INSO-ISO-IEC
27017
1st.Edition
2017

Identical with
ISO/IEC
27017:2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران
ایزو- آی ای سی
۲۷۰۱۷
چاپ اول
۱۳۹۶

فناوری اطلاعات-
فنون امنیتی- آیین کار برای واپایش(کنترل)های امنیت اطلاعات براساس استاندارد ISO/IEC27002 برای خدمات ابری

Information technology — Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ICS: 03.100.70; 35.030

استاندارد ملی ایران شماره ایران-ایزو-آی ایی سی ۲۷۰۱۷ : سال ۱۳۹۶

سازمان ملی استاندارد ایران

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

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

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

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

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

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

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri .gov.ir

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف درکمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح، بررسی و درصورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که براساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

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

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به‌منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمانها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان استاندارد ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را براساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و درصورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International organization for Standardization
2- International Electro technical Commission
3- International Organization for Legal Metrology (Organization International de Metrology Legal)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی- آیین کار برای واپایش‌های امنیت اطلاعات براساس استاندارد ISO/IEC27002 برای خدمات ابری»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات- سیستم‌های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون مدیر کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
عباسپور، مقصود (دکتری مهندسی کامپیوتر- معماری)	دانشیار– معاون مرکز فناوری دانشگاه شهید بهشتی
ناظمی، اسلام (دکتری مهندسی کامپیوتر)	دانشیار- دانشگاه شهید بهشتی
نصیری آسایش، حمیدرضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی

ویراستار:

رضایی، رامین

(کارشناسی مهندسی الکترونیک)

سمت و/ یا محل اشتغال:

معاون طرح و توسعه - مرکز تحقیقات صنایع انفورماتیک

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار ل
مقدمه م
۱ هدف و دامنه کاربرد ۱
۲ مراجع الزامی ۱
۳ اصطلاحات، تعاریف و کوته‌نوشت‌ها ۲
۴ مفاهیم بخش خاص ابر ۳
۴-۱ مرور کلی ۳
۴-۲ روابط تأمین‌کننده در خدمات ابری ۴
۴-۳ روابط بین مشتریان خدمت ابری و ارائه‌کنندگان خدمت ابری ۵
۴-۴ مدیریت مخاطرات امنیت اطلاعات در خدمات ابری ۵
۴-۵ ساختار این استاندارد ۶
۵ خط‌مشی‌های امنیت اطلاعات ۷
۵-۱ جهت‌گیری مدیریت برای امنیت اطلاعات ۷
۵-۱-۱ خط‌مشی‌های امنیت اطلاعات ۷
۵-۱-۲ بازنگری خط‌مشی‌های امنیت اطلاعات ۸
۶ سازمان امنیت اطلاعات ۸
۶-۱ سازمان داخلی ۸
۶-۱-۱ نقش‌ها و مسئولیت‌های امنیت اطلاعات ۸
۶-۱-۲ تفکیک وظایف ۹
۶-۱-۳ برقراری ارتباط با مراجع دارای اختیار ۱۰
۶-۱-۴ برقراری ارتباط با گروه‌های دارای علاقه‌مندی‌های خاص ۱۰
۶-۱-۵ امنیت اطلاعات در مدیریت پروژه ۱۰
۶-۲ افزاره‌های سیار و دورکاری ۱۰
۶-۲-۱ خط‌مشی افزاره سیار ۱۰
۶-۲-۲ دورکاری ۱۱
۷ امنیت منابع انسانی ۱۱
۷-۱ پیش از اشتغال ۱۱
۷-۱-۱ گزینش ۱۱
۷-۱-۲ ضوابط و شرایط اشتغال ۱۱
۷-۲ در زمان اشتغال ۱۱

عنوان **صفحه**

۷-۲-۱ مسئولیت‌های مدیریت ۱۱
۷-۲-۲ آگاه‌سازی، تحصیل و آموزش امنیت اطلاعات ۱۱
۷-۲-۳ فرایند انضباطی ۱۲
۷-۳ خاتمه و تغییر شغل ۱۲
۷-۳-۱ مسئولیت‌های خاتمه یا تغییر اشتغال ۱۲
۸ مدیریت دارایی ۱۲
۸-۱ مسئولیت دارایی‌ها ۱۲
۸-۱-۱ فهرست اموال ۱۲
۸-۱-۲ مالکیت دارایی‌ها ۱۳
۸-۱-۳ استفاده پسندیده از دارایی‌ها ۱۳
۸-۱-۴ بازگرداندن دارایی‌ها ۱۳
۸-۲ طبقه‌بندی اطلاعات ۱۳
۸-۲-۱ طبقه‌بندی اطلاعات ۱۴
۸-۲-۲ علامت‌گذاری اطلاعات ۱۴
۸-۲-۳ اداره کردن دارایی‌ها ۱۴
۸-۳ اداره کردن رسانه‌های ذخیره‌سازی ۱۴
۸-۳-۱ مدیریت رسانه‌های ذخیره‌سازی قابل جابه‌جایی ۱۴
۸-۳-۲ امحای رسانه‌های ذخیره‌سازی ۱۴
۸-۳-۳ انتقال رسانه‌های ذخیره‌سازی فیزیکی ۱۵
۹ واپایش دسترسی ۱۵
۹-۱ الزامات کسب‌وکار واپایش دسترسی ۱۵
۹-۱-۱ خط‌مشی واپایش دسترسی ۱۵
۹-۱-۲ دسترسی به شبکه و خدمات شبکه ۱۵
۹-۲ مدیریت دسترسی کاربر ۱۵
۹-۲-۱ ثبت و حذف کاربر ۱۵
۹-۲-۲ قوانین دسترسی کاربر ۱۶
۹-۲-۳ مدیریت حقوق دسترسی ویژه ۱۶
۹-۲-۴ مدیریت اطلاعات محرمانه اصالت‌سنجی کاربران ۱۷
۹-۲-۵ بازنگری حقوق دسترسی کاربر ۱۷
۹-۲-۶ حذف یا تنظیم حقوق دسترسی ۱۷
۹-۳ مسئولیت‌های کاربر ۱۷

عنوان **صفحه**

۹-۳-۱ استفاده از اطلاعات اصالت‌سنجی ۱۷
۹-۴ واپایش دسترسی به برنامه‌های کاربردی و سامانه‌ها ۱۸
۹-۴-۱ محدودسازی دسترسی به اطلاعات ۱۸
۹-۴-۲ روش‌های اجرایی ورود امن ۱۸
۹-۴-۳ سامانه مدیریت کلمات عبور ۱۸
۹-۴-۴ استفاده از برنامه‌های کمکی ویژه ۱۸
۹-۴-۵ واپایش دسترسی به کد منبع برنامه ۱۹
۱۰ رمزنگاری **Error! Bookmark not defined.**
۱۰-۱ واپایش‌های رمزنگاشتی ۱۹
۱۰-۱-۱ خط‌مشی استفاده از واپایش‌های رمزنگاشتی ۱۹
۱۰-۱-۲ مدیریت کلید ۲۰
۱۱ امنیت فیزیکی و محیطی ۲۰
۱۱-۱ نواحی امن ۲۰
۱۱-۱-۱ حصار امنیت فیزیکی ۲۱
۱۱-۱-۲ واپایش‌های ورودی فیزیکی ۲۱
۱۱-۱-۳ امن‌سازی دفاتر، اتاق‌ها و تسهیلات ۲۱
۱۱-۱-۴ محافظت در برابر تهدیدهای بیرونی و محیطی ۲۱
۱۱-۱-۵ کار در نواحی امن ۲۱
۱۱-۱-۶ نواحی تحویل و بارگیری ۲۱
۱۱-۲ تجهیزات ۲۱
۱۱-۲-۱ استقرار و حفاظت تجهیزات ۲۱
۱۱-۲-۲ ابزارهای پشتیبانی ۲۲
۱۱-۲-۳ امنیت کابل‌کشی ۲۲
۱۱-۲-۴ نگهداری تجهیزات ۲۲
۱۱-۲-۵ خروج دارایی ۲۲
۱۱-۲-۶ امنیت تجهیزات خارج از محوطه ۲۲
۱۱-۲-۷ امحاء یا استفاده مجدد از تجهیزات به‌صورت امن ۲۲
۱۱-۲-۸ تجهیزات بدون مراقبت کاربر ۲۳
۱۱-۲-۹ خط‌مشی میز پاک و صفحه پاک ۲۳
۱۲ امنیت عملیات ۲۳
۱۲-۱ مسئولیت‌ها و روش‌های اجرایی عملیاتی ۲۳

عنوان **صفحه**

۱۲-۱-۱ روش‌های اجرایی عملیاتی مدون ۲۳
۱۲-۱-۲ مدیریت تغییر ۲۳
۱۲-۱-۳ مدیریت ظرفیت ۲۴
۱۲-۱-۴ جداسازی محیط توسعه، آزمون و عملیاتی ۲۵
۱۲-۲ حفاظت در برابر بدافزار ۲۵
۱۲-۲-۱ واپایش‌هایی در برابر بدافزار ۲۵
۱۲-۳ نسخ پشتیبان ۲۵
۱۲-۳-۱ ایجاد پشتیبان از اطلاعات ۲۵
۱۲-۴ واقعه‌نگاری و پایش ۲۶
۱۲-۴-۱ واقعه‌نگاری رویداد ۲۶
۱۲-۴-۲ حفاظت از اطلاعات ثبت‌شده وقایع ۲۷
۱۲-۴-۳ ثبت وقایع سرپرست سامانه و بهره‌بردار ۲۷
۱۲-۴-۴ همزمان‌سازی ساعت‌ها ۲۷
۱۲-۵ واپایش نرم‌افزارهای عملیاتی ۲۸
۱۲-۵-۱ نصب نرم‌افزار بر سامانه‌های عملیاتی ۲۸
۱۲-۶ مدیریت آسیب‌پذیری فنی ۲۸
۱۲-۶-۱ مدیریت آسیب‌پذیری‌های فنی ۲۸
۱۲-۶-۲ محدودسازی در نصب نرم‌افزار ۲۸
۱۲-۷ ملاحظات ممیزی سامانه‌های اطلاعاتی ۲۸
۱۲-۷-۱ واپایش‌های ممیزی سامانه‌های اطلاعاتی ۲۹
۱۳ امنیت ارتباطات ۲۹
۱۳-۱ مدیریت امنیت شبکه ۲۹
۱۳-۱-۱ واپایش‌های شبکه ۲۹
۱۳-۱-۲ امنیت خدمات شبکه ۲۹
۱۳-۱-۳ تفکیک در شبکه‌ها ۲۹
۱۳-۲ انتقال اطلاعات ۳۰
۱۳-۲-۱ خط‌مشی‌ها و روش‌های اجرایی انتقال اطلاعات ۳۰
۱۳-۲-۲ توافقنامه‌های انتقال اطلاعات ۳۰
۱۳-۲-۳ پیام‌رسانی الکترونیکی ۳۰
۱۳-۲-۴ توافقنامه‌های محرمانگی یا عدم افشاء ۳۰
۱۴ اکتساب، توسعه و نگهداری سامانه ۳۰

عنوان **صفحه**

۱۴-۱ الزامات امنیتی سامانه‌های اطلاعاتی ۳۰
۱۴-۱-۱ تحلیل و تعیین الزامات امنیت اطلاعات ۳۰
۱۴-۱-۲ امن‌سازی خدمات کاربردی در شبکه‌های همگانی ۳۱
۱۴-۱-۳ محافظت از تراکنش‌های خدمات کاربردی ۳۱
۱۴-۲ امنیت در فرایندهای توسعه و پشتیبانی ۳۱
۱۴-۲-۱ خط‌مشی توسعه امن ۳۱
۱۴-۲-۲ روش‌های اجرایی واپایش تغییر سامانه ۳۱
۱۴-۲-۳ بازنگری فنی نرم‌افزارهای کاربردی پس از تغییرات بسترهای نرم‌افزاری ۳۲
۱۴-۲-۴ محدودسازی در اعمال تغییرات در بسته‌های نرم‌افزاری ۳۲
۱۴-۲-۵ اصول مهندسی نرم‌افزار امن ۳۲
۱۴-۲-۶ محیط توسعه امن ۳۲
۱۴-۲-۷ توسعهٔ برون‌سپاری شده ۳۲
۱۴-۲-۸ آزمون سامانه امنیت ۳۲
۱۴-۲-۹ آزمون پذیرش سامانه ۳۲
۱۴-۳ داده آزمون ۳۳
۱۴-۳-۱ حفاظت از داده آزمون ۳۳
۱۵ روابط تأمین‌کننده ۳۳
۱۵-۱ امنیت اطلاعات در روابط با تأمین‌کننده ۳۳
۱۵-۱-۱ خط‌مشی امنیت اطلاعات برای ارتباط با تأمین‌کنندگان ۳۳
۱۵-۱-۲ پرداختن به امنیت درون توافقنامه‌های تأمین‌کننده ۳۳
۱۵-۱-۳ زنجیره تأمین فناوری ارتباطات و اطلاعات ۳۴
۱۵-۲ مدیریت تحویل خدمت تأمین‌کننده ۳۴
۱۵-۲-۱ پایش و بازنگری خدمات تأمین‌کننده ۳۴
۱۵-۲-۲ مدیریت تغییرات در خدمات تأمین‌کننده ۳۵
۱۶ مدیریت رخداد امنیت اطلاعات ۳۵
۱۶-۱ مدیریت رخدادهای امنیت اطلاعات و بهبودها ۳۵
۱۶-۱-۱ مسئولیت‌ها و روش‌های اجرایی ۳۵
۱۶-۱-۲ گزارش‌دهی رویدادهای امنیت اطلاعات ۳۵
۱۶-۱-۳ گزارش‌دهی ضعف‌های امنیتی ۳۶
۱۶-۱-۴ برآورد و تصمیم برای رویدادهای امنیت اطلاعات ۳۶
۱۶-۱-۵ پاسخ به رویداد امنیت اطلاعات ۳۶

عنوان	صفحه
۱۶-۱-۶ یادگیری از رویدادهای امنیت اطلاعات	۳۶
۱۶-۱-۷ گردآوری شواهد	۳۷
۱۷ جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار	۳۷
۱۷-۱ تداوم امنیت اطلاعات	۳۷
۱۷-۱-۱ طرح‌ریزی تداوم امنیت اطلاعات	۳۷
۱۷-۱-۲ پیاده‌سازی تداوم امنیت اطلاعات	۳۷
۱۷-۱-۳ بررسی، بازنگری و ارزیابی تداوم امنیت اطلاعات	۳۷
۱۷-۲ افزونگی‌ها	۳۷
۱۷-۲-۱ دسترس‌پذیری تسهیلات پردازش اطلاعات	۳۸
۱۸ انطباق	۳۸
۱۸-۱ انطباق با الزامات قانونی و قراردادی	۳۸
۱۸-۱-۱ شناسایی الزامات قانونی و قراردادی قابل‌اجرا	۳۹
۱۸-۱-۲ حقوق دارایی فکری	۳۹
۱۸-۱-۳ حفاظت از سوابق	۳۹
۱۸-۱-۴ حریم خصوصی و حفاظت از اطلاعات شخصی قابل‌شناسایی	۳۹
۱۸-۱-۵ قواعد واپایش‌های رمزنگاشتی	۴۰
۱۸-۲ بازنگری‌های امنیت اطلاعات	۴۰
۱۸-۲-۱ بازنگری مستقل امنیت اطلاعات	۴۰
۱۸-۲-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی	۴۰
۱۸-۲-۳ بازنگری انطباق فنی	۴۱
پیوست الف (الزامی) مجموعه تعمیم‌یافته واپایش خدمات ابری	۴۲
پیوست ب (آگاهی‌دهنده) مراجع مخاطره امنیت اطلاعات مربوط به رایانش ابری	۴۸
کتاب‌نامه	۵۰

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- آیین کار برای واپایش‌های امنیت اطلاعات براساس استاندارد ISO/IEC27002 برای خدمات ابری» که پیش‌نویس آن در کمیسیون‌های مربـوط بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره شده دربارهٔ الف، بند ۷، استاندارد ملی شماره ۵ تهیه و تدوین شده، در چهارصد و نود و ششمین اجلاسیه کمیته ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۶/۰۲/۰۹ تصویب شد. اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می شود.

