ارائه‌ی الگوی پیاده‌سازی نظام مدیریت امنیت اطلاعات در محیط رایانش ابری

مهدی نقیان فشارکی
مصطفی تمتاجی

تاریخ دریافت: ۹۳/۸/۱۷
تاریخ پذیرش: ۹۳/۹/۲۳

چکیده:

رایانش ابری، مدل رو به رشد ارائه‌ی خدمات فناوری اطلاعات است که در آن کاربر از طریق اتصال به وب، به‌سرعت و با کمترین تلاش و تعامل، به منابع رایانشی موردنیاز دسترسی می‌یابد. رایانش ابری ضمن صرفه‌جویی در هزینه‌ها، دغدغه‌هایی از قبیل مقیاس‌پذیری، فراهم‌آوری منابع و انعطاف‌پذیری را کاهش می‌دهد.

در کنار مزایای متعدد رایانش ابری، دغدغه‌ی امنیت در محیط پیچیده‌ی ابری، از مهم‌ترین چالش‌هایی است که باید به آن پاسخ داده شود.

تجارب موفق و الزامات امنیتی مناسب در استاندارد نظام مدیریت امنیت اطلاعات (ISO/IEC27001:2013) جمع‌شده است تا تضمین کند که امنیت در سازمان در سطح مطلوب بوده و رو به بهبود است.

در این مقاله، ضمن معرفی مختصر رایانش ابری و چالش‌های آن، الگویی برای پیاده‌سازی نظام مدیریت امنیت اطلاعات در محیط رایانش ابری ارائه خواهد شد. الگوی مذکور مشتمل بر مجموعه‌ی کاملی از ۳۵۵ مؤلفه‌ی امنیتی در هفت گروه است که در این مقاله ضمن معرفی این هفت گروه، مؤلفه‌های مذکور از سطح دغدغه تا راهکار در سه سطح دسته‌بندی‌شده و نگاشت سطوح یک و دو با کنترل‌های استاندارد ISO/IEC 27001:2013 ارائه خواهد شد. الگوی ارائه‌شده به سازمان کمک می‌کند تا مؤلفه‌های موردنیاز برای پیاده‌سازی نظام مدیریت امنیت اطلاعات در محیط رایانش ابری را شناسایی و نسبت به ارائه‌ی راهکار قابل‌اجرا برای هر مؤلفه اقدام کند.

واژگان کلیدی:

رایانش ابری، امنیت، نظام مدیریت امنیت اطلاعات

۱) مقدمه

رایانش ابری یک مدل برای دسترسی فراگیر، راحت و به‌محض درخواست به مخزن منابع رایانشی قابل پیکربندی و به اشتراک گذاشته‌شده (برای مثال شبکه‌ها، سرورها، ذخیره‌سازها، برنامه‌های کاربردی و سرویس‌ها) است که می‌تواند به‌سرعت و با کمینه تلاش مدیریتی یا تعامل با ارائه‌دهنده‌ی سرویس، تأمین‌شده و در دسترس کاربر قرار گیرد[۱].

امنیت اطلاعات، یک حوزه‌ی مطالعاتی بین‌رشته‌ای و فعالیت حرفه‌ای است که با توسعه و پیاده‌سازی انواع مختلف سازوکارهای امنیتی (فنی، سازمانی، دارای منشأ انسانی و قانونی) مرتبط است و هدف آن دور نگه‌داشتن اطلاعات در همه‌ی مکان‌ها (داخل سازمان یا بیرون آن) و چرخه‌ی اطلاعات (هنگام ایجاد، پردازش، ذخیره‌سازی، انتقال و امحا) از تهدایدت به‌منظور دستیابی به اهداف امنیتی است. اهداف امنیتی علاوه بر دسترس‌پذیری، جامعیت و محرمانگی می‌توانند شامل اصالت، قابلیت اعتماد، حریم خصوصی، پاسخ‌گویی و قابلیت ممیزی باشند[۲].

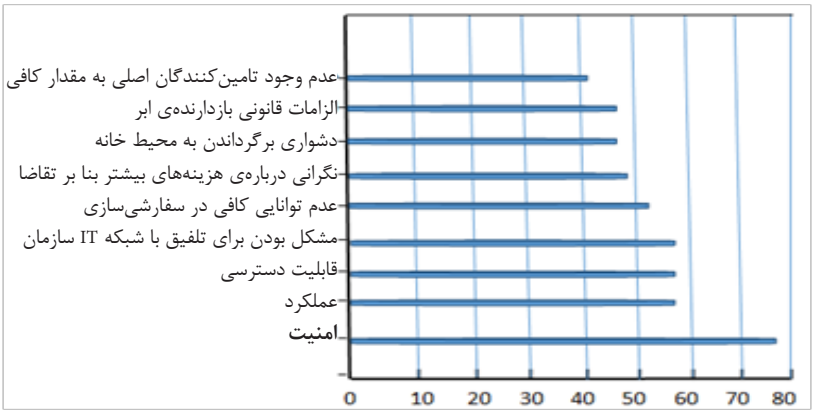
در محیط ابری، الگوهای دسترسی و مسئولیت‌ها تغییر می‌کند. کنترل‌ها جابه‌جا می‌شود، مقیاس‌پذیری منابع موردتقاضا واقع می‌شود، سرعت دسترسی به داده و برنامه افزایش می‌یابد. به‌عبارت‌دیگر همه‌ی جنبه‌های مطرح در امنیت فناوری اطلاعات دستخوش تغییر و حتی دگرگونی می‌شود. شاید واژه‌های یکسان، مفاهیم مختلف و

