت- راهروها و مسیرها

۱- آیا مسیرها به مناطق و محل‌ها شناسایی شده‌اند؟

- مسیر برای افراد
- کابل‌ها (مسیر برای کسب اطلاعات)

۲- آیا راه‌های جایگزین وجود دارد؟
۳- آیا این راه‌ها حفاظت و نظارت شده هستند؟

ث- پایش

۱- آیا ابزار پایش می‌توانند بدون دیده شدن پایش را انجام دهند؟
۲- آیا ابزار پایش می‌توانند نفوذ از راه دور را تشخیص دهند؟
۳- چه زمانی پایش فعال است؟
۴- کجا و چگونه سوابق نگهداری و تحلیل می‌شوند؟

ج- وسایل

۱- مناسب برای ذخیره اطلاعات هستند؟
۲- به درستی قرار داده شده‌اند؟
۳- همانطور که انتظار می‌رود عمل می‌کنند؟

ب-۴-۲ آیا مکان‌ها برای ICT امن هستند؟

الف- تدارک توان

1- Gates

۱- کافی/مناسب
۲- جایگزین؟
ب- تدارک تهویه هوا
۱- کافی/مناسب
۲- جایگزین؟
پ- تدارک مبارزه با آتش سوزی
۱- کافی/مناسب
۲- جایگزین؟

ب-۴-۳ آیا اماکن برای افراد امن هستند؟

۱- آیا خروجی‌های اضطراری وجود دارد (و با کنترل‌های مناسب)؟
۲- آیا نشتی‌ها (منبع تغذیه، آب، گاز، سیالات) یک خطر بالقوه برای افراد محسوب می‌شوند؟
۳- آیا دما، رطوبت، مواد[1] و لرزش‌ها خطر بالقوه برای افراد محسوب می‌شوند؟
۴- آیا تجهیزات قرار داده شده نمی‌تواند برای افراد آسیب پذیر باشد؟
۵- آیا درگاه‌های نصب و راه‌اندازی شده به گونه‌ای است که نتواند برای افراد ایجاد آسیب کند؟
۶- آیا وسایل نصب و نگهداری شده به گونه‌ای است که نتواند برای افراد ایجاد آسیب کند؟

ب-۵ مدیریت رویداد

الف- آیا رخدادهای امنیت اطلاعات تعریف شده‌اند؟
ب- آیا ظرفیت و توانمندی پاسخ دادن به رخدادهای امنیت اطلاعات ایجاد شده است؟
۱- راهنماها؟
۲- نقش‌ها و مسئولیت‌ها؟
۳- ابزار و منابع

1- Stuff

کتاب‌نامه

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

[۲] استاندارد ملی ایران به شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستمهای مدیریت امنیت اطلاعات – آیین کار مدیریت امنیت اطلاعات

[3] ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management

[4] ISO/IEC 27006:2007, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[5] ISO/IEC 27007:2011, Information technology — Security techniques — Guidelines for information security management systems auditing

[6] ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

[7] ISO Guide 73:2009, Risk management — Vocabulary

[8] NIST Special publication (SP) 800-53A, Guide for reviewing the controls in federal information systems , July 2008. Available from: http://csrc.nist.gov/publications/PubsSPs.html

[9] Institute For Security And Open Methodologies, Open-Source Security Testing Methodology Manual . Available from: http://www.isecom.org/osstmm/

[10] Federal Office for Information Security (BSI), Germany, Standard 100-1, Information Security Management Systems (ISMS); 100-2, IT-Grundschutz Methodology; 100-3, Risk Analysis based on IT-Grundschutz and IT-Grundschutz Catalogues (available in German and English). Available from : https://www.bsi.bund.de/cln_174/EN/Publications/publications_node.html

[11] Information Security Forum, The Standard of Good Practice for Information Security, 2007. Available from: https://www.securityforum.org/services/publicresearch/