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

این استاندارد ملی برمبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است.

ISO/IEC 27017: 2015, Information technology — Security techniques– Code of practice for information security controls based on ISO/IEC 27002 for cloud services

مقدمه

راهنماهایی که در این استاندارد آورده شده است، افزون و کامل‌کنندهٔ راهنماهای بیان شده در استاندارد ISO/IEC 27002 است. به ویژه، این استاندارد راهنماهایی برای پشتیبانی از پیاده‌سازی واپایش‌های امنیت اطلاعات برای مشتریان خدمت ابری و ارائه‌کنندگان خدمت ابری فراهم می‌کند. برخی راهنماها برای مشتریان خدمت ابری است که واپایش‌ها را پیاده‌سازی می‌کنند و دیگر راهنماها برای ارائه‌کنندگان خدمات ابری است که پیاده‌سازیِ آن واپایش‌ها را پشتیبانی می‌کنند. انتخاب واپایش‌های مناسب امنیت اطلاعات و کاربرد راهنمای پیاده‌سازی ارائه شده، به ارزیابی مخاطره[1] و هر نوع الزامات امنیت اطلاعات قانونی، قراردادی و مقرراتی یا دیگر الزامات امنیت اطلاعات بخش خاص صنایع ابر، بستگی خواهد داشت.

1 - Risk Assessment

فناوری اطلاعات- فنون امنیتی- آیین کار برای واپایش‌های امنیت اطلاعات براساس استاندارد ISO/IEC27002 برای خدمات ابری

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و ارائه راهنماهایی برای واپایش‌های کاربردپذیر امنیت اطلاعات در تدارک و استفاده از خدمات ابری است که از طریق ارائه موارد زیر است:

- راهنمای افزوده پیاده‌سازی برای واپایش‌های مرتبط مشخص شده در استاندارد ISO/IEC 27002؛
- واپایش‌های افزوده با راهنمای پیاده‌سازی که به ویژه در ارتباط با خدمات ابری است.

این استاندارد واپایش‌ها و راهنمای پیاده‌سازی را برای ارائه‌کنندگان خدمت ابری و همچنین مشتریان خدمت ابری فراهم می‌کند.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آنها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. دربارهٔ مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

2-1 Recommendation ITU-T Y.3500 (in force) | ISO/IEC 17788: (in force), Information technology – Cloud computing – Overview and vocabulary

2-2 Recommendation ITU-T Y.3502 (in force) | ISO/IEC 17789: (in force), Information technology – Cloud computing – Reference architecture

2-3 ISO/IEC 27000: (in force), Information technology – Security techniques – Information security management systems – Overview and vocabulary

یادآوری- استاندارد ملی ایران با شماره INSO-ISO-IEC ۲۷۰۰۰ در سال ۱۳۹۴ با استفاده از استاندارد ISO/IEC 27000:2014 تدوین شده است.

2-4 ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

یادآوری- استاندارد ملی ایران با شماره INSO-ISO-IEC ۲۷۰۰۲ در سال ۱۳۹۴ با استفاده از استاندارد ISO/IEC 27002:2013+Cor1:2014 تدوین شده است.

۳ اصطلاحات، تعاریف و کوته‌نوشت‌ها

۳-۱ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در استانداردهای ISO/IEC 27000، Rec. ITU-T Y.3500 | ISO/IEC 17788 و Rec. ITU-T Y.3502 | ISO/IEC 17789، اصطلاحات و تعاریف زیر نیز به‌کار می‌روند:

۳-۱-۱

توانمندی

capability

کیفیتِ توانمندی انجام فعالیت معین است.

[منبع: استاندارد ISO 19440]

۳-۱-۲

۳-۱-۲-۱

نقض داده

data breach

نقض امنیت که به‌صورت تصادفی یا غیرقانونی منجر به تخریب، از دست رفتن، تحریف، افشا یا دسترسی غیرمجاز به داده‌های محافظت‌شده‌ای می‌شود که انتقال می‌یابند، ذخیره می‌شوند یا پردازش می‌شوند.

[منبع: استاندارد ISO/IEC 27040]

۳-۱-۲-۱

چند اجاره‌ای امن

secure multi-tenancy

نوعی از چند اجاره‌ای که واپایش‌های امنیتی را به‌کار می‌گیرد تا به صورت صریح در برابر نقض داده حفاظت کند و اعتبارسنجیِ این واپایش‌ها را به منظور حاکمیت مناسب فراهم می‌کند.

[منبع: استاندارد ISO/IEC 27040]

یادآوری ۱- چند اجاره‌ای امن، هنگامی پدید می‌آید که رخ‌نمون مخاطره مستأجر منفرد، بیشتر از مخاطره‌ای که به محیط تک مستأجری اختصاص دارد، نباشد.

یادآوری ۲- در محیط‌های خیلی امن، حتی هویت مستأجران را مخفی نگاه می‌دارند.

۳-۱-۳

ماشین مجازی

virtual machine

محیط کاملی که از اجرای نرم‌افزار میهمان پشتیبانی می‌کند.

[منبع: استاندارد ISO/IEC 17203]

یادآوری- ماشین مجازی، پوشینه‌دارسازی[1] کاملی از سخت‌افزار مجازی، لوح‌های مجازی و فراداده مربوط به آن است. ماشین‌های مجازی، تسهیم ماشین فیزیکی زیرین را از طریق لایه نرم‌افزاری به نام اَبر-ناظر[2] ممکن می‌سازد.

۳-۲ کوته‌نوشت‌ها

خدمات اَبری زیرساخت (خاز)	Infrastructure as a Service	IaaS
خدمات اَبری بُن‌سازه (خاب)	Platform as a Service	PaaS
اطلاعات قابل‌شناسایی شخصی	Personally Identifiable Information	PII
خدمات اَبری نرم‌افزار (خانا)	Software as a Service	SaaS
توافقنامه سطح خدمت	Service Level Agreement	SLA
ماشین مجازی	Virtual Machine	VM

۴ مفاهیم بخش خاص ابر

۴-۱ مرور کلی

استفاده از رایانش ابری نحوه ارزیابی و کاهش مخاطرات امنیت اطلاعات را تغییر داده است، به دلیل این‌که تغییرات چشمگیری در چگونگی طراحی، عملیات و حاکمیت منابع رایانش به وجود آورده است. این استاندارد راهنمای افزوده پیاده‌سازی خاص ابر را بر اساس استاندارد ISO/IEC 27002 و واپایش‌های افزوده برای پرداختن به مخاطرات و تهدیدهای امنیت اطلاعات خاص ابر را ارائه می‌کند.

توصیه می‌شود کاربران این استاندارد برای دستیابی به واپایش‌ها، راهنماهای پیاده‌سازی و اطلاعات دیگر به

1 - Encapsulation
2 - Hypervisor

بندهای ۵ تا ۱۸ از استاندارد ISO/IEC 27002 مراجعه کنند. به دلیل کاربردپذیری عمومی استاندارد ISO/IEC 27002، بسیاری از واپایش‌ها، راهنمای پیاده‌سازی و اطلاعات دیگر در هر دو زمینه عمومی و رایانش ابری در سازمان به‌کار می‌روند. به‌عنوان مثال بند «۶-۱-۲ تفکیک وظایف» در استاندارد ISO/IEC 27002 واپایشی را ارائه می‌کند که می‌تواند در سازمانی که به‌عنوان ارائه‌کننده خدمات ابری عمل می‌کند یا نمی‌کند، به‌کار رود. به‌علاوه، مشتری خدمت ابری می‌تواند الزاماتی را برای تفکیک وظایف در محیط ابری از واپایش مشابه استخراج کند. به‌عنوان مثال، تفکیک مشتریان خدمت ابر، سرپرستان خدمات ابری[1] و کاربران خدمات ابری.

در این استاندارد، به‌عنوان تعمیم برای استاندارد ISO/IEC 27002، واپایش‌های مشخص خدمات ابری، راهنمای پیاده‌سازی و اطلاعات دیگر (به بند ۴-۵ مراجعه شود) به منظور کاهش مخاطرات ارائه می‌شود که با ویژگی‌های فنی و عملیاتی خدمات ابری همراه است (به پیوست ب مراجعه شود). مشتری خدمت ابری و ارائه‌کنندگان خدمات ابری می‌توانند به استاندارد ISO/IEC 27002 و این استاندارد مراجعه کنند تا واپایش-هایی با راهنمای پیاده‌سازی انتخاب کرده، در صورت لزوم، واپایش‌های دیگری را اضافه کنند. این فرایند می‌تواند به‌وسیله اجرای ارزیابی مخاطره امنیت اطلاعات و رفع مخاطرات در زمینه کسب‌وکار و سازمانی انجام شود که خدمات ابری استفاده یا تأمین می‌شوند (به بند ۴-۴ مراجعه شود).

۴-۲ روابط تأمین‌کننده در خدمات ابری

استاندارد ISO/IEC 27002 بند ۱۵ «روابط تأمین‌کنندگان» واپایش‌ها، راهنمای پیاده‌سازی و اطلاعات دیگر دربارهٔ مدیریت امنیت اطلاعات در روابط تأمین‌کنندگان را ارائه می‌کند. تدارک و استفاده از خدمات ابری نوعی رابطه تأمین‌کننده است که مشتری خدمت ابری به‌عنوان متقاضی و ارائه‌کننده خدمت ابری به‌عنوان تأمین‌کننده هستند. بنابراین بند ۱۵ دربارهٔ مشتریان خدمت ابری و ارائه‌کنندگان خدمت ابری به‌کار می‌رود.

همچنین مشتریان خدمت ابری و ارائه‌کنندگان خدمت ابری می‌توانند زنجیره تأمین را تشکیل دهند. فرض کنید ارائه‌کننده خدمت ابری خدمات نوع توانمندی‌های زیرساخت را فراهم کند. به‌علاوه، ارائه‌کننده خدمت ابری دیگر می‌تواند خدمات نوع توانمندی‌های برنامه کاربردی را تأمین کند. در این مورد با توجه به ارائه‌کننده خدمت ابری اول، دومین ارائه‌کننده، مشتری خدمت ابری است و تأمین‌کننده خدمت ابری نیز به‌عنوان مشتری خدمت ابری، از خدمات او استفاده می‌کند. این مثال موردی را نشان می‌دهد که این استاندارد در سازمان، به‌عنوان هم مشتری خدمت ابری و هم ارائه‌کننده خدمت ابری به‌کار می‌رود. بند ۱۵-۱-۳ «زنجیره تأمین فناوری ارتباطات و اطلاعات» در استاندارد ISO/IEC 27002 به دلیل اینکه مشتری خدمت ابری و ارائه‌کننده خدمت ابری زنجیره تأمین را از طریق طراحی و پیاده‌سازی خدمات ابری تشکیل می‌دهند، به‌کار می‌رود.

استاندارد چند قسمتیِ ISO/IEC 27036، «امنیت اطلاعات برای روابط با تامین کننده» در رابطه با امنیت اطلاعات در روابط تأمین‌کننده با متقاضی و تأمین‌کننده محصولات و خدمات، راهنمایی با جزئیات ارائه می-

1 - Cloud service administrators

کند.

استاندارد ISO/IEC 27036-4 به طور مستقیم با امنیت خدمات ابری در روابط تأمین‌کننده سروکار دارد. همچنین این استاندارد دربارهٔ مشتری خدمت ابری به‌عنوان متقاضی و ارائه‌کننده خدمت ابری به‌عنوان تأمین‌کننده کاربردپذیر است.

۴-۳ روابط بین مشتریان خدمت ابری و ارائه‌کنندگان خدمت ابر

در محیط رایانش ابری، داده‌های مشتری خدمت ابری به وسیله خدمت ابری ذخیره، منتقل و پردازش می‌شوند. بنابراین فرایندهای کسب‌وکار مشتری خدمت ابری می‌تواند به امنیت اطلاعات خدمات ابری بستگی داشته باشد. در صورت عدم واپایش مناسب روی خدمات ابری، ممکن است مشتری خدمت ابری نیاز به احتیاط بیشتری در کارهای امنیت اطلاعات خود داشته باشد.

مشتری خدمت ابری قبل از ورود به رابطه تأمین‌کننده نیاز دارد خدمات ابری را انتخاب کرده و شکاف‌های ممکن بین الزامات امنیت اطلاعات مشتری خدمات ابری و توانمندی‌های امنیت اطلاعات پیشنهاد شده از سوی خدمات را در نظر گیرد. هرگاه خدمات ابری انتخاب شد، توصیه می‌شود مشتری خدمت ابری، استفاده از خدمات ابری را به گونه‌ای مدیریت کند که الزامات امنیت اطلاعات برآورده شود. در این رابطه، توصیه می-شود ارائه‌کننده خدمت ابری، اطلاعات و پشتیبانی فنی را که برای برآورده کردن الزامات امنیت اطلاعات مشتری خدمت ابری مورد نیاز است، فراهم کند. هرگاه واپایش‌های امنیت اطلاعات فراهم شده توسط ارائه‌کننده خدمت ابری از پیش تعیین شده باشد و نتواند توسط مشتری خدمت ابری تغییر کند، ممکن است مشتری خدمت ابری نیاز به پیاده‌سازی واپایش‌های افزوده برای کاهش مخاطرات آن داشته باشد.