راهکارهـای پیاده‌سـازی متفاوتـی را در محیـط ابـری رقـم بزننـد و ایـن خـود مسـئله‌ای اسـت کـه بایـد در محیـط ابـری بـه آن توجـه ویـژه کـرد. شـکل (۱) چنـد نمونـه موضوعـات متـداول امنیتـی و تعبیـر آن در محیـط ابـری را نشـان می‌دهـد[۳].

شکل ۱: تغییر مفاهیم در محیط رایانش ابری [۳]

همان‌طـور کـه بیـان شـد، هنـگام مواجه‌شـدن بـا رایانـش ابـری، امنیـت مهم‌تریـن دغدغـه اسـت. امنیـت در رایانـش ابـری یکـی از مسـائل پیچیـده به‌شـمار رفتـه کـه به‌عنـوان مانعـی در مقابـل اسـتفاده‌ی کاربـران از مزایـای رایانـش ابـری قلمـداد می‌شـود. چالـش اصلـی امنیـت ایـن اسـت کـه مالـک داده، کنترلـی روی آن نـدارد.

نتایـج حاصـل از نظرسـنجی شـرکت IDC[1] از ۲۴۴ مدیـر فنـاوری اطلاعـات مطابـق شـکل (۲) نشـان داد کـه در بیـن نُـه چالـش اساسـی مطـرح در حـوزه‌ی رایانـش ابـری، امنیـت بزرگ‌تریـن چالـش اسـت و بـا کسـب ۷۴٫۵ درصـد، مقـام نخسـت دغدغه‌هـای مدیـران سـازمان‌ها را بـه خـود اختصـاص داده اسـت[۴].



شکل ۲: رتبه‌بندی چالش‌های اساسی رایانش ابری [۴]

ازآنجاکـه رایانـش ابـری شـامل بسـیاری از فناوری‌هـا ازجملـه شـبکه، پایگاه‌هـای داده، سیسـتم عامل‌هـا، زمان‌بنـدی منابـع، مدیریـت تراکنش‌هـا، کنتـرل هم‌زمانـی و مدیریـت حافظـه اسـت، لـذا تهدیـدات امنیتـی مختلفـی بـا توجـه بـه نیازمندی‌هـای مختلـف امنیتـی (محرمانگـی، یکپارچگـی، دسـترس‌پذیری و ...) قابل‌تصـور اسـت. ایـن تنـوع، سـبب می‌شـود مواجهـه بـا امنیـت در چنیـن محیطـی سـخت و نیازمنـد طرح‌ریـزی مناسـب باشـد.

۲) نظام مدیریت امنیت اطلاعات[2]

بـا توجـه بـه رشـد روزافـزون و چشـمگیر فنـاوری اطلاعـات و لـزوم اسـتانداردسـازی در ایـن حـوزه و به‌منظـور وجـود نگـرش جامـع نسـبت بـه اسـتانداردسـازی در زمینـه‌ی مباحـث فنـاوری اطلاعـات، سـازمان بین‌المللـی اسـتانداردسـازی (ISO) و کمیسـیون بین‌المللـی الکتروتکنیـک (IEC) اقـدام بـه ایجـاد کمیتـه‌ی فنـی مشـترک (JTC1) بـه نـام "فنـاوری اطلاعـات" بـا ۱۸ زیـر کمیتـه فعـال کردنـد کـه تاکنـون ۲۷۲۹ اسـتاندارد

1. International Data Corporation
2. Information Security Management System-ISMS

در زمینه‌های مختلف فناوری اطلاعات منتشر کرده‌اند. استانداردهای حوزه‌ی امنیت اطلاعات، در کمیته‌ی فرعی امنیت (SC۲۷) بررسی می‌شود[۵].

با توجه به چندوجهی‌بودن مقوله‌ی امنیت و لزوم توجه چندبعدی به آن و همچنین توجه روزافزون به مباحث مدیریت امنیت اطلاعات از طریق برقراری قوانین و ضوابط ملی، منطقه‌ای و بین‌المللی و راهبردهای جدید به‌منظور پاسخ‌گویی به انتظارات و الزامات طرف‌های ذی‌نفع نسبت به اطمینان از امنیت اطلاعات، کمیته‌ی فرعی امنیت تصمیم به تدوین استاندارد "نظام مدیریت امنیت اطلاعات" در کنار استانداردهای فنی گرفت و بر این اساس خانواده‌ی استانداردهای ۲۷۰۰۰ به‌عنوان مرجع بین‌المللی پذیرفته‌شده برای امنیت اطلاعات مطرح شدند. از این خانواده تاکنون بیش از ۳۵ استاندارد منتشرشده یا در حال انتشار است که برخی از آن‌ها در جدول (۱) معرفی شده‌اند[۵].

کد استاندارد	عنوان استاندارد	وضعیت	سال
ISO/IEC 27000	کلیات و واژگان	Published	۲۰۱۴
ISO/IEC 27001	الزامات نظام مدیریت امنیت اطلاعات	Published	۲۰۱۳
ISO/IEC 27002	آیین کار نظام مدیریت امنیت اطلاعات	Published	۲۰۱۳
ISO/IEC 27003	راهنمای پیاده‌سازی نظام مدیریت امنیت اطلاعات	Under Revision	۲۰۱۰
ISO/IEC 27004	اندازه‌گیری نظام مدیریت امنیت اطلاعات	Under Revision	۲۰۰۹
ISO/IEC 27005	مدیریت مخاطرات امنیت اطلاعات	Under Revision	۲۰۱۱
ISO/IEC 27006	الزامات نهادهای ممیزی و صدور گواهی‌نامه‌ی نظام مدیریت امنیت اطلاعات	Under Revision	۲۰۱۱
ISO/IEC 27007	راهنمای ممیزی نظام مدیریت امنیت اطلاعات	Published	۲۰۱۱
ISO/IEC TR 27008	راهنمای ممیزان برای کنترل‌های امنیت اطلاعات	Published	۲۰۱۱
ISO/IEC 27009	استفاده و به‌کارگیری ISO/IEC 27001 برای صدور گواهی شخص ثالث Sector/Service	Under Development	-
ISO/IEC 27011	راهنمای نظام مدیریت امنیت اطلاعات برای سازمان‌های مخابراتی	Under Revision	۲۰۰۸
ISO/IEC 27013	راهنمای پیاده‌سازی یکپارچه ISO/IEC 27001 و ISO 20000-1	Under Revision	۲۰۱۲
ISO/IEC 27014	حاکمیت امنیت اطلاعات	Published	۲۰۱۳
ISO/IEC TR 27015	راهنمای مدیریت امنیت اطلاعات برای خدمات مالی	Published	۲۰۱۲

جدول ۱: استانداردهای خانواده ۲۷۰۰۰ [۵]

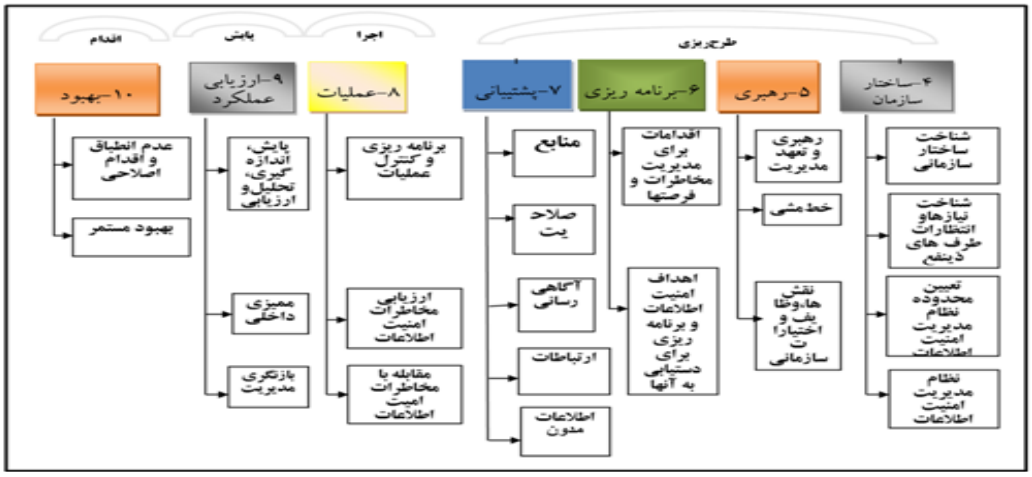
همچنین برخی از استانداردهای بین‌المللی حوزه‌ی رایانش ابری در جدول (۲) ذکرشده است[۵].

کد استاندارد	عنوان استاندارد	وضعیت	سال
ISO/IEC 27018	آیین کار حفاظت اطلاعات شناسایی در محیط ابر عمومی	Published	2014
ISO/IEC 17826	واسط مدیریتی داده‌های ابری(CDMI)	Published	2012
ISO/IEC CD 27017	راهنمای کنترل‌های امنیتی ۲۷۰۰۲ برای سرویس‌های مبتنی بر رایانش ابری	Under Development	-
ISO/IEC WD 27036-4	امنیت اطلاعات در تعامل با تأمین‌کنندگان ـ راهنمایی برای خدمات ابری	Under Development	-
ISO/IEC PRF 17788	کلیات و واژگان رایانش ابری	Under Development	-
ISO/IEC DIS 17789	معماری مرجع رایانش ابری	Under Development	-
ISO/IEC NP 19086	چارچوب و واژه‌شناسی توافق‌نامه‌ی سطح خدمات در رایانش ابری	Under Development	-
ISO/IEC DTR 20000-9	مدیریت خدمات ـ راهنمای به‌کارگیری ISO/IEC 20000-1 در خدمات ابری	Under Development	-
ISO/IEC DIS 19831	مدل واسط مدیریتی زیرساخت ابری	Under Development	-