۴-۴ مدیریت مخاطرات امنیت اطلاعات در خدمات ابری

توصیه می‌شود مشتری خدمت ابری و ارائه‌کننده خدمت ابری، دارای فرایندهای مدیریت مخاطره امنیت اطلاعات باشند. به آن‌ها توصیه می‌شود برای الزاماتِ هدایت مدیریت مخاطره در سامانه‌های مدیریت امنیت اطلاعات خود به استاندارد ISO/IEC 27005[1] مراجعه کنند. استاندارد ISO 31000[2] که منطبق بر استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 27005 است هم می‌تواند به درک عمومی از مدیریت مخاطره کمک کند.

رایانش ابری در مقایسه با کاربردپذیری عمومی فرایندهای مدیریت مخاطره امنیت اطلاعات، انواعِ منابع مخاطرهٔ خود را دارد. این منابع مخاطره شامل تهدیدها و آسیب‌پذیری‌ها است که از ویژگی‌های خود مشتق می‌شود: ویژگی‌هایی مانند شبکه‌سازی، مقیاس‌پذیری و توانمندی ارتجاعی سامانه، به اشتراک‌گذاری منبع، تدارک خود خدماتی، اداره کردن بر مبنای تقاضا، تدارک خدمات قضایی متقابل و بینش محدود نسبت به

۱- استاندارد ملی ایران با شماره INSO-ISO/IEC ۲۷۰۰۵ در سال ۱۳۹۲ با استفاده از استاندارد ISO/IEC 27005:2011 تدوین شده است.

۲ - استاندارد ملی ایران به شماره ۱۳۲۴۵: سال ۱۳۸۹ با استفاده از استاندارد ISO 31000:2009 تدوین شده است.

پیاده‌سازی واپایش‌ها. پیوست (ب) مراجعی را مطرح می‌کند که اطلاعاتی دربارهٔ این منابع مخاطره و مخاطرات مرتبط با تدارک و استفاده از خدمات ابری را ارائه می‌کنند.

واپایش‌ها و راهنماهای پیاده‌سازی داده شده در بندهای ۵ تا ۱۸ و پیوست (الف) از این استاندارد به منابع مخاطره و مخاطرات خاص رایانش ابری می‌پردازد.

۵-۴ ساختار این استاندارد

این استاندارد در قالبی مشابه با استاندارد ISO/IEC 27002 ساختاربندی شده است. این استاندارد بندهای ۵ تا ۱۸ از استاندارد ISO/IEC 27002 را از طریق بیان کاربردپذیری‌های متن‌هایش در هر بند و پاراگراف شامل می‌شود.

هرگاه اهداف و واپایش‌های مشخص شده در استاندارد ISO/IEC 27002 بدون نیاز به اطلاعات مازاد کاربرد-پذیر باشند، تنها یک اشاره به استاندارد ISO/IEC 27002 صورت می‌گیرد.

هرگاه هدف به همراه واپایش‌ها یا واپایشِ تحت یک هدف از استاندارد ISO/IEC 27002 علاوه بر آن‌هایی که در استاندارد ISO/IEC 27002 هستند مورد نیاز باشد، در پیوست الزامی (الف) آورده شده است: مجموعه تعمیم‌یافته واپایش خدمات ابری. هرگاه واپایش از استاندارد ISO/IEC 27002 یا پیوست (الف) از این استاندارد، به راهنماهای افزون پیاده‌سازی مشخص خدمات ابری در ارتباط با آن واپایش نیاز داشته باشد، تحت عنوان «**راهنمای پیاده‌سازی برای خدمات ابری**» آورده می‌شود. راهنما در یکی از دو نوع زیر ارائه می‌شود:

نوع ۱ زمانی استفاده می‌شود که راهنمای مجزا برای مشتری خدمت ابری و ارائه‌کننده خدمت ابری وجود دارد.

نوع ۲ زمانی استفاده می‌شود که راهنما برای هم مشتری خدمت ابری و هم ارائه‌کننده خدمت ابری یکسان است.

نوع ۱

مشتری خدمت ابری	ارائه‌کننده خدمت ابری

نوع ۲

مشتری خدمت ابری	ارائه‌کننده خدمت ابری

اطلاعات افزوده که ممکن است مد نظر قرار گیرد، تحت عنوان «**اطلاعات دیگر برای خدمات ابری**» آورده می‌شود.

۵ خط‌مشی‌های امنیت اطلاعات

۵-۱ جهت‌گیری مدیریت برای امنیت اطلاعات

هدف مشخص شده در بند ۵-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۵-۱-۱ خط‌مشی‌های امنیت اطلاعات

واپایش بند ۵-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود خط‌مشی امنیت اطلاعات برای رایانش ابری به‌عنوان خط‌مشی موضوع خاص مشتری خدمت ابری تعریف شود. توصیه می‌شود خط‌مشی امنیت اطلاعات مشتری خدمت ابری برای رایانش ابری با سطوح قابل قبول مخاطرات امنیت اطلاعات برای اطلاعات و دیگر دارایی‌هایش سازگار باشد. در هنگام تعریف خط‌مشی امنیت اطلاعات برای رایانش ابری، توصیه می‌شود مشتری خدمت ابری موارد زیر را در نظر گیرد: - اطلاعات ذخیره شده در محیط رایانش ابری می‌تواند موضوع دسترسی و مدیریت به‌وسیله ارائه‌کننده خدمت ابری باشد؛ - دارایی‌ها می‌تواند در محیط رایانش ابری نگه‌داری شود، مثلاً برنامه‌های کاربردی؛ - فرایندها می‌توانند در خدمت ابریِ چند اجاره‌ای و مجازی‌شده اجرا شوند؛ - کاربران خدمات ابری و زمینه‌ای که از خدمات ابری استفاده می‌کنند؛ - اداره‌کنندگان خدمات ابریِ مشتری خدمت ابری که امتیاز خاص دسترسی دارند؛ - مکان جغرافیایی سازمان‌ها و کشورهای ارائه‌کننده خدمت ابری که ارائه‌کننده خدمت ابری می‌تواند داده مشتری خدمت ابری را در آن ذخیره کند (حتی به‌طور موقت).	توصیه می‌شود ارائه‌کننده خدمات ابری خط‌مشی امنیت اطلاعات خود را برای پرداختن به تدارک و استفاده از خدمات ابری خود تقویت کند و موارد زیر را در نظر گیرد: - الزامات مبنا و کاربردپذیر امنیت اطلاعات در طراحی و پیاده‌سازی خدمات ابری؛ - مخاطرات ناشی از کارمندان مجاز داخلی؛ - جداسازی مشتری خدمت ابری و چنداجاره‌ای (شامل مجازی‌سازی)؛ - دسترسی به دارایی‌های مشتری خدمت ابری توسط کارکنان ارائه‌کننده خدمت ابری؛ - روش‌های اجرایی واپایش دسترسی، مثلاً، اصالت-سنجی قوی برای دسترسی راهبرانه به خدمات ابری؛ - ارتباطات با مشتری خدمت ابری در طی تغییر مدیریت؛ - امنیت مجازی‌سازی؛ - دسترسی و حفاظت از داده مشتری خدمت ابری؛ - مدیریت چرخه عمر حساب‌های مشتری خدمت ابری؛ - ابلاغ نقض‌ها و راهنماهای اشتراک اطلاعات برای کمک به تحقیقات و مسائل قانونی؛

اطلاعات دیگر برای خدمات ابری

خط‌مشی امنیت اطلاعات مشتری خدمت ابری برای رایانش ابری یکی از خط‌مشی‌های موضوع خاص تشریح شده در بند ۵-۱-۱ استاندارد ISO/IEC 27002 است. خط‌مشی امنیت اطلاعات سازمان با اطلاعات و فرایندهای کسب‌وکار آن سروکار دارد. هرگاه سازمانی از خدمات ابری استفاده کند، می‌تواند خط‌مشی برای رایانش ابری به‌عنوان مشتری خدمت ابری داشته باشد. خدمات سازمان می‌تواند در محیط خدمات ابری نگهداری و ذخیره شود و فرایندهای کسب و کار می‌توانند در محیط خدمات ابری عمل کنند. الزامات عمومی امنیت اطلاعات بیان شده در خط‌مشی امنیت اطلاعات در سطح بالا توسط خط‌مشی رایانش ابری دنبال می‌شود.

در طرف مقابل، خط‌مشی امنیت اطلاعات برای تأمین خدمات ابری با اطلاعات مشتری خدمت ابری و فرایندهای کسب و کار سروکار دارد و با اطلاعات ارائه‌کننده خدمت ابری و فرایندهای کسب و کار آن سروکار ندارد. توصیه می‌شود الزامات امنیت اطلاعات برای تدارک خدمات ابری، مشتریان خدمت ابری در آینده را برآورده کند. در نتیجه، ممکن است آن الزامات با الزامات امنیت اطلاعات و فرایندهای کسب و کار ارائه‌کننده خدمت ابری سازگار نباشند. حوزه خط‌مشی امنیت اطلاعات اغلب به صورت خدمات تعریف می‌شود اما تنها از طریق ساختار سازمانی یا مکان‌های فیزیکی تعریف نمی‌شود.

چندین جنبه امنیت مجازی‌سازی برای رایانش ابری، شامل مدیریت چرخه عمر نمونه‌های مجازی، ذخیره‌سازی و دسترسی به واپایش‌ها برای تصاویر مجازی، راه‌اندازی نمونه‌های مجازی برون‌خط[1]، تصویر لحظه‌ای، محافظت از اَبر-ناظرها و واپایش‌های امنیت حاکم بر استفاده از درگاه‌های خویش‌یار[2].

۵-۱-۲ بازنگری خط‌مشی‌های امنیت اطلاعات

واپایش ۵-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC27002 به‌کار می‌روند.

۶ سازمان امنیت اطلاعات

۶-۱ سازمان داخلی

هدف مشخص شده در بند ۶-۱ از استاندارد ISO/IEC27002 به‌کار می‌رود.

۶-۱-۱ نقش‌ها و مسئولیت‌های امنیت اطلاعات

واپایش ۶-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

1 - Offline virtual instances
2 - Self-service portals

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری با ارائه‌کننده خدمت ابری دربارهٔ تخصیص مناسب مسئولیت‌ها و نقش‌های امنیت اطلاعات توافق کرده و تأیید کند که می‌تواند نقش‌ها و مسئولیت‌های تخصیص داده شده را برآورده کند.توصیه می‌شود مسئولیت‌ها و نقش‌های امنیت اطلاعات هر دو طرف در توافق‌نامه بیان شود. توصیه می‌شود مشتری خدمت ابری رابطه خود با پشتیبانی مشتری را شناسایی و مدیریت کند و مراقب عملیات ارائه‌کننده خدمت ابری باشد.	توصیه می‌شود ارائه‌کننده خدمت ابری دربارهٔ تخصیص مناسب نقش‌ها و مسئولیت‌های امنیت اطلاعات با مشتریان خدمت ابری، ارائه‌کنندگان خدمت ابری و تامین‌کنندگان خود توافق کرده و آن‌ها را مستند (مکتوب) کند.

اطلاعات دیگر برای خدمات ابری

حتی زمانی‌که مسئولیت‌ها درون و بین طرفین تعیین می‌شود، مشتری خدمت ابری برای تصمیم‌گیری برای استفاده از خدمات مسئول است. توصیه می‌شود این تصمیم‌گیری مطابق با نقش‌ها و مسئولیت‌های معین شده درون سازمان مشتری خدمت ابری باشد. ارائه‌کننده خدمت ابری برای امنیت اطلاعات بیان شده به‌عنوان بخشی از توافق خدمات ابری مسئول است. توصیه می‌شود پیاده‌سازی و تدارک امنیت اطلاعات مطابق با نقش‌ها و مسئولیت‌های معین شده درون سازمان ارائه‌کننده خدمت ابری باشد.

ابهام در نقش‌ها و تعاریف و تخصیص مسئولیت‌های مربوط به مواردی مثل مالکیت داده، واپایش دسترسی و نگهداری زیرساخت در کسب و کار یا مشاجره‌ها، به خصوص هنگام سرو کار داشتن با طرف سوم[1]، می‌تواند افزایش یابد.

داده و پرونده‌ها روی سامانه‌های ارائه‌کننده خدمت ابری که در طی استفاده از خدمات ابری ایجاد یا اصلاح می‌شود، می‌تواند در عملیات امن، بازیابی و تداوم خدمات، بحرانی باشد. توصیه می‌شود مالکیت تمام دارایی‌ها و طرف‌هایی که برای عملیات مرتبط با این دارایی‌ها مثل پشتیبانی و بهبود عملیات دارای مسئولیت هستند، تعریف و مستند شوند. در غیر این صورت مخاطره‌ای که وجود دارد این است که ارائه‌کننده خدمت ابری فرض می‌کند مشتری خدمت ابری این وظایف حیاتی را اجرا می‌کند (یا برعکس) و در نتیجه داده ممکن است از دست برود.

۶-۱-۲ تفکیک وظایف

واپایش بند ۶-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC27002 به کار می‌روند.

1 - Third party

۶-۱-۳ برقراری ارتباط با مراجع دارای اختیار

واپایش بند ۶-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اختیارات مرتبط با عملیات ترکیبیِ مشتری خدمت ابری و ارائه‌کننده خدمت ابری را شناسایی کند.	توصیه می‌شود ارائه‌کننده خدمات ابری، مشتری خدمت ابری را از مکان‌های جغرافیایی سازمان ارائه‌کننده خدمات ابری و کشورهایی که ارائه‌کننده خدمات ابری می‌تواند داده‌های مشتری خدمت ابری را ذخیره کند، آگاه سازد.

اطلاعات دیگر برای خدمات ابری

اطلاعات دربارهٔ مکان‌های جغرافیایی که داده مشتری خدمت ابری می‌تواند ذخیره، پردازش یا انتقال داده شود، می‌تواند به مشتری خدمت ابری در تعیین اختیارات و حوزه‌های قضایی[1] کمک کند.