جدول ۲: استانداردهای رایانش ابری سازمان ISO [۵]

نظام مدیریت امنیت اطلاعات، بخشی از نظام مدیریت بناشده مبتنی بر دیدگاه مخاطرات کسب‌وکار، به‌منظور ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات است. یک نظام مدیریتی مشتمل بر ساختار سازمانی، خط‌مشی‌ها، طرح‌ریزی فعالیت‌ها، مسئولیت‌ها، تجارب، روش‌های اجرایی مدون، فرایندها و منابع است[۶] و [۷].

استاندارد فوق شامل ۱۴ حوزه، ۳۶ هدف کنترلی و ۱۱۴ کنترل امنیتی به‌منظور اقدامات بازدارنده و نظارتی است. شکل (۳) فهرست الزامات ذکرشده در متن استاندارد را نشان می‌دهد[۵] و [۸].



شکل ۳: الزامات متن استاندارد ISO/IEC 27001:2013 [۵]

در جدول (۳) حوزه‌ها و اهداف کنترلی ضمیمه‌ی (الف) استاندارد مذکور تشریح‌شده است.

حوزه‌ی کنترلی	اهداف کنترلی
الف ـ۵ خط‌مشی‌های امنیت اطلاعات	الف ـ۵ـ۱ هدایت امنیت اطلاعات توسط مدیریت
الف ـ۶ سازمان امنیت اطلاعات	الف ـ۶ـ۱ سازمان داخلی الف ـ۶ـ۲ دستگاه‌های سیار و دورکاری
الف ـ۷ امنیت منابع انسانی	الف ـ۷ـ۱ پیش از استخدام الف ـ۷ـ۲ حین استخدام الف ـ۷ـ۳ خاتمه‌ی استخدام یا تغییر شغل
الف ـ۸ مدیریت دارایی	الف ـ۸ـ۱ مسئولیت دارایی‌ها الف ـ۸ـ۲ طبقه‌بندی اطلاعات الف ـ۸ـ۳ ساماندهی رسانه‌ها
الف ـ۹ کنترل دسترسی	الف ـ۹ـ۱ الزامات کسب‌وکار برای کنترل دسترسی الف ـ۹ـ۲ مدیریت دسترسی کاربر الف ـ۹ـ۳ مسئولیت‌های کاربر الف ـ۹ـ۴ کنترل دسترسی به سامانه و برنامه‌های کاربردی
الف ـ۱۰ رمزنگاری	الف‌ـ۱۰ـ۱ کنترل رمزنگاری
الف ـ۱۱ امنیت فیزیکی و محیطی	الف ـ۱۱ـ۱ نواحی امن الف ـ۱۱ـ۲ تجهیزات
الف ـ۱۲ امنیت عملیات	الف ـ۱۲ـ۱ مسئولیت‌ها و رویه‌های عملیاتی الف ـ۱۲ـ۲ حفاظت در برابر بدافزارها الف ـ۱۲ـ۳ نسخه‌ی پشتیبان الف ـ۴ واقعه‌نگاری و پایش الف ـ۱۲ـ۵ کنترل نرم‌افزار عملیاتی الف ـ۱۲ـ۶ مدیریت آسیب‌پذیری فنی الف ـ۱۲ـ۷ ملاحظات ممیزی سامانه‌های عملیاتی
الف ـ۱۳ امنیت ارتباطات	الف ـ۱۳ـ۱ مدیریت امنیت شبکه الف ـ۱۳ـ۲ انتقال اطلاعات
الف ـ۱۴ اکتساب، توسعه و نگهداری سامانه	الف ـ۱۴ـ۱ الزامات امنیتی سامانه‌های اطلاعاتی الف ـ۱۴ـ۲ امنیت در فرایندهای توسعه و پشتیبانی الف ـ۱۴ـ۳ داده‌های آزمون

حوزه‌ی کنترلی	اهداف کنترلی
الف ـ۱۵ ارتباط با تأمین‌کنندگان	الف ـ۱۵ـ۱ امنیت اطلاعات در ارتباط با تأمین‌کنندگان الف ـ۱۵ـ۲ مدیریت تحویل خدمات تأمین‌کنندگان
الف ـ۱۶ مدیریت حوادث امنیت اطلاعات	الف ـ۱۶ـ۱ مدیریت بهبودها و حوادث امنیت اطلاعات
الف ـ۱۷ جنبه‌های امنیت اطلاعات در مدیریت تداوم کسب‌وکار	الف ـ۱۷ـ۱ تداوم کسب‌وکار الف ـ۱۷ـ۲ افزونگی‌ها
الف ـ۱۸ انطباق	الف ـ۱۸ـ۱ انطباق با الزامات قانونی و قراردادی الف ـ۱۸ـ۲ بازنگری‌های امنیت اطلاعات

جدول ۳: حوزه‌ها و اهداف کنترلی ضمیمه‌ی استاندارد ISO/IEC 27001:2013 [۸ و ۵]

۳) چالش‌های محیط رایانش ابری

الگوی جدید رایانش ابری گرچه مزایا و منافع متعددی را نسبت به الگوهای قبلی فراهم‌کرده و سازمان‌های بسیاری خود را با آن وفق داده‌اند، ولی هنوز چالش‌های متعددی وجود دارند که به‌طور کامل حل نشده‌اند.

مشابه سایر فناوری‌های نوظهور، رایانش ابری نیز تعدادی مسئله‌ی حل‌نشده (باز) دارد که لزوماً منحصر به ابر نیستند و برخی از آن‌ها دغدغه‌هایی برای همه‌ی سرویس‌ها هستند. به‌طور خلاصه مسائل حل‌نشده و دغدغه‌های بی‌پاسخ رایانش ابری را می‌توان به پنج دسته‌ی زیر تقسیم کرد:[۹]

ـ کارایی رایانش (تأخیر، مدیریت ذخیره‌سازی داده، برنامه‌نویسی مقیاس‌پذیر)،

ـ قابلیت اطمینان ابر (وابستگی به شبکه، قطعی خدمات، پردازش امن)،

ـ اهداف اقتصادی (مخاطرات تداوم کسب‌وکار، ارزیابی توافق‌نامه‌ی سرویس، تعامل بین ارائه‌دهندگان، بازیابی حادثه)،

ـ انطباق (محل فیزیکی داده، قوانین، تفحص)،

ـ امنیت اطلاعات (مخاطرات افشای ناخواسته‌ی اطلاعات، حریم خصوصی، چند مستاجری، مدیریت کلید).

سند NIST-SP800-144 با عنوان"راهنمای امنیت و حریم خصوصی در رایانش ابری عمومی"، چالش‌ها و موضوعات عمده و اثرگذار روی برقراری امنیت و حفظ حریم خصوصی را در نُه دسته‌ی زیر طبقه‌بندی کرده است: [۱۰]

۱. حاکمیت[1]: حاکمیت روی کنترل و نظارت سازمان در خط‌مشی‌ها، رویه‌ها و استانداردهای مورداستفاده در توسعه‌ی برنامه‌های کاربردی و اکتساب سرویس‌های فناوری اطلاعات شامل طراحی، پیاده‌سازی، آزمون، استفاده و پایش سرویس تمرکز دارد. با توجه به دسترس‌پذیری وسیع سرویس‌های رایانش ابری، فقدان کنترل روی کاربران منشأ مشکلات متعددی است. باوجوداینکه رایانش ابری اکتساب و فراهم‌آوری منابع و سکو[2] را ساده می‌کند ولی نیاز به حاکمیت را نه‌تنها کاهش نداده بلکه ضروری می‌سازد. اگر اقدامات حاکمیتی توسط سازمان طرح‌ریزی و اجرا نشوند، خط‌مشی‌ها و رویه‌های امنیت و حریم خصوصی سازمان موردتوجه قرار نخواهند گرفت و سازمان با مخاطره‌ی بزرگی مواجه خواهد شد. به‌عنوان‌مثال، سیستم‌های آسیب‌پذیر استفاده خواهند شد، الزامات قانونی چشم‌پوشی خواهند شد، منابع برای اهداف غیرضروری به‌کارگیری می‌شوند.

۲. انطباق[3]: مسئولیت سازمان در برآورده‌سازی قوانین، مقررات، استانداردها و ویژگی‌ها را بیان می‌کند. انواع مختلفی از قوانین حریم خصوصی و امنیتی در هر کشور وجود دارد که خود موضوعات پیچیده‌ی بالقوه‌ای برای رایانش ابری هستند. موضوعاتی مانند محل ذخیره‌سازی اطلاعات، کنترل‌های امنیتی، مدیریت ذخیره‌سازی و کشف الکترونیکی[4] در این حوزه قرار می‌گیرند.

۳. اعتماد[5]: اعتماد به موضوعات و چالش‌های تهدیدات داخلی ناشی از چند مستاجری، حفظ مالکیت داده و

1. Governance
2. Platform
3. Compliance
4. Electronic discovery
5. Trust

حقـوق مالکیـت معنـوی، مدیریـت مخاطـرات و شـفافیت عملکـرد بـه ارائه‌دهنـده‌ی ابـر برمی‌گـردد.

۴. معمـاری: معمـاری نرم‌افـزار و سـخت‌افزار مورداسـتفاده بـرای ارائـه‌ی خدمـات ابـری در میـان ارائه‌دهنـدگان ابرهـای عمومـی بـرای هـر مـدل خدمـات خـاص می‌توانـد به‌طـور قابل‌توجهـی متفـاوت باشـد. معمـاری موضوعـات مرتبـط بـا سیسـتم‌های نرم‌افـزاری استفاده‌شـده در سـکوی ابـری را مطـرح می‌کنـد. ایـن موضوعـات شـامل مـواردی چـون امنیـت ابرناظـر[1]، حفاظـت شـبکه‌ی مجـازی، تصاویـر ماشـین مجـازی و حفاظـت از سـمت کاربـر اسـت.