۶-۱-۴ برقراری ارتباط با گروه‌های دارای علاقه‌مندی‌های خاص

واپایش بند ۶-۱-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۶-۱-۵ امنیت اطلاعات در مدیریت پروژه

واپایش بند ۶-۱-۵ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۶-۲ افزاره‌های سیار و دورکاری[2]

هدف مشخص شده در بند ۶-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۶-۲-۱ خط‌مشی افزاره سیار[3]

واپایش بند ۶-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

1 - Jurisdictions
2 - Teleworking
3 - Mobile device policy

۶-۲-۲ دورکاری

واپایش بند ۶-۲-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۷ امنیت منابع انسانی

۷-۱ پیش از اشتغال

هدف مشخص شده در بند ۷-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۷-۱-۱ گزینش

واپایش بند ۷-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۷-۱-۲ ضوابط و شرایط اشتغال

واپایش بند ۷-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۷-۲ در زمان اشتغال

هدف مشخص شده در بند ۷-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۷-۲-۱ مسئولیت‌های مدیریت

واپایش بند ۷-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۷-۲-۲ آگاه‌سازی، تحصیل و آموزش امنیت اطلاعات

واپایش بند ۷-۲-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری موارد زیر را به برنامه آگاه‌سازی، تحصیل و آموزش برای مدیران خدمات ابری کسب و کار، خدمات ابری اداری، یکپارچه‌سازان خدمات ابری و کاربران خدمات ابری شامل کارمندان و پیمانکاران مرتبط اضافه کند:	توصیه می‌شود ارائه‌کننده خدمت ابری در ارتباط با ادارهٔ مناسب داده مشتری خدمت ابری و داده مشتق‌شده خدمت ابری، آگاه‌سازی، تحصیل و آموزش برای

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
- استانداردها و روش‌های اجرایی برای استفاده از خدمات ابری - مخاطرات امنیت اطلاعات مرتبط با خدمات ابری و چگونگی مدیریت این مخاطرات - مخاطرات محیط شبکه و سامانه با استفاده از خدمات ابری - ملاحظات مقرراتی و قانونی[1] کاربردپذیر توصیه می‌شود برنامه‌های آگاه‌سازی، تحصیل و آموزش امنیت اطلاعات دربارهٔ خدمات ابری به مدیریت و مدیران ناظر شامل واحدهای کسب و کار ارائه شوند. این تلاش‌ها از فعالیت‌های هماهنگ و مؤثر امنیت اطلاعات پشتیبانی می‌کند.	کارمندان فراهم آورد و از پیمانکاران بخواهد همان کار را انجام دهند. این داده می‌تواند حاوی اطلاعات محرمانه مشتری خدمت ابری باشد یا موضوع محدودیت‌های مشخص شامل محدودیت‌های مقرراتی در دسترسی و استفاده توسط ارائه‌کننده خدمت ابری باشد.

۷-۲-۳ فرایند انضباطی

واپایش بند ۷-۲-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۷-۳ خاتمه و تغییر شغل

هدف مشخص شده در بند ۷-۳ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۷-۳-۱ مسئولیت‌های خاتمه یا تغییر اشتغال

واپایش بند ۷-۳-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۸ مدیریت دارایی

۸-۱ مسئولیت دارایی‌ها

هدف مشخص شده در بند ۸-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۸-۱-۱ فهرست اموال

واپایش بند ۸-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

1 - Legal

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود فهرست دارایی‌های مشتری خدمت ابری برای اطلاعات و دارایی‌های ذخیره شده مرتبط با آن در محیط رایانش ابری در نظر گرفته شود. توصیه می‌شود سوابق فهرست نشان دهند دارایی‌ها کجا نگهداری می‌شوند، مثلاً شناسایی خدمات ابری.	توصیه می‌شود فهرست دارایی‌های ارائه‌کننده خدمت ابری به طور صریح شناسایی شود. - داده مشتری خدمت ابری - داده مشتق شده خدمات ابری

اطلاعات دیگر برای خدمات ابری

برنامه‌های کاربردی خدمات ابری وجود دارد که کارکردهایی را برای مدیریت اطلاعات به وسیله افزودن داده مشتق شده خدمات ابری به داده مشتری خدمت ابری تأمین می‌کند. شناسایی این چنین داده‌های مشتق شده خدمات ابری به‌عنوان دارایی و نگهداری آن‌ها در فهرست دارایی‌ها می‌تواند به بهبود امنیت اطلاعات کمک کند.

۸-۱-۲ مالکیت دارایی‌ها

واپایش بند ۸-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

اطلاعات دیگر برای خدمات ابری

مالکیت دارایی‌ها احتمالاً بسته به طبقه‌بندی خدمات ابری استفاده شده متفاوت خواهد بود. هنگام استفاده از خدمات اَبری بُن‌سازه (خاب) یا خدمات اَبری زیرساخت (خاز)، نرم‌افزار کاربردی متعلق به مشتری خدمت ابری خواهد بود، در حالی که اگر از خدمات اَبری نرم‌افزار (خانا) استفاده کند، نرم‌افزار کاربردی متعلق به ارائه‌کننده خدمت ابری خواهد بود.

۸-۱-۳ استفاده پسندیده از دارایی‌ها

واپایش بند ۸-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به کار می‌روند.

۸-۱-۴ بازگرداندن دارایی‌ها

واپایش بند ۸-۱-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۸-۲ طبقه‌بندی اطلاعات

هدف مشخص شده در بند ۸-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۸-۲-۱ طبقه‌بندی اطلاعات

واپایش بند ۸-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۸-۲-۲ علامت‌گذاری اطلاعات

واپایش بند ۸-۲-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اطلاعات و دارایی‌های نگهداری شده در محیط رایانش ابری را مطابق با روش‌های اجرایی اتخاذ شده مشتری خدمت ابری برای علامت‌گذاری، علامت گذاری کنند. درصورت کاربردپذیر بودن، کارکرد تأمین شده به‌وسیله ارائه‌کننده خدمت ابری که از علامت‌گذاری پشتیبانی می‌کند، می‌تواند اتخاذ شود.	توصیه می‌شود ارائه‌کننده خدمت ابری هر کارکرد خدمت را که به مشتری خدمت ابری اجازه می‌دهد اطلاعات خود و دارایی‌های مرتبط با آن را طبقه‌بندی و علامت‌گذاری کند، مستند و آشکار کند.

۸-۲-۳ اداره کردن دارایی‌ها

واپایش بند ۸-۲-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۸-۳ اداره کردن رسانه‌های ذخیره‌سازی[1]

هدف مشخص شده در بند ۸-۳ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۸-۳-۱ مدیریت رسانه‌های ذخیره‌سازی قابل جابه‌جایی

واپایش بند ۸-۳-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۸-۳-۲ امحای رسانه‌های ذخیره‌سازی

واپایش بند ۸-۳-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

1 - Media handling

۸-۳-۳ انتقال رسانه‌های ذخیره‌سازی فیزیکی

واپایش بند ۸-۳-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۹ واپایش دسترسی

۹-۱ الزامات کسب‌وکار واپایش دسترسی

هدف مشخص شده در بند ۹-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۹-۱-۱ خط‌مشی واپایش دسترسی

واپایش بند ۹-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۹-۱-۲ دسترسی به شبکه و خدمات شبکه

واپایش بند ۹-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود خط‌مشی واپایش دسترسی مشتری خدمت ابری برای استفاده از خدمات شبکه، الزامات دسترسی کاربر به هر خدمات ابری جدا که استفاده شده‌اند را مشخص کند.	(هیچ‌گونه راهنمای افزوده پیاده‌سازی وجود ندارد.)

۹-۲ مدیریت دسترسی کاربر

هدف مشخص شده در بند ۹-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۹-۲-۱ ثبت و حذف کاربر

واپایش بند ۹-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
(هیچ‌گونه راهنمای افزوده پیاده‌سازی وجود ندارد.)	توصیه می‌شود برای مدیریت دسترسی به خدمات ابری به‌وسیله کاربران خدمات ابری مشتری خدمت ابر، ارائه‌کننده خدمت ابری کارکردهای ثبت‌نام و حذف نام کاربران و مشخصات استفاده از این کارکردها را برای مشتری خدمت ابری تأمین کند.

۹-۲-۲ قوانین دسترسی کاربر

واپایش بند ۹-۲-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
(هیچ‌گونه راهنمای افزوده پیاده‌سازی وجود ندارد.)	توصیه می‌شود ارائه‌کننده خدمت ابری کارکردهایی برای مدیریت حقوق دسترسی کاربران خدمات ابری مشتری خدمت ابری و مشخصاتی برای استفاده از این کارکردها را تأمین کند.

اطلاعات دیگر برای خدمات ابری

توصیه می‌شود ارائه‌کننده خدمت ابری از هویت طرف سوم و فناوری‌های مدیریت دسترسی برای خدمات ابری خود و واسطهای اداری مرتبط با آن پشتیبانی کند. این فناوری‌ها می‌توانند آسان‌تر یکپارچه شوند و شناسایی کاربر بین سامانه‌های مشتری خدمت ابری و خدمات ابری را مدیریت کنند و می‌توانند استفاده از خدمات ابری چندگانه را آسان‌تر سازند و از این چنین توانمندی‌هایی به‌عنوان امضا قرارداد اشتغال واحد، پشتیبانی کند.

۹-۲-۳ مدیریت حقوق دسترسی ویژه

واپایش بند ۹-۲-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری از فنون اصالت‌سنجی مناسب (مثلاً اصالت‌سنجی چندعاملی) برای اصالت‌سنجی اداره‌کنندگان خدمات ابری مشتری خدمت ابری، برای توانمندی‌های اداری خدمات ابری مطابق با	توصیه می‌شود ارائه‌کننده خدمت ابری فنون اصالت‌سنجی مناسب را برای اصالت‌سنجی اداره‌کنندگان خدمات ابری مشتری خدمت ابری، برای توانمندی-های اداری خدمات ابری مطابق با مخاطرات شناسایی شده تأمین کند. به‌عنوان مثال، ارائه‌کننده خدمت ابری می‌تواند توانمندی‌های اصالت‌سنجی چندعاملی را فراهم کرده یا استفاده از سازوکار اصالت‌سنجی چندعاملی طرف

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
مخاطرات شناسایی شده استفاده کند.	سوم را فعال کند.

۹-۲-۴ مدیریت اطلاعات محرمانه اصالت‌سنجی کاربران

واپایش بند ۹-۲-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری تأیید کند که روش اجرایی مدیریت ارائه‌کننده خدمت ابری برای تخصیص اطلاعات محرمانه اصالت‌سنجی، مثل رمز عبور، الزامات مشتری خدمت ابری را برآورده کرده است.	توصیه می‌شود ارائه‌کننده خدمت ابری اطلاعات روش‌های اجرایی مدیریت اطلاعات محرمانه اصالت‌سنجی مشتری خدمت ابری، شامل روش‌های اجرایی برای تخصیص این اطلاعات و اصالت‌سنجی کاربران را فراهم کند.

اطلاعات دیگر برای خدمات ابری

توصیه می‌شود مشتری خدمت ابری، مدیریت اطلاعات محرمانه اصالت‌سنجی را با استفاده از شناسه خود یا طرف سوم و فناوری‌های مدیریت دسترسی واپایش کند.

۹-۲-۵ بازنگری حقوق دسترسی کاربر

واپایش بند ۹-۲-۵ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۹-۲-۶ حذف یا تنظیم[1] حقوق دسترسی

واپایش بند ۹-۲-۶ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به کار می‌روند.

۹-۳ مسئولیت‌های کاربر

هدف مشخص شده در بند ۹-۳ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۹-۳-۱ استفاده از اطلاعات اصالت‌سنجی

واپایش بند ۹-۳-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

1 - Adjustment

۹-۴ واپایش دسترسی به برنامه‌های کاربردی و سامانه‌ها

هدف مشخص شده در بند ۹-۴ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۹-۴-۱ محدودسازی دسترسی به اطلاعات

واپایش بند ۹-۴-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اطمینان یابد که دسترسی به اطلاعات در خدمات ابری می‌تواند در تطابق با خط‌مشی واپایش دسترسی خود محدود شود و اینکه این محدودیت‌ها درک شده باشند. این موارد شامل محدود کردن دسترسی به خدمات ابری نگهداری شده در خدمات هستند.	توصیه می‌شود ارائه‌کننده خدمت ابری واپایش‌های دسترسی را فراهم کند که به مشتری خدمت ابری اجازه دهد دسترسی به خدمات ابری خود، کارکردهای خدمات ابری خود و داده مشتری خدمت ابری نگهداری شده در خدمات را محدود کند.

اطلاعات دیگر برای خدمات ابری

محیط رایانش ابری شامل محدوده‌های دیگر است که نیاز به واپایش‌های دسترسی دارد. ممکن است دسترسی به کارکردها و خدمات به‌عنوان بخشی از خدمات ابری یا کارکردهای خدمات ابری، مثل کارکرد-های مدیریت اَبرناظر و واپایش‌های اداری، نیاز به واپایش دسترسی افزوده داشته باشند.

۹-۴-۲ روش‌های اجرایی ورود امن

واپایش بند ۹-۴-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۹-۴-۳ سامانه مدیریت کلمات عبور

واپایش بند ۹-۴-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۹-۴-۴ استفاده از برنامه‌های کمکی ویژه

واپایش بند ۹-۴-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای قسمت خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری در جایی که استفاده از برنامه‌های کاربردپذیر مجاز هستند، برنامه کاربردپذیر را برای استفاده در محیط رایانش ابری خود شناسایی کند و اطمینان یابد که با واپایش‌های خدمات ابری تداخل ندارد.	توصیه می‌شود ارائه‌کننده خدمت ابری الزامات هر برنامه سودمند استفاده شده درون خدمات ابری را شناسایی کند. توصیه می‌شود ارائه‌کننده خدمت ابری اطمینان یابد که هرگونه استفاده از برنامه‌های کاربردپذیر که قادر است از بهره‌برداری عادی یا روش‌های اجرایی امنیتی عبور کند، مؤکداً محدود به اصالت‌سنجی افراد شود و اینکه استفاده از این برنامه‌ها به طور منظم بازنگری و ممیزی شوند.

۹-۴-۵ واپایش دسترسی به کد منبع برنامه

واپایش بند ۹-۴-۵ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۰ رمزنگاری

۱۰-۱ واپایش‌های رمزنگاشتی

هدف مشخص شده در بند ۱۰-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۰-۱-۱ خط‌مشی استفاده از واپایش‌های رمزنگاشتی

واپایش بند ۱۰-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای قسمت خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اگر در تحلیل مخاطره توجیه شده باشد، واپایش‌های رمزنگاشتی را برای استفاده خود از خدمات ابری، پیاده کند. توصیه می‌شود واپایش‌ها، قدرت کافی برای کم کردن مخاطرات شناسایی شده داشته باشند، اگرچه این واپایش‌ها توسط مشتری خدمت ابری یا ارائه‌کننده خدمت ابری تهیه شده باشند. توصیه می‌شود هرگاه ارائه‌کننده خدمت ابری رمزنگاری را پیشنهاد می‌کند، مشتری خدمت ابری هرگونه اطلاعات تهیه شده به‌وسیله ارائه‌کننده خدمت ابری را مرور کند تا تأیید کند توانمندی‌های رمزنگاشتی: - الزامات خط‌مشی مشتری خدمت ابری را برآورده می‌سازند؛	توصیه می‌شود ارائه‌کننده خدمت ابری دربارهٔ شرایطی که مطابق آن، برای حفاظت از اطلاعات در حال پردازش از رمزنگاشتی استفاده می‌کند، اطلاعاتی را به مشتری خدمت ابری ارائه کند. همچنین توصیه می‌شود ارائه‌کننده خدمت ابری دربارهٔ هرگونه توانمندی او که بتواند به مشتری خدمت ابری کمک کند تا حفاظت از رمزنگاشتی خود را به‌کار گیرد، اطلاعاتی را به مشتری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
- با هر حفاظت رمزنگاشتی استفاده شده توسط مشتری خدمت ابری سازگار هستند؛ - به داده در انتها و در انتقال از/ به و درون خدمات ابری اعمال می‌شوند.	خدمت ابری ارائه کند.