۵. مدیریـت دسترسـی و تشـخیص هویـت: تمرکـز ایـن بخـش روی سـازوکارهای احـراز هویـت، تأییـد هویـت و کنتـرل دسترسـی اسـت. بـرای احـراز هویـت اسـتفاده از SAML[2] و بـرای کنتـرل دسترسـی اسـتفاده از XACML[3] توصیه‌شـده اسـت.

۶. جداسـازی نرم‌افـزار[4]: ایـن بخـش بـه تهدیـدات مرتبـط بـا چنـد مسـتاجری ازجملـه حمـلات بـرداری و پیچیدگی ابرناظرهـا اشـاره می‌کنـد. صرف‌نظـر از مـدل خدمـات و معمـاری نرم‌افـزار چندکاربـره استفاده‌شـده، محاسـبات مصرف‌کننـدگان مختلـف بایـد در محیـط جداشـده از دیگـر کاربـران انجـام شـود کـه عمدتـاً از سـازوکارهای جداسـازی منطقـی اسـتفاده می‌شـود.

۷. حفاظـت از داده: داده‌هـای ذخیره‌شـده در ابـر در یـک فضـای مشـترک بـا سـایر مشـتریان ابـر و در مکانـی معمـولاً نامعلـوم ذخیـره می‌شـوند. لـذا اطمینـان از محافظـت داده در برابـر دسترسـی سـایر مشـتریان و جداسـازی آن موضـوع مهمـی اسـت.

۸. دسـترس‌پذیری: بـه عبـارت سـاده، دسـترس‌پذیری بـازه‌ای اسـت کـه در آن مجموعـه‌ی کامـل منابـع رایانشـی موردنیـاز سـازمان در دسـترس و قابل‌اسـتفاده اسـت. دسـترس‌پذیری می‌توانـد به‌صـورت موقتـی یـا دائمـی سـازمان را تحـت تأثیـر قـرار دهـد و گم‌شـدن داده می‌توانـد جزئـی یـا کلـی باشـد. حمـلات رد سـرویس[5]، خرابـی تجهیـزات و حـوادث طبیعـی ازجملـه تهدیـدات دسـترس‌پذیری هسـتند.

۹. پاسـخ‌گویی بـه حـوادث: پیچیدگـی سـرویس‌های ابـری، تفکیـک نقش‌هـا و مسـئولیت‌ها در مقابـل حـوادث امنیتـی، سـازوکار کنتـرل و کاهـش پیامدهـای امنیتـی بـر کسـب‌وکار سـازمان ازجملـه موضوعـات مهـم در ایـن حـوزه هسـتند.

۴) الگوی پیاده‌سازی ISMS در محیط رایانش ابری

همان‌طـور کـه قبـلاً بیـان شـد نظـام مدیریـت امنیـت اطلاعـات به‌عنـوان یـک راهـکار جامـع مدیریتـی و فنـی بـرای مقابلـه بـا مخاطـرات امنیتـی پذیرفته‌شـده اسـت. لیکـن پیاده‌سـازی ایـن نظـام نیازمنـد وجـود یـک الگـوی جامـع اسـت. پیچیدگی‌هـای موجـود در محیـط رایانـش ابـری، لـزوم چنیـن الگویـی را مضاعـف می‌سـازد. در ایـن تحقیـق بـرای دسـتیابی بـه ایـن الگـو از روش زیـر استفاده‌شـده اسـت:

۱. گـردآوری مجموعـه‌ی کامـل مؤلفه‌هـای امنیتـی رایانـش ابـری،

۲. دسـته‌بندی و طبقه‌بنـدی مؤلفه‌هـای امنیتـی مبتنـی بـر نیازهـای امنیتـی سـازمان،

۳. نگاشـت بیـن مؤلفه‌هـای امنیتـی و کنترل‌هـای امنیتـی اسـتاندارد ISO/IEC 27001:2013،

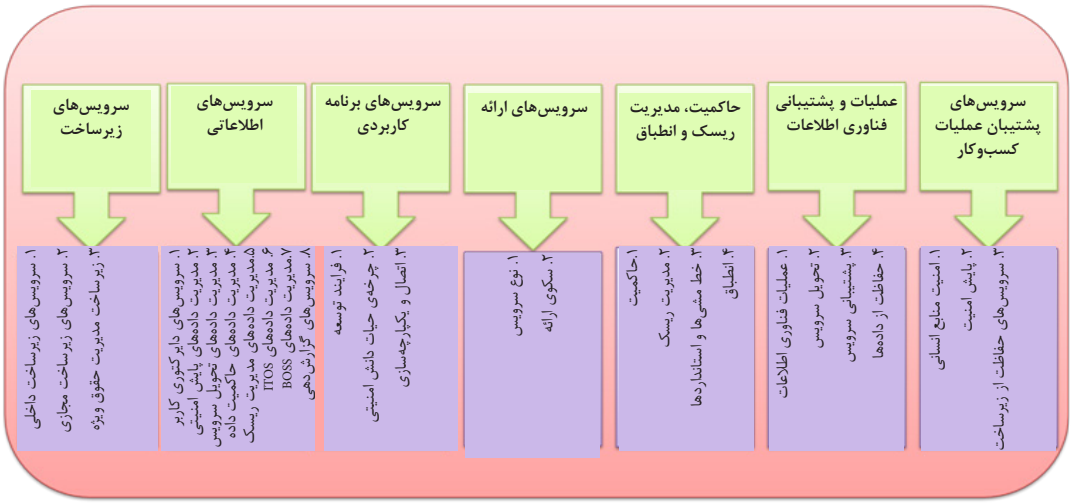
۴. ارزیابـی الگـوی به‌دسـت‌آمده بـا اسـتفاده از روش دلفـی.