اطلاعات دیگر برای خدمات ابری

ممکن است در برخی حوزه‌های قضایی نیاز به به‌کارگیری رمزنگاری برای محافظت از انواع خاص اطلاعات مثل داده‌های سلامت، شماره ثبت سکونت، شماره پاسپورت و شماره گواهینامه رانندگی باشد.

۱۰-۱-۲ مدیریت کلید

واپایش بند ۱۰-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری کلیدهای رمزنگاشتی برای هر خدمات ابری و روش‌های اجرایی پیاده‌سازی هر مدیریت کلید را شناسایی کند. هرگاه خدمت ابری، کارکرد مدیریت کلید را برای استفاده توسط مشتری خدمت ابری تأمین کند، توصیه می‌شود مشتری خدمت ابری اطلاعات زیر را در روش‌های اجرایی استفاده شده برای مدیریت کلیدهای مربوط به خدمات ابری درخواست کند: - انواع کلیدها؛ - مشخصات سامانه مدیریت کلید، شامل روش‌های اجرایی برای هر مرحله از چرخه عمر کلید مثل تولید، تغییر یا به‌روزرسانی، ذخیره‌سازی، کناره‌گیری، بازیابی، حفظ و از بین بردن؛ - روش‌های اجرایی مدیریت کلید توصیه شده برای استفاده توسط مشتری خدمت ابری. توصیه می‌شود وقتی مشتری خدمت ابری، مدیریت کلید یا خدمات مدیریت کلید جدا و متمایز خود را به‌کار می‌گیرد، اجازه ذخیره و مدیریت کلیدهای رمزنگاشتی برای عملیات رمزنگاشتی را به ارائه‌کننده خدمت ابری ندهد.	(هیچ‌گونه راهنمای افزوده پیاده‌سازی وجود ندارد.)

۱۱ امنیت فیزیکی و محیطی

۱۱-۱ نواحی امن

هدف مشخص شده در بند ۱۱-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۱-۱-۱ حصار امنیت فیزیکی[1]

واپایش بند ۱۱-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۱-۲ واپایش‌های ورودی فیزیکی

واپایش بند ۱۱-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۱-۳ امن‌سازی دفاتر، اتاق‌ها و تسهیلات[2]

واپایش بند ۱۱-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۱-۴ محافظت در برابر تهدیدهای بیرونی و محیطی

واپایش بند ۱۱-۱-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۱-۵ کار در نواحی امن

واپایش بند ۱۱-۱-۵ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۱-۶ نواحی تحویل و بارگیری

واپایش بند ۱۱-۱-۶ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۲ تجهیزات

هدف مشخص شده در بند ۱۱-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۱-۲-۱ استقرار و حفاظت تجهیزات

واپایش بند ۱۱-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

---

1 - Physical Security Perimeter
2 - Facilities

۱۱-۲-۲ ابزارهای پشتیبانی

واپایش بند ۱۱-۲-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۲-۳ امنیت کابل‌کشی

واپایش بند ۱۱-۲-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به کار می‌روند.

۱۱-۲-۴ نگهداری تجهیزات

واپایش بند ۱۱-۲-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۲-۵ خروج دارایی

واپایش بند ۱۱-۲-۵ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۲-۶ امنیت تجهیزات خارج از محوطه

واپایش بند ۱۱-۲-۶ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۲-۷ امحاء یا استفاده مجدد از تجهیزات به‌صورت امن

واپایش بند ۱۱-۲-۷ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری تأییدیه‌ای درخواست کند که ارائه‌کننده خدمت ابری دارای خط‌مشی‌ها و روش‌های اجرایی برای امحاء یا استفاده مجدد از منابع است.	توصیه می‌شود ارائه‌کننده خدمت ابری اطمینان یابد ترتیباتی به‌وجود می‌آید که امحاء یا استفاده مجدد از منابع مثل (تجهیزات، ذخیره‌سازی داده، پرونده‌ها، حافظه) به موقع انجام شود.

اطلاعات دیگر برای خدمات ابری

اطلاعات افزوده دربارهٔ امحاء امن در استاندارد ISO/IEC 27040 آمده است.

۱۱-۲-۸ تجهیزات بدون مراقبت کاربر

واپایش بند ۱۱-۲-۸ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۱-۲-۹ خط‌مشی میز پاک و صفحه پاک[1]

واپایش بند ۱۱-۲-۹ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۲ امنیت عملیات

۱۲-۱ مسئولیت‌ها و روش‌های اجرایی عملیاتی

هدف مشخص شده در بند ۱۲-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۲-۱-۱ روش‌های اجرایی عملیاتی مدون

واپایش بند ۱۲-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۲-۱-۲ مدیریت تغییر

واپایش بند ۱۲-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به کار می‌روند. راهنمای قسمت خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود فرایند مدیریت مشتری خدمت ابری تأثیر هر تغییر ایجاد شده به‌وسیله ارائه‌کننده خدمت ابری را تخمین بزند.	توصیه می‌شود ارائه‌کننده خدمت ابری اطلاعاتی دربارهٔ تغییرات خدمات ابری که می‌تواند تأثیر منفی روی خدمات ابری داشته باشد را به مشتری خدمت ابری ارائه کند. موارد زیر می‌تواند به مشتری خدمت ابری کمک کند تا تأثیر منفی تغییرات روی امنیت اطلاعات را تعیین کند: - رده‌های تغییرات - زمان و تاریخ طرح‌ریزی شده تغییرات - توصیف‌های فنی تغییرات در خدمات ابری و سامانه‌های زیربنایی - اطلاع‌رسانی شروع و خاتمه تغییرات هرگاه ارائه‌کننده خدمت ابری، خدمات ابری را پیشنهاد دهد که بستگی به ارائه‌کننده خدمت ابری همتا دارد، ممکن است که نیاز باشد ارائه‌کننده خدمت ابری مشتری خدمت ابری را از تغییرات

1 - Clear Desk and Clear Screen Policy

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
	ایجاد شده به وسیله ارائه‌کننده خدمت ابری همتا مطلع کند.

اطلاعات دیگر برای خدمات ابری

فهرست مواردی که توصیه می‌شود در آگاه‌سازی گنجانده شوند، می‌تواند در قرارداد، مثل قرارداد خدمات اصلی یا قرارداد سطح خدمات مشخص شوند.

۱۲-۱-۳ مدیریت ظرفیت

واپایش بند ۱۲-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اطمینان حاصل کند که ظرفیت قراردادی تهیه شده توسط خدمات ابری، الزامات مشتری خدمت ابری را برآورده می‌سازد. توصیه می‌شود مشتری خدمت ابری استفاده از خدمات ابری را پایش کرده و نیازهای ظرفیت آن‌ها را پیش‌بینی کند تا از عملکرد خدمات ابری طی گذشت زمان اطمینان یابد.	توصیه می‌شود ارائه‌کننده خدمت ابری ظرفیت منابع کل را برای جلوگیری از رخدادهای امنیت اطلاعات به دلیل کمبود منابع، پایش کند.

اطلاعات دیگر برای خدمات ابری

خدمات ابری حاوی منابعی هستند که تحت واپایش ارائه‌کننده خدمت ابری قرار دارند و تحت شرایط توافق-نامه اصلی خدمات و SLA مربوط به آن، در دسترس مشتری خدمت ابری هستند. این منابع شامل نرم‌افزار، سخت‌افزار پردازش‌گر، ذخیره‌سازی داده و اتصال شبکه هستند.

عموماً الاستیک بودن، مقیاس‌پذیر بودن و تخصیص منابع بر مبنای تقاضا در خدمات ابری، ظرفیت کل خدمات را افزایش می‌دهد. به هرحال توصیه می‌شود مشتری خدمت ابری آگاه باشد که منابع تأمین‌شده می‌توانند محدودیت ظرفیت داشته باشند. مثال‌هایی از محدودیت ظرفیت شامل تعداد هسته‌های پردازشگر برای برنامه کاربردی، حجم ذخیره در دسترس، یا پهنای باند در دسترس شبکه است.

محدودیت‌ها می‌توانند بسته به خدمات ابری خاص یا اشتراک خاصی که مشتری خدمت ابری می‌خرد، متفاوت باشند. اگر مشتری خدمت ابری الزاماتی داشته باشد که از محدودیت‌ها تجاوز کند، ممکن است مشتری خدمت ابری نیاز به تغییر خدمات ابری یا تغییر اشتراک داشته باشد.

برای اینکه مشتری خدمت ابری مدیریت ظرفیت را برای خدمات ابری اجرا کند، توصیه می‌شود مشتری خدمت ابری به آمار مربوط در استفاده از منابع نظیر موارد زیر دسترسی داشته باشد:

- آمار طول دوره زمانی خاص؛
- بیشینه سطح استفاده از منبع.

۱۲-۱-۴ جداسازی محیط توسعه، آزمون و عملیاتی

واپایش بند ۱۲-۱-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۲-۲ حفاظت در برابر بدافزار

هدف مشخص شده در بند ۱۲-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۲-۲-۱ واپایش‌هایی در برابر بدافزار

واپایش بند ۱۲-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۲-۳ نسخ پشتیبان

هدف مشخص شده در بند ۱۲-۳ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۲-۳-۱ ایجاد پشتیبان از اطلاعات

واپایش بند ۱۲-۳-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود هرگاه ارائه‌کننده خدمت ابری ظرفیت‌های پشتیبان‌گیری را به‌عنوان بخشی از خدمات ابری فراهم کند، مشتری خدمت ابری مشخصات ظرفیت پشتیبان‌گیری را از ارائه‌کننده خدمت ابری در خواست کند. توصیه می‌شود مشتری خدمت ابری تأیید کند که آن‌ها الزامات پشتیبان‌گیری را برآورده کرده‌اند. اگر ارائه‌کننده خدمت ابری آن‌ها را فراهم نکند، مشتری خدمت ابری مسئول	توصیه می‌شود ارائه‌کننده خدمت ابری مشخصات ظرفیت‌های پشتیبانی خود را برای مشتری ابر فراهم کند. توصیه می‌شود مشخصات به صورت مناسبی شامل اطلاعات زیر باشد: - حوزه و زمان‌بندی پشتیبان‌گیری - روش‌ها و قالب داده پشتیبان‌گیری شامل رمزگذاری، اگر مرتبط باشد. - دوره زمانی نگهداری داده‌های پشتیبان‌گیری - روش‌های اجرایی برای تأیید یکپارچگی داده پشتیبان‌گیری - روش‌های اجرایی و مقیاس زمانی شامل شده در بازگرداندن داده از پشتیبان‌گیری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
پیاده‌سازی ظرفیت‌های پشتیبان‌گیری است.	- روش‌های اجرایی آزمودن ظرفیت‌های پشتیبان‌گیری - مکان ذخیره‌سازی پشتیبان‌گیری‌ها توصیه می‌شود ارائه‌کننده خدمت ابری دسترسی امن و تفکیک شده‌ای به پشتیبان‌گیری مثل عکس‌های فوری مجازی فراهم کند، البته اگر این خدمات به مشتری خدمت ابری پیشنهاد شده باشد.

اطلاعات دیگر برای خدمات ابری

تخصیص مسئولیت‌ها برای پشتیبانی‌گیری در محیط رایانش ابری اغلب نامشخص است. دربارهٔ IaaS، عموماً مسئولیت‌های پشتیبان‌گیری با مشتری خدمت ابری است. به هر حال مشتری خدمت ابری ممکن است از مسئولیتش در پشتیبان‌گیری از کل داده مشتری خدمت ابری تولید شده در سامانه رایانش ابری، مثل پرونده‌های قابل اجرای تولید شده توسط استفاده از ظرفیت‌های توسعه خدمات PaaS آگاه نباشد.

یادآوری- ممکن است تغییر سطوح پشتیبان‌گیری و بازیابی به‌عنوان خدمات با هزینه بیشتر پیشنهاد شود، در این مورد مشتری خدمت ابری می‌تواند نوع و زمان پشتیبان‌گیری را انتخاب کند.

۱۲-۴ واقعه‌نگاری[1] و پایش

هدف مشخص شده در بند ۱۲-۴ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۲-۴-۱ واقعه‌نگاری رویداد[2]

واپایش بند ۱۲-۴-۱و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری الزامات خود برای رویداد ثبت را تعریف کرده و تأیید کند که خدمات ابری این الزامات را برآورده می‌کند.	توصیه می‌شود ارائه‌کننده خدمت ابری برای مشتری خدمت ابری ظرفیت‌های ثبت را فراهم کند.

اطلاعات دیگر برای خدمات ابری

مسئولیت مشتری خدمت ابری و ارائه‌کننده خدمت ابری برای رویداد ثبت، بسته به نوع خدمات ابری استفاده شده متفاوت است. به‌عنوان مثال، مسئولیت ثبت ارائه‌کننده خدمت ابری با IaaS می‌تواند محدود به اجزاء زیرساخت رایانش ابری باشد و مشتری خدمت ابری می‌تواند مسئول ثبت رویدادهای برنامه‌های

1 - Logging
2 - Event logging

کاربردی و ماشین‌های مجازی خود باشد.

۱۲-۴-۲ حفاظت از اطلاعات ثبت‌شده وقایع

واپایش بند ۱۲-۴-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۲-۴-۳ ثبت وقایع سرپرست سامانه و بهره‌بردار

واپایش بند ۱۲-۴-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
اگر عملگر ممتاز به مشتری خدمت ابری واگذار شده باشد، توصیه می‌شود عملیات و عملکرد این عملیات ثبت شوند. توصیه می‌شود مشتری خدمت ابری معین کند ظرفیت‌های ثبت تأمین شده توسط ارائه‌کننده خدمت ابری مناسب هستند یا آیا توصیه می‌شود مشتری خدمت ابری ظرفیت‌های ثبت افزوده را پیاده‌سازی کند.	(هیچ‌گونه راهنمای افزوده پیاده‌سازی وجود ندارد.)

اطلاعات دیگر برای خدمات ابری

توصیه می‌شود تقسیم مسئولیت‌ها بین مشتری خدمت ابری و ارائه‌کننده خدمت ابری، عملیات خاص(ممتاز) مربوط به خدمات ابری را پوشش دهد. پایش و ثبت استفاده از عملیات ممتاز، در پشتیبانی از اقدامات پیشگیرانه و اصلاحی در برابر استفاده نادرست از این عملیات ضروری است.

۱۲-۴-۴ همزمان‌سازی ساعت‌ها

واپایش بند ۱۲-۴-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اطلاعاتی دربارهٔ همزمان‌سازی ساعت استفاده شده برای سامانه ارائه‌کننده خدمت ابری را درخواست کند.	توصیه می‌شود ارائه‌کننده خدمت ابری اطلاعاتی دربارهٔ ساعت استفاده شده به‌وسیله سامانه‌های ارائه‌کننده خدمت ابری و اطلاعاتی دربارهٔ چگونگی هماهنگ کردن ساعت‌های محلی مشتری خدمت ابری با ساعت خدمات ابری برای مشتری خدمت ابری را فراهم کند.

اطلاعات دیگر برای خدمات ابری

در نظر گرفتن هماهنگی ساعت سامانه‌های مشتری خدمت ابری با سامانه‌های ارائه‌کننده خدمت ابری که خدمات ابری استفاده شده توسط مشتری خدمت ابری را راه می‌اندازد، ضروری است. بدون وجود چنین هماهنگی، تطبیق رویدادهای سامانه‌های مشتری خدمت ابری با رویدادهای سامانه‌های ارائه‌کننده خدمت ابری دشوار است.

۱۲-۵ واپایش نرم‌افزارهای عملیاتی

هدف مشخص شده در بند ۱۲-۵ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۲-۵-۱ نصب نرم‌افزار روی سامانه‌های عملیاتی

واپایش بند ۱۲-۵-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۲-۶ مدیریت آسیب‌پذیری فنی

هدف مشخص شده در بند ۱۲-۶ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۲-۶-۱ مدیریت آسیب‌پذیری‌های فنی

واپایش بند ۱۲-۶-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اطلاعاتی از ارائه‌کننده خدمت ابری دربارهٔ مدیریت آسیب‌پذیری‌های فنی که روی خدمات تأمین شده ابر تأثیر می‌گذارد را درخواست کند. توصیه می‌شود مشتری خدمت ابری آسیب‌پذیری‌های فنی که باید مدیریت شوند را شناسایی کند و به وضوح فرایند مدیریت آن‌ها را تعریف کند.	توصیه می‌شود ارائه‌کننده خدمت ابری به اطلاعات مشتری خدمت ابری درباره مدیریت آسیب‌پذیری-های فنی که روی خدمات تأمین شده ابر تأثیر می‌گذارد، دسترسی داشته باشد.

۱۲-۶-۲ محدودسازی در نصب نرم‌افزار

واپایش بند ۱۲-۶-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۲-۷ ملاحظات ممیزی سامانه‌های اطلاعاتی

هدف مشخص شده در بند ۱۲-۷ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۲-۷-۱ واپایش‌های ممیزی سامانه‌های اطلاعاتی

واپایش بند ۱۲-۷-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۳ امنیت ارتباطات

۱۳-۱ مدیریت امنیت شبکه

هدف مشخص شده در بند ۱۳-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۳-۱-۱ واپایش‌های شبکه

واپایش بند ۱۳-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۳-۱-۲ امنیت خدمات شبکه

واپایش بند ۱۳-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۳-۱-۳ تفکیک در شبکه‌ها

واپایش بند ۱۳-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری الزامات خود برای تفکیک شبکه‌ها در دستیابی به ایزوله‌سازی مستأجر در محیط به اشتراک گذاشته شده خدمات ابری را تعریف کرده و تأیید کند که ارائه‌کننده خدمت ابری این الزامات را برآورده می‌کند.	توصیه می‌شود ارائه‌کننده خدمت ابری تفکیک دسترسی به شبکه را برای موارد زیر تاکید کند: - تفکیک بین مستأجرین در محیط چنداجاره‌ای - تفکیک بین محیط اداری درونی ارائه‌کننده خدمت ابری و محیط رایانش ابری مشتری خدمت ابری توصیه می‌شود هرکجا مناسب باشد ارائه‌کننده خدمت ابری به مشتری خدمت ابری در تأیید تفکیک پیاده شده به وسیله ارائه‌کننده خدمت ابری کمک کند.

اطلاعات دیگر برای خدمات ابری

ممکن است بنا به قوانین و مقررات نیاز باشد که تفکیک شبکه‌ها یا ایزوله‌سازی ترافیک شبکه‌ها وجود داشته

باشد.

۱۳-۲ انتقال اطلاعات

هدف مشخص شده در بند ۱۳-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۳-۲-۱ خط‌مشی‌ها و روش‌های اجرایی انتقال اطلاعات

واپایش بند ۱۳-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۳-۲-۲ توافقنامه‌های انتقال اطلاعات

واپایش بند ۱۳-۲-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۳-۲-۳ پیام‌رسانی الکترونیکی

واپایش بند ۱۳-۲-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۳-۲-۴ توافقنامه‌های محرمانگی یا عدم افشاء

واپایش بند ۱۳-۲-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴ اکتساب، توسعه و نگهداری سامانه

۱۴-۱ الزامات امنیتی سامانه‌های اطلاعاتی

اهداف مشخص شده در بند ۱۴-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۴-۱-۱ تحلیل و تعیین الزامات امنیت اطلاعات

واپایش بند ۱۴-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای قسمت خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری الزامات امنیت اطلاعات خود را برای خدمات ابری معین کند و سپس ارزیابی کند که آیا سامانه‌های	توصیه می‌شود ارائه‌کننده خدمت ابری اطلاعاتی دربارهٔ ظرفیت‌های امنیت اطلاعاتی که آن‌ها

پیشنهاد شده به‌وسیله ارائه‌کننده خدمت ابری می‌تواند این الزامات را برآورده سازد یا نه. توصیه می‌شود مشتری خدمت ابری برای این ارزیابی، اطلاعاتی دربارهٔ ظرفیت‌های امنیت اطلاعات از ارائه‌کننده خدمات درخواست کند.	استفاده می‌کند را به مشتری خدمت ابری ارائه کند. توصیه می‌شود این اطلاعات آگاهی‌دهنده بوده، بدون افشای اطلاعاتی که بتواند برای کسی با سود قصد، مفید باشد.

اطلاعات دیگر برای خدمات ابری

توصیه می‌شود از افشای محدود جزئیات پیاده‌سازی شده واپایش‌های امنیتی مراقبت شود، زیرا آن‌ها مربوط به خدمات ابری تأمین شده برای مشتری خدمت ابری یا مشتری خدمت ابری بالقوه هستند که دارای توافق عدم افشاء در محل است.

۱۴-۱-۲ امن‌سازی خدمات کاربردی در شبکه‌های همگانی

واپایش بند ۱۴-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴-۱-۳ محافظت از تراکنش‌های خدمات کاربردی

واپایش بند ۱۴-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴-۲ امنیت در فرایندهای توسعه و پشتیبانی

هدف مشخص شده در بند ۱۴-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۴-۲-۱ خط‌مشی توسعه امن

واپایش بند ۱۴-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای قسمت خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اطلاعاتی را از ارائه‌کننده خدمت ابری دربارهٔ استفاده ارائه‌کننده خدمت ابری از عملیات و روش‌های اجرایی توسعه امن درخواست کند.	توصیه می‌شود ارائه‌کننده خدمت ابری اطلاعاتی را دربارهٔ استفاده خود از عملیات و روش‌های اجرایی توسعه امن برای سازگاری بیشتر با خط‌مشی خود در افشا، فراهم کند.

اطلاعات دیگر برای خدمات ابری

عملیات و روش‌های اجرایی امن ارائه‌کننده خدمت ابری، می‌تواند برای SaaS بحرانی باشد.

۱۴-۲-۲ روش‌های اجرایی واپایش تغییر سامانه

واپایش بند ۱۴-۲-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴-۲-۳ بازنگری فنی نرم‌افزارهای کاربردی پس از تغییرات بسترهای نرم‌افزاری

واپایش بند ۱۴-۲-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴-۲-۴ محدودسازی در اعمال تغییرات در بسته‌های نرم‌افزاری

واپایش بند ۱۴-۲-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴-۲-۵ اصول مهندسی نرم‌افزار امن

واپایش بند ۱۴-۲-۵ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴-۲-۶ محیط توسعه امن

واپایش بند ۱۴-۲-۶ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴-۲-۷ توسعهٔ برون‌سپاری شده

واپایش بند ۱۴-۲-۷ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴-۲-۸ آزمون سامانه امنیت

واپایش بند ۱۴-۲-۸ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۴-۲-۹ آزمون پذیرش سامانه

واپایش بند ۱۴-۲-۹ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

اطلاعات دیگر برای خدمات ابری

در رایانش ابری، راهنمایی برای آزمون پذیرش سامانه در استفاده از خدمات ابری توسط مشتری خدمت ابری

به‌کار می‌رود.

۱۴-۳ داده آزمون[1]

هدف مشخص شده در بند ۱۴-۳ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۴-۳-۱ حفاظت از داده آزمون

واپایش بند ۱۴-۳-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۵ روابط تأمین‌کننده

۱۵-۱ امنیت اطلاعات در روابط با تأمین‌کننده

هدف مشخص شده در بند ۱۵-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۵-۱-۱ خط‌مشی امنیت اطلاعات برای روابط تأمین‌کننده

واپایش بند ۱۵-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای قسمت خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری، ارائه‌کننده خدمت ابری را به‌عنوان نوعی تامین‌کننده در خط‌مشی امنیت اطلاعات خود برای روابط تامین‌کننده در نظر بگیرد. این به مدیریت و کاهش مخاطره مرتبط با دسترسی ارائه‌کننده خدمت ابری به اطلاعات مشتری خدمت ابری، کمک می‌کند.	(هیچ‌گونه راهنمای افزوده پیاده‌سازی وجود ندارد.)

۱۵-۱-۲ پرداختن به امنیت درون توافقنامه‌های تأمین‌کننده

واپایش بند ۱۵-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری نقش‌ها و مسئولیت‌های امنیت اطلاعات مرتبط با خدمات ابری را همانطور که در توافقنامه تشریح شده است، تأیید کند. این موارد می-	توصیه می‌شود ارائه‌کننده خدمت ابری اندازه‌های امنیت اطلاعات

1 - Test data

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توانند شامل فرایندهای زیر باشند. حفاظت بدافزار پشتیبان‌گیری واپایش‌های رمزنگاشتی مدیریت آسیب‌پذیری مدیریت رخداد بررسی تطابق فنی آزمون امنیت ممیزی جمع‌آوری، نگهداری و حفاظت از شواهد شامل ثبت‌های ورود و رَدهای(اثرهای) ممیزی[1] حفاظت از اطلاعات در خاتمه توافق خدمت واپایش دسترسی و اصالت‌سنجی مدیریت دسترسی و هویت	مرتبط به‌عنوان بخشی از توافق را که ارائه‌کننده خدمت ابری پیاده‌سازی می‌کند، مشخص کند تا اطمینان یابد که هیچ سوءتفاهمی بین ارائه‌کننده خدمت ابری و مشتری خدمت ابری وجود ندارد. اندازه‌های امنیت اطلاعات مرتبط که ارائه‌کننده خدمت ابری پیاده می‌کند، می‌تواند بسته به نوع خدمات ابری که مشتری خدمت ابری استفاده می‌کند متغیر باشد.

۱۵-۱-۳ زنجیره تأمین فناوری ارتباطات و اطلاعات

واپایش بند ۱۵-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
(هیچ‌گونه راهنمای افزوده پیاده‌سازی وجود ندارد.)	اگر ارائه‌کننده خدمت ابری از خدمات ابری ارائه‌کننده خدمت ابری همتا استفاده کند، توصیه می‌شود ارائه‌کننده خدمت ابری اطمینان یابد سطوح امنیت اطلاعات خدمات مشتری خود تأمین شده یا (حتی) فراتر رفته است. هرگاه ارائه‌کننده خدمت ابری، خدمات ابری مبتنی بر زنجیره تأمین را فراهم کند، توصیه می‌شود ارائه‌کننده خدمت ابری اهداف امنیت اطلاعات را برای تأمین‌کنندگان فراهم کرده و از هر تامین‌کننده بخواهد فعالیت‌های مدیریت مخاطره را اجرا کند تا به این اهداف دست یابد.

1 - Audit trails

۱۵-۲ مدیریت تحویل خدمت تأمین‌کننده

هدف مشخص شده در بند ۱۵-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۵-۲-۱ پایش و بازنگری خدمات تأمین‌کننده

واپایش بند ۱۵-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۵-۲-۲ مدیریت تغییرات در خدمات تأمین‌کننده

واپایش بند ۱۵-۲-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۶ مدیریت رخداد امنیت اطلاعات

۱۶-۱ مدیریت رخدادهای امنیت اطلاعات و بهبودها

هدف مشخص شده در بند ۱۶-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۶-۱-۱ مسئولیت‌ها و روش‌های اجرایی

واپایش بند ۱۶-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای قسمت خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری تخصیص مسئولیت‌ها برای مدیریت رخداد امنیت اطلاعات را تأیید کند و توصیه می‌شود اطمینان یابد که الزامات مشتری خدمت ابری را برآورده می‌کند.	توصیه می‌شود ارائه‌کننده خدمت ابری به‌عنوان بخشی از مشخصات خدمات تخصیص مدیریت، مسئولیت‌ها و روش‌های اجرایی رخداد امنیت اطلاعات بین مشتری خدمت ابری و ارائه‌کننده خدمت ابری را تعریف کند. توصیه می‌شود ارائه‌کننده خدمت ابری پوشش مستندات زیر را برای مشتری خدمت ابری فراهم کند: هدف از رخدادهای امنیت اطلاعات که ارائه‌کننده خدمت ابری به مشتری خدمت ابری گزارش می‌دهد. سطح افشاء کشف رخدادهای امنیت اطلاعات و پاسخ‌های مرتبط با آن قالب زمانی مورد نظر که وقوع رخدادهای امنیت اطلاعات را تذکر می‌دهد. روش اجرایی برای تذکر رخدادهای امنیت اطلاعات اطلاعات تماس برای رسیدگی به موارد مربوط به رخدادهای امنیت اطلاعات

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
	هر چاره‌ای که می‌تواند در صورت وقوع رخدادهای امنیت اطلاعات معین به‌کار رود.