۴ـ۱) گردآوری و طبقه‌بندی مؤلفه‌های امنیتی

شـکل (۴) ۷ حـوزه و مؤلفه‌هـای امنیتـی سـطح اول آن‌هـا را نشـان می‌دهـد. ۳۵۵ مؤلفـه‌ی امنیتـی از معمـاری مرجـع ویرایـش دوم انجمـن امنیـت ابـر[6] استخراج‌شـده [۱۱] و در ۷ حـوزه و سـه سـطح تقسـیم‌بندی شـده‌اند. مبنـای دسـته‌بندی سـطوح، مطابـق مرجـع مورداسـتفاده، رسـیدن بـه راهـکار امنیتـی قابـل پیاده‌سـازی اسـت. به‌عبارت‌دیگـر طبقه‌بنـدی مؤلفه‌هـای امنیتـی درواقـع پاسـخ بـه دغدغه‌هـا یـا همـان چالش‌هـای امنیتـی از طریـق ارائـه‌ی راهـکار امنیتـی متناسـب اسـت.

4.Software Isolation
5. denial of service
6. Cloud Security Alliance-CSA

1. Hypervisor
2. Security Assertion Markup Language
3. eXtensible Access Control Markup Language



شکل ۴: دسته‌بندی مؤلفه‌های امنیتی رایانش ابری

۴ـ۱ـ۱) حوزه‌ی سرویس‌های پشتیبان عملیات کسب‌وکار[1]

این حوزه، جنبه‌ها و موضوعاتی از قبیل منابع انسانی، پایش امنیت، اطمینان از عملکرد زیرساخت را در نظر می‌گیرد. مؤلفه‌های این حوزه عبارت‌اند از:

الف) امنیت منابع انسانی: اغلب حوادث و نقض‌های امنیتی به‌دلیل عدم وجود کنترل، آگاهی و راهنمایی‌های کاربران رخ می‌دهد. این قابلیت به‌منظور حصول اطمینان از وجود فرایند رسمی، روش‌های اجرایی، گزینش مناسب کارکنان و سایر موارد مرتبط با کارکنان و اشخاص ثالث همکار با سازمان ایجادشده است.

ب) پایش امنیت: رویداد نگاری وقایع و تحلیل آن‌ها، پایش پایگاه‌های داده و برنامه‌های کاربردی در این دسته قرار دارند.

پ) سرویس‌های حفاظت از زیرساخت: سرور، نقطه‌ی انتهایی[2]، شبکه و لایه‌ی برنامه‌های کاربردی را امن می‌سازد.

۴ـ۱ـ۲) حوزه‌ی عملیات و پشتیبانی فناوری اطلاعات[3]

این حوزه، همان واحد فناوری اطلاعات سازمان است که مسئول دریافت، ثبت و رفع مشکلات عملیات فناوری اطلاعات است. مؤلفه‌های این حوزه عبارت‌اند از:

الف) عملیات فناوری اطلاعات: عملیات فناوری اطلاعات، ساختار سازمانی، الزامات مهارتی واحد فناوری اطلاعات و رویه‌های مدیریت عملیات را تعریف می‌کند تا سازمان توانایی مدیریت عملیات فناوری اطلاعات و زیرساخت مرتبط با آن را داشته باشد. این عملیات باید همسو با راهبرد سازمان باشد،

ب) تحویل سرویس: تحویل سرویس با فناوری‌های ضروری برای برقراری سرویس‌های بدون وقفه سروکار دارد. سرویس‌های این حوزه معمولاً شامل آن‌هایی می‌شوند که برای کارکنان مناسب هستند مثل مدیریت دسترس‌پذیری، مدیریت سطح سرویس، تداوم سرویس و مدیریت ظرفیت،

پ) پشتیبانی سرویس: پشتیبانی سرویس روی دغدغه‌ی اصلی کاربران یعنی اطمینان از دسترسی به‌موقع به سرویس‌های موردنیاز تمرکز دارد.

ت) حفاظت از داده‌ها: در عصر اطلاعات، داده یک دارایی است؛ اما بیشتر داده‌ها تا زمانی‌که محافظت‌شده باشند، دارای ارزش هستند. حفاظت از داده باید شامل همه مراحل چرخه‌ی عمر داده، انواع داده و وضعیت‌های مختلف باشند.