۱۶-۱-۲ گزارش‌دهی رویدادهای امنیت اطلاعات

واپایش بند ۱۶-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای قسمت خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اطلاعات دربارهٔ سازوکارهای زیر را از ارائه‌کننده خدمت ابری درخواست کند: - گزارش دادنِ رویداد امنیت اطلاعات که از طرف مشتری خدمت ابری تشخیص داده شده است به ارائه‌کننده خدمت ابری. - دریافت گزارش مربوط به رویداد امنیت اطلاعات کشف شده به وسیله ارائه‌کننده خدمت ابر به ارائه‌کننده خدمت ابری - رهگیریِ وضعیتِ رویداد امنیت اطلاعات گزارش‌شده، توسط مشتری خدمت ابری	توصیه می‌شود ارائه‌کننده خدمت ابری سازوکارهایی برای موارد زیر فراهم کند: - گزارش دادنِ رویداد امنیت اطلاعات از سوی مشتری خدمت ابری به ارائه‌کننده خدمت ابری. - گزارش دادنِ رویداد امنیت اطلاعات از سوی ارائه-کننده خدمت ابری به مشتری خدمت ابری - رهگیریِ وضعیتِ رویداد امنیت اطلاعات گزارش‌شده، توسط مشتری خدمت ابری.

اطلاعات دیگر برای خدمات ابری

توصیه می‌شود سازوکارها فقط روش اجرایی را تعریف نکنند، بلکه اطلاعات ضروری مانند شماره تلفن تماس، نشانی رایانامه و زمان‌های خدمات را به مشتری خدمت ابری و ارائه‌کننده خدمت ابری بدهند.

یک رویداد امنیت اطلاعات می‌تواند هم توسط مشتری خدمت ابری و هم توسط ارائه‌کننده خدمت ابری کشف شود. بنابراین توصیه می‌شود مسئولیت افزوده اصلی رایانش ابری این باشد که کشف رویداد توسط یک بخش، دارای روش‌های اجرایی برای گزارش رویداد بلافاصله به قسمت دیگر باشد.

۱۶-۱-۳ گزارش‌دهی ضعف‌های امنیتی

واپایش بند ۱۶-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۶-۱-۴ برآورد و تصمیم برای رویدادهای امنیت اطلاعات

واپایش بند ۱۶-۱-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۶-۱-۵ پاسخ به رخدادهای امنیت اطلاعات

واپایش بند ۱۶-۱-۵ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۶-۱-۶ یادگیری از رخدادهای امنیت اطلاعات

واپایش بند ۱۶-۱-۶ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۶-۱-۷ گردآوری شواهد

واپایش بند ۱۶-۱-۷ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود ارائه‌کننده خدمت ابری و مشتری خدمت ابری دربارهٔ روش اجرایی پاسخ به درخواست‌های شواهد رقمی بالقوه یا اطلاعات دیگر از درون محیط رایانش ابری، توافق داشته باشند.	

۱۷ جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار

۱۷-۱ تداوم امنیت اطلاعات

هدف مشخص شده در بند ۱۷-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۷-۱-۱ طرح‌ریزی تداوم امنیت اطلاعات

واپایش بند ۱۷-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۷-۱-۲ پیاده‌سازی تداوم امنیت اطلاعات

واپایش بند ۱۷-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۷-۱-۳ بررسی، بازنگری و ارزیابی تداوم امنیت اطلاعات

واپایش بند ۱۷-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۷-۲ افزونگی‌ها[1]

هدف مشخص شده در بند ۱۷-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۷-۲-۱ دسترس‌پذیری تسهیلات پردازش اطلاعات

واپایش بند ۱۷-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۸ انطباق

۱۸-۱ انطباق با الزامات قانونی و قراردادی

هدف مشخص شده در بند ۱۸-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۸-۱-۱ شناسایی الزامات قانونی[2] و قراردادی[3] قابل اجرا

واپایش بند ۱۸-۱-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری موردی را در نظر بگیرد که قوانین و آیین‌نامه‌های مرتبط می‌توانند علاوه بر حاکمیت مشتری خدمت ابری، حوزه‌های قضایی حاکمیت ارائه‌کننده خدمت ابری باشند. توصیه می‌شود مشتری خدمت ابری شواهد انطباق ارائه‌کننده خدمت ابری با آیین‌نامه‌ها و استانداردهای مورد نیاز کسب‌وکار مشتری خدمت ابری را درخواست کند. این شواهد می‌تواند گواهینامه‌های تولید شده توسط ممیزین طرف سوم باشد.	توصیه می‌شود ارائه‌کننده خدمت ابری، مشتری خدمت ابری را از حوزه‌های قضایی حاکمیت قانونی خدمات ابری آگاه سازد. توصیه می‌شود ارائه‌کننده خدمت ابری الزامات قانونی مرتبط خود را شناسایی کند (مثلاً رمزنگاشتی مورد نظر برای محافظت از اطلاعات قابل‌شناسایی شخصی (PII)[4]). همچنین توصیه می‌شود این اطلاعات، حسب درخواست مشتری خدمت ابری، به وی ارائه شود. توصیه می‌شود ارائه‌کننده خدمت ابری شواهدی از انطباق جاری خود با الزامات قانونی و قراردادی کاربردپذیر را به مشتری خدمت ابری ارائه کند.

اطلاعات دیگر برای خدمات ابری

توصیه می‌شود الزامات آیین‌نامه‌ای و قانونی که برای تدارک و استفاده از خدمات ابری به‌کار می‌روند

1 - Redundancies
2 - Legal
3 - Contractual
4 - Personally Identifiable Information

شناسایی شوند، به خصوص هرکجا ظرفیت‌های پردازش، ذخیره‌سازی و ارتباطات به لحاظ جغرافیایی پخش شده است و می‌تواند شامل حوزه قضایی چندگانه باشد.

یادآوری این نکته مهم است که الزامات انطباق چه قانونی باشد و چه قراردادی، مسئولیت مشتری خدمت ابری به قوت خود باقی است. مسئولیت‌های انطباق نمی‌تواند به ارائه‌کننده خدمت ابری منتقل شود.

۱۸-۱-۲ حقوق دارایی فکری

واپایش بند ۱۸-۱-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای قسمت خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
نصب نرم‌افزار مجاز تجاری در خدمات ابری می‌تواند سبب نقض شرایط مجاز نرم‌افزار شود. توصیه می‌شود مشتری خدمت ابری روش اجرایی برای شناسایی الزامات مجاز مشخصات ابری، قبل از اجازه نصب هرگونه نرم‌افزار مجاز در خدمات ابری داشته باشد. توصیه می‌شود توجه خاصی به مواردی که خدمات ابری، الاستیک و مقیاس‌پذیر است و نرم‌افزار می‌تواند روی سامانه‌ها و هسته‌های پردازش‌گر بیشتری نسبت به موارد اجازه داده شده توسط شرایط مجاز اجرا شود، صورت گیرد.	توصیه می‌شود ارائه‌کننده خدمت ابری فرآیندی را برای پاسخ به شکایت‌های حقوق مالکیت معنوی ایجاد کند.

۱۸-۱-۳ حفاظت از سوابق

واپایش بند ۱۸-۱-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اطلاعاتی دربارهٔ حفاظت از ثبت‌های جمع‌آوری و ذخیره شده توسط ارائه‌کننده خدمت ابری که مرتبط با استفاده از خدمات ابری توسط مشتری خدمت ابری است را از ارائه‌کننده خدمت ابری درخواست کند.	توصیه می‌شود ارائه‌کننده خدمت ابری اطلاعاتی دربارهٔ حفاظت از ثبت‌های مربوط به استفاده از خدمات ابری توسط مشتری خدمت ابری که توسط ارائه‌کننده خدمت ابری جمع‌آوری و ذخیره می‌شوند را به مشتری خدمت ابری ارائه کند.

۱۸-۱-۴ حریم خصوصی و حفاظت از اطلاعات شخصی قابل‌شناسایی

واپایش بند ۱۸-۱-۴ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

اطلاعات دیگر برای خدمات ابری

استاندارد ISO/IEC 27018، آیین کار برای حفاظت PII در ابرهای عمومی که به‌عنوان پردازشگر PII عمل می‌کند، اطلاعات افزوده برای این موضوع پیشنهاد می‌کند.

۱۸-۱-۵ قواعد واپایش‌های رمزنگاشتی

واپایش بند ۱۸-۱-۵ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری تأیید کند که مجموعه‌ای از واپایش‌های رمزنگاشتی که برای استفاده از خدمات ابری به‌کار می‌رود، مطابق با توافق‌ها، قوانین و مقررات مرتبط است.	توصیه می‌شود ارائه‌کننده خدمت ابری توصیفی از واپایش‌های رمزنگاشتی پیاده شده توسط ارائه‌کننده خدمت ابری را به منظور بازنگری انطباق با توافق‌ها، قوانین و مقررات کاربردپذیر، به مشتری خدمت ابری ارائه کند.

۱۸-۲ بازنگری‌های امنیت اطلاعات

هدف مشخص شده در بند ۱۸-۲ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

۱۸-۲-۱ بازنگری مستقل امنیت اطلاعات

واپایش بند ۱۸-۲-۱ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند. راهنمای بخش خاص زیر نیز به‌کار می‌رود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری شواهد مستند شده‌ای که پیاده‌سازی واپایش‌های امنیت اطلاعات و راهنماهایی برای خدمات ابری در راستای هر ادعای ارائه‌کننده خدمت ابری است را درخواست کند. این شواهد می‌تواند شامل گواهینامه‌هایی در برابر	توصیه می‌شود ارائه‌کننده خدمت ابری شواهد مستند شده‌ای را به منظور اثبات ادعای خود در پیاده‌سازی واپایش‌های امنیت اطلاعات، به مشتری خدمت ابری ارائه کند. توصیه می‌شود جایی که هر یک از ممیزی‌های مشتری خدمت ابری غیرعملی هستند یا می‌توانند مخاطرات امنیت اطلاعات را افزایش دهند، ارائه‌کننده خدمت ابری شواهد مستقلی فراهم کند که امنیت اطلاعات در تطابق با خط‌مشی‌ها و روش‌های اجرایی ارائه‌کننده خدمت ابری، پیاده‌سازی و اجرا شده است. توصیه می‌شود پیش از ورود به قرارداد، آن‌ها در دسترس مشتری خدمت ابری باشند. توصیه می‌شود ممیزی مستقل مرتبط که توسط ارائه‌کننده خدمت ابری انتخاب می‌شود، به طور عادی روش قابل قبولی برای برآورده کردن خواسته مشتری خدمت ابری در مرور عملیات و تأمین شفافیت کافی ارائه‌کننده خدمت ابری باشد. توصیه می‌شود هرگاه ممیزی مستقل غیرعملی باشد،

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
استانداردهای مرتبط باشد.	ارائه‌کننده خدمت ابری ارزیابی شخصی را هدایت کند و فرآیند و نتایج خود را برای مشتری خدمت ابری افشا کند.

۱۸-۲-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی

واپایش بند ۱۸-۲-۲ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

۱۸-۲-۳ بازنگری انطباق فنی

واپایش بند ۱۸-۲-۳ و راهنمای پیاده‌سازی مربوط به آن و اطلاعات دیگر مشخص شده در استاندارد ISO/IEC 27002 به‌کار می‌روند.

پیوست الف

(الزامی)

مجموعه تعمیم‌یافته واپایش خدمات ابری

این پیوست اهداف واپایش، راهنمای واپایش‌ها و پیاده‌سازی اضافه‌ای را به‌عنوان مجموعه واپایش گسترش-یافته خدمات ابری ارائه می‌کند. اهداف واپایش استاندارد ISO/IEC 27002 مرتبط با آن واپایش‌ها، تکرار نمی‌شود.

توصیه می‌شود سازمانی که مایل به پیاده‌سازی این واپایش‌ها در سامانه مدیریت امنیت اطلاعات (ISMS)[1] است که باید مطابق با استاندارد ISO/IEC27001 باشد، بیانیه کاربردپذیری (SOA)[2] خود را با شمول واپایش‌های بیان شده در این پیوست، توسعه دهد.

CLD-۶-۳ رابطه بین مشتری خدمت ابری و تأمین‌کننده خدمت ابر

هدف - روشن‌سازی رابطه بین مشتری خدمت ابری و ارائه‌کننده خدمت ابری برای مدیریت امنیت اطلاعات با توجه به مسئولیت‌ها و نقش‌های به اشتراک گذاشته شده.

CLD-۶-۳-۱ مسئولیت‌ها و نقش‌های به اشتراک گذاشته شده درون محیط رایانش ابری

واپایش

توصیه می‌شود مسئولیت‌های نقش‌های امنیت اطلاعات به اشتراک گذاشته شده در استفاده از خدمات ابری، توسط هر دو مشتری خدمت ابری و ارائه‌کننده خدمت ابری، به طرف‌های شناسایی شده، مستند شده، مکاتبه شده و پیاده‌سازی شده تخصیص یابند.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری خط‌مشی‌ها و روش‌های اجرایی موجود خود را در تطابق با استفاده از خدمات ابری تعریف کند یا توسعه دهد و کاربران خدمات ابری را از نقش‌ها و مسئولیت‌های آنها در استفاده از خدمات ابری آگاه سازد.	توصیه می‌شود ارائه‌کننده خدمت ابری توانمندی‌ها، نقش‌ها و مسئولیت‌های امنیت اطلاعات خود را برای استفاده از خدمات ابری خود، همراه با مسئولیت‌ها و نقش‌های امنیت اطلاعات برای مشتری خدمت ابری که نیاز به پیاده‌سازی و مدیریت به‌عنوان بخشی از استفاده آن از خدمات ابری است را مستند و مکاتبه کند.

1 - Information Security Management System
2- Statement of Applicability

اطلاعات دیگر برای خدمات ابری

در رایانش ابری نقش‌ها و مسئولیت‌ها نوعاً بین کارکنان مشتری خدمت ابری و کارکنان ارائه‌کننده خدمت ابری تقسیم شده‌اند. توصیه می‌شود تخصیص نقش‌ها و مسئولیت‌ها، داده مشتری خدمت ابری و برنامه‌های کاربردی مشتری خدمت ابری که ارائه‌کننده خدمت ابری متولی آن است را در نظر بگیرد.

CLD-۸-۱ مسئولیت دارایی‌ها

هدف مشخص شده در بند ۸-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

CLD-۸-۱-۵ خروج[1] دارایی‌های مشتری خدمت ابری

واپایش

توصیه می‌شود دارایی‌های مشتری خدمت ابری که در حیطه ارائه‌کننده خدمت ابری هستند، درصورت لزوم، به‌مجرد خاتمه توافق‌نامه خدمت ابری، بازگردانده و زدوده[2] شوند.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری تشریح مستندی از خاتمه فرآیند خدمت را درخواست کند که برداشتن و بازگرداندن دارایی‌های مشتری خدمت ابری را با حذف تمام نسخه‌های آن دارایی‌ها از سامانه ارائه‌کننده خدمت ابری، پوشش دهد. توصیه می‌شود این تشریح تمام دارایی‌ها را فهرست کرده و برنامه زمانی ختم خدمات را مستند کند که توصیه می‌شود به موقع رخ دهد.	توصیه می‌شود ارائه‌کننده خدمت ابری اطلاعاتی دربارهٔ ترتیبات برداشتن و بازگرداندن هرگونه دارایی‌های مشتری خدمت ابری، به‌مجرد خاتمه توافقنامه استفاده از خدمت ابری را ارائه کند. توصیه می‌شود ترتیبات برداشتن و بازگرداندن دارایی‌ها در توافقنامه مستند شود و توصیه می‌شود به موقع اجرا شود. توصیه می‌شود ترتیبات، دارایی‌هایی را که باید برداشته و بازگردانده شوند را مشخص کند.

CLD-۹-۵ واپایش دسترسی به داده مشتری خدمت ابری در محیط مجازی به اشتراک گذاشته شده

هدف- کاهش مخاطرات امنیت اطلاعات در هنگام استفاده از محیط مجازی به اشتراک گذاشته شده رایانش ابری.

CLD-۹-۵-۱ تفکیک در محیط پردازش مجازی

واپایش

توصیه می‌شود محیط مجازی مشتری خدمت ابری که در خدمات ابری اجرا می‌شود از دیگر مشتریان

1 - Removal
2 - Removed

خدمت ابری و اشخاص غیرمجاز محافظت شود.

راهنمای پیاده‌سازی خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
(هیچ‌گونه راهنمای افزوده پیاده‌سازی وجود ندارد.)	توصیه می‌شود ارائه‌کننده خدمت ابری، تفکیک منطقی مناسبی از داده مشتری خدمت ابری، برنامه‌های کاربردی مجازی شده، سامانه‌های عامل، ذخیره‌سازی و شبکه را برای موارد زیر اجرا کند: - جداسازی منابع استفاده شده توسط مشتری خدمت ابری در محیط‌های چنداجاره‌ای - جداسازی ادارات درونی ارائه‌کننده خدمت ابری از منابع استفاده شده توسط مشتری خدمت ابری توصیه می‌شود هرگاه خدمات ابری شامل چنداجاره‌ای باشد، ارائه‌کننده خدمت ابری، واپایش‌های امنیت اطلاعات را برای اطمینان از ایزوله‌سازی مناسب منابع استفاده شده توسط مستأجرین متفاوت پیاده‌سازی کند. توصیه می‌شود ارائه‌کننده خدمت ابری مخاطره مرتبط با اجرای نرم‌افزار تهیه شده توسط مشتری خدمت ابری درون خدمات ابری که توسط ارائه‌کننده خدمت ابری پیشنهاد شده است را در نظر بگیرد.

اطلاعات دیگر برای خدمات ابری

پیاده‌سازی تفکیک منطقی وابسته به فناوری‌های به‌کار رفته در مجازی‌سازی است:

- هرگاه کارکرد مجازی‌سازی، نرم‌افزار محیط مجازی را تأمین کند (مثل سامانه بهره‌برداری مجازی)، پیکربندی‌های شبکه و حافظه می‌توانند مجازی شوند. به‌علاوه تفکیک مشتری خدمت ابری در محیط مجازی شده نرم‌افزار می‌تواند با استفاده از کارکردهای تفکیک نرم‌افزار طراحی و پیاده‌سازی شود.
- هرگاه اطلاعات مشتری خدمت ابری در فضای حافظه فیزیکی به اشتراک گذاشته شده با «جدول فراداده» خدمت ابری ذخیره شود، تفکیک اطلاعات از دیگر مشتریان خدمت ابری می‌تواند با واپایش دسترسی روی «جدول فراداده» پیاده‌سازی شود.

چند اجاره‌ای امن و راهنمای مرتبط داده شده در استاندارد «ISO/IEC 27040، فناوری اطلاعات - فنون امنیتی- امنیت ذخیره‌سازی» می‌تواند در محیط رایانش ابری به‌کار رود.

CLD-۹-۵-۲ مقاوم‌سازی ماشین مجازی

واپایش

توصیه می‌شود ماشین‌های مجازی در محیط رایانش ابری برای برآوردن نیازهای کسب‌وکار مقاوم شوند.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود در هنگام پیکربندی ماشین‌های مجازی، مشتری خدمت ابری و ارائه‌کننده خدمت ابری، اطمینان حاصل کنند که جنبه‌های مقتضی مقاوم شده‌اند (مثلاً، فقط آن درگاه‌ها، پروتکل‌ها و خدماتی که نیاز است) و اینکه اقدامات فنی مناسب (مثل ضدبدافزار، واقعه‌نگاری) برای هر ماشین مجازی استفاده شده، برقرار شده باشند.	

CLD-۱۲-۱ مسئولیت‌ها و روش‌های اجرایی

هدف مشخص شده در بند ۱۲-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

CLD-۱۲-۱-۵ امنیت عملیاتی مدیران

واپایش

توصیه می‌شود روش‌های اجرایی برای عملیات محیط رایانش ابری تعریف، مستند و پایش شوند.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری روش‌های اجرایی برای عملیات بحرانی که شکست می‌تواند سبب آسیب غیرقابل بازیابی به دارایی‌ها در محیط رایانش ابری شود را مستند کند. مثال‌هایی از عملیات بحرانی عبارتند از: - نصب، تغییر و حذف افزاره‌های مجازی شده مثل کارسازها، شبکه‌ها و حافظه - روش‌های اجرایی خاتمه، برای استفاده از خدمات ابری - پشتیبان‌گیری و بازیابی توصیه می‌شود سند مشخص کند که ناظر، این عملیات را پایش می‌کند.	توصیه می‌شود ارائه‌کننده خدمات ابری، مستندی را دربارهٔ عملیات و روش‌های اجرایی بحرانی برای مشتری خدمت ابری که آن را نیاز دارد، فراهم کند.

اطلاعات دیگر برای خدمات ابری

رایانش ابری دارای فواید تدارکات سریع، اداره کردن و خدمات سرخود مبتنی بر تقاضا است. اغلب این عملیات به‌وسیله اداره‌کنندگان مشتری خدمت ابری و ارائه‌کننده خدمت ابری اجرا می‌شوند.

توصیه می‌شود به این دلیل که مداخله انسانی در این عملیات بحرانی می‌تواند سبب رخدادهای امنیت اطلاعات جدی شود، سازوکارهایی برای محافظت از این عملیات در نظر گرفته شده و در صورت لزوم، تعریف و پیاده‌سازی شوند. مثال‌هایی از رخدادهای جدی شامل پاک شدن یا خاموش شدن تعداد زیادی از کارسازهای مجازی یا تخریب دارایی‌های مجازی است.

CLD-۱۲-۴ ثبت و پایشگری

هدف مشخص شده در بند ۱۲-۴ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

CLD-۱۲-۴-۵ پایش خدمات ابری

واپایش

توصیه می‌شود مشتری خدمت ابری توانمندی پایش جنبه‌های مشخص عملیات خدمات ابری که مشتری خدمت ابری استفاده می‌کند را داشته باشد.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
توصیه می‌شود مشتری خدمت ابری اطلاعاتی درباره توانمندی‌های پایش خدمات در دسترس برای هر خدمات ابری را از ارائه‌کننده خدمت ابری درخواست کند.	توصیه می‌شود ارائه‌کننده خدمت ابری توانمندی‌هایی فراهم کند که مشتری خدمت ابری را قادر به پایش جنبه‌های مشخص، مرتبط با مشتری خدمت ابری، عملیات خدمات ابری می‌سازد. به‌عنوان مثال پایش و کشف این که خدمات ابری به‌عنوان سکویی برای حمله به دیگران استفاده شده است یا داده‌های حساس از خدمات ابری نشت کرده است. توصیه می‌شود واپایش دسترسی مناسب استفاده از توانمندی‌ها، تنها دسترسی به اطلاعات مربوط به مثال‌های خدمات ابری مشتری خدمت ابری را فراهم کند. توصیه می‌شود ارائه‌کننده خدمت ابری مستنداتی از توانمندی‌های پایش خدمات برای مشتری خدمت ابری را فراهم کند. توصیه می‌شود پایش، داده‌های یکپارچه با رویدادهای ورود تشریح شده در بند ۱۲-۴-۱ و معطوف به شرایط SLA را تأمین کند.

CLD-۱۳-۱ مدیریت امنیت شبکه

هدف مشخص شده در بند ۱۳-۱ از استاندارد ISO/IEC 27002 به‌کار می‌رود.

CLD-۱۳-۱-۴ هم‌ترازی مدیریت امنیت برای شبکه‌های فیزیکی و مجازی

واپایش

توصیه می‌شود در پیکربندی شبکه‌های مجازی، ثبات پیکربندی‌های بین شبکه‌های فیزیکی و مجازی براساس خط‌مشی امنیت شبکه ارائه‌کننده خدمت ابری درستی‌سنجی شود.

راهنمای پیاده‌سازی برای خدمات ابری

مشتری خدمت ابری	ارائه‌کننده خدمت ابری
(هیچ‌گونه راهنمای افزوده پیاده‌سازی وجود ندارد.)	توصیه می‌شود ارائه‌کننده خدمات ابری، خط‌مشی امنیت اطلاعات را برای پیکربندی شبکه مجازی شامل خط‌مشی امنیت اطلاعات برای شبکه فیزیکی تعیین و مستند کند. توصیه می‌شود ارائه‌کننده خدمت ابری اطمینان حاصل کند که پیکربندی شبکه مجازی مطابق با خط‌مشی امنیت اطلاعات صرف‌نظر از مفاهیم استفاده شده در ایجاد پیکربندی، است.

اطلاعات دیگر برای خدمات ابری

در محیط رایانش ابری ساخته شده در فناوری مجازی‌سازی، شبکه مجازی در زیرساخت مجازی بر روی شبکه فیزیکی پیکربندی شده است. در این محیط‌ها، عدم ثبات خط‌مشی‌های شبکه می‌تواند سبب قطع سامانه یا واپایش دسترسی معیوب شود.

یادآوری- مسئولیت‌های پیکربندی شبکه مجازی می‌تواند بسته به نوع خدمات ابری، بین مشتری خدمت ابری و ارائه‌کننده خدمت ابری متغیر باشد.

پیوست ب

(آگاهی‌دهنده)

مراجع مخاطره امنیت اطلاعات مربوط به رایانش ابری

استفاده مناسب از واپایش‌های امنیت اطلاعات ارائه شده توسط این استاندارد به ارزیابی و برطرف‌سازی مخاطره امنیت اطلاعات سازمان وابسته است. اگرچه این موضوعات مهم هستند، اما تمرکز این استاندارد در مسیر ارزیابی و برطرف‌سازی مخاطره امنیت اطلاعات نیست. در زیر فهرستی از مراجعی که شامل تشریح منابع مخاطره و مخاطرات تدارک و استفاده از خدمات ابری هستند، آورده شده است. باید یادآوری شود که منابع مخاطره و مخاطرات با توجه به نوع و ماهیت خدمات و فناوری‌های در حال ظهور خدمات ابری تغییر می‌کنند. به کاربران این استاندارد پیشنهاد می‌شود که در صورت لزوم به نسخه‌های جاریِ مستندات مراجعه کنند.

- Recommendation ITU-T X.1601 (2014), Security framework for cloud computing.
- Australian Government Information Management Office 2013, Summary of Checkpoints in: Privacy and Cloud Computing for Australian Government Agencies, Better Practice Guide, Version 1.1, February, pg. 8. http://www.finance.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf
- Australian Government Cyber Security Centre 2015, Cloud Computing Security for Tenants – April. http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Tenants.pdf
- Australian Government Cyber Security Centre 2015, Cloud Computing Security for Cloud Service Providers – April. http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Cloud_Service_Providers.pdf
- Cloud Security Alliance 2014, Cloud Controls Matrix – January.
- ENISA 2009, Cloud Computing Security Risk Assessment – November.
- ENISA 2009, Cloud Computing Information Assurance Framework – November.
- Hong Kong OGCIO 2013, Security & Privacy Checklist for Cloud Service Providers in Handling Personal Identifiable Information in Cloud Platforms – April.
- Hong Kong OGCIO 2013, Security Checklists for Cloud Service Consumers – January.
- ISACA 2012, Security Considerations for Cloud Computing – July.
- NIST, SP 800-144 2011, Guidelines on Security and Privacy in Public Cloud Computing – December.
- NIST, SP 800-146 2012, Cloud Computing Synopsis and Recommendations – May.
- SPRING Singapore 2012, Annex A: Virtualisation Security Risk Assessment of Singapore Technical Reference 30:2012 Technical Reference for virtualisation security for servers – March.

- SPRING Singapore 2012, Annex A: Checklist of security and service level considerations when reviewing SaaS of Singapore Technical Reference 31:2012 Technical Reference for security and service level guidelines for the usage of public cloud computing services – March.
- SPRING Singapore 2013, Annex A: Cloud Service Provider Disclosure of Singapore Standard SS 584:2013 Specification for Multi-Tiered Cloud Computing Security – August.
- SPRING Singapore 2012, Annex B: Checklist of security and service level considerations when reviewing IaaS of Singapore Technical Reference 31:2012 Technical Reference for security and service level guidelines for the usage of public cloud computing services – March.
- SPRING Singapore 2013, Singapore Standard SS 584:2013 Specification for Multi-Tiered Cloud Computing Security – August.
- SPRING Singapore 2012, Singapore Technical Reference 30:2012 Technical Reference for virtualisation security for servers – March.
- SPRING Singapore 2012, Singapore Technical Reference 31:2012 Technical Reference for security and service level guidelines for the usage of public cloud computing services – March.
- US Government FedRAMP PMO 2014, FedRAMP Security Controls Baseline Version 2.0 – June

کتاب‌نامه

[1] Recommendation ITU-T X.805 (2003), Security architecture for systems providing end-to-end communications.

[2] ISO/IEC 17203:2011, Information technology – Open Virtualization Format (OVF) specification.

[3] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.

[4] ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management.

[5] ISO/IEC 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

[6] ISO/IEC 27036-1:2014, Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts.

[7] ISO/IEC 27036-2:2014, Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements.

[8] ISO/IEC 27036-3:2013, Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security.

[9] ISO/IEC CD 27036-4, Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services – (Under development).

[10] ISO/IEC 27040:2015, Information technology – Security techniques – Storage security.

[11] ISO 19440:2007, Enterprise integration – Constructs for enterprise modelling.

[12] ISO 31000:2009, Risk management – Principles and guidelines.

[13] NIST, SP 800-145 2011, The NIST Definition of Cloud Computing.

[14] NIST 2009, Effectively and Securely Using the Cloud Computing Paradigm.

[15] ENISA 2009, Cloud Computing Benefits, risks and recommendations for information security.

[16] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.

[17] Cloud Security Alliance, Top Threats to Cloud Computing V1.0.

[18] Cloud Security Alliance, Domain 12: Guidance for Identity & Access Management V2.1.

[19] ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives.

[20] ISACA, Cloud Computing Management Audit/Assurance Program.