۴ـ۱ـ۳) حوزه‌ی حاکمیت، مدیریت مخاطرات و انطباق

این حوزه شامل برنامه‌ی امنیت اطلاعات سازمان به‌منظور محافظت از دارایی‌ها و کشف، ارزیابی و

1. Business Operation Support Services-BOSS
2. End-point
3. Information Technology Operation & Support-ITOS

پایش مخاطرات اطلاعات سازمان است. مؤلفه‌های این حوزه عبارت‌اند از:

الف) حاکمیت: فعالیت‌هایی ازجمله حاکمیت سازمانی، مدیریت سطح بلوغ امنیتی سازمان و اطمینان از قابل‌قبول بودن آن، سیاست‌گذاری‌های کلان و اطمینان از یکپارچگی خط‌مشی‌ها و رویه‌های امنیتی در این حوزه قرار می‌گیرد.

ب) مدیریت مخاطرات: مدیریت مخاطرات سازمان، مدیریت مخاطرات باقی‌مانده و پایش وضعیت آن‌ها و همچنین مدیریت تهدیدات و آسیب‌پذیری‌ها که جز مراحل ارزیابی مخاطرات سازمان است در این بخش قرار دارد.

پ) خط‌مشی‌ها و استانداردها: خط‌مشی‌های امنیتی از الزامات مبتنی بر مخاطرات کسب‌وکار به‌دست‌آمده و در سطوح مختلف ازجمله خط‌مشی امنیت اطلاعات، خط‌مشی امنیت فیزیکی، خط‌مشی تداوم کسب‌وکار، خط‌مشی‌های امنیت زیرساخت، خط‌مشی‌های امنیت برنامه‌های کاربردی و خط‌مشی مدیریت مخاطرات عملیاتی کسب‌وکار وجود دارند.

ت) انطباق: تمرکز این قابلیت در ردیابی و اثبات انطباق و برنامه‌ریزی برای رفع موارد عدم انطباق با الزامات قانونی، مقرراتی و قراردادی است.

۴ـ۱ـ۴) حوزه‌ی سرویس‌های ارائه

محلی است که کاربر نهایی با یک راهکار فناوری اطلاعات تعامل برقرار می‌کند. سرویس‌های این حوزه عبارت‌اند از:

الف) نوع سرویس: الزامات امنیتی برای این حوزه براساس نوع کاربر و نوع سرویس تغییر می‌کند. برای مثال یک وب‌سایت تجارت الکترونیکی چالش‌های امنیتی متفاوتی نسبت به سایت شبکه‌ی اجتماعی دارد. نوع سرویس روی این قبیل چالش‌های امنیتی تمرکز دارد که براساس نوع کاربر و نوع سرویس متفاوت هستند.

ب) سکوی ارائه: سرویس‌های سکوی ارائه روی انواع مختلف نقاط انتهایی که کاربر در تعامل با راهکار استفاده می‌کند از قبیل تجهیزات سیار، تجهیزات قابل‌حمل یا تجهیزات دارای کاربرد خاص تمرکز دارد. الزامات امنیتی برحسب نوع دستگاهی که کاربر استفاده می‌کند، متفاوت است.

۴ـ۱ـ۵) حوزه‌ی سرویس‌های برنامه‌ی کاربردی

شامل قوانین و فرایندهای پشت واسط کاربری است که داده‌ها را دست‌کاری می‌کند و تعاملات کاربر را انجام می‌دهد. مثلاً در یک بانک آنلاین، این سرویس تراکنش پرداخت صورت‌حساب است که مقدار وجه را از حساب کاربر کسر و به‌حساب گیرنده اضافه می‌کند. همچنین این سرویس‌ها فرایندهای توسعه‌ی برنامه‌ی کاربردی را نیز شامل می‌شود. سرویس‌های این حوزه عبارت‌اند از:

الف) فرایند توسعه: فرایند توسعه باید چالش‌های امنیتی را حین ساخت راهکار لحاظ کنند. این کار می‌تواند با استفاده از ابزارهایی مانند مرورگر کد منبع که درزهای امنیتی را نشان می‌دهد یا مرورگر آسیب‌پذیری برنامه‌های وب که مقاومت برنامه در برابر حملات متداول هکرها را نمایش می‌دهد، انجام شود.

ب) چرخه‌ی حیات دانش امنیتی: برای ساخت برنامه‌های کاربردی امن، تیم توسعه باید به اطلاعات جدید و آخرین تهدیدات و شاخص‌های مناسب آگاهی داشته باشد.

پ) اتصال و یکپارچه‌سازی: واسط‌های برنامه‌نویسی، میان‌افزارهای یکپارچه‌ساز و مکانیزم‌ها، پروتکل‌ها و زبان مشترک برای انتقال داده‌ی معنادار بین دو برنامه‌ی کاربردی در این بخش قرار دارند.

۴ـ۱ـ۶) حوزه‌ی سرویس‌های اطلاعاتی[1]

یکی از نقاط قابل‌توجه در سازمان‌ها، حجم داده‌های تولیدشده در سازمان شامل داده‌های افزونه و تکراری است. همه این داده‌ها باید به اطلاعات مفیدی تبدیل گردند تا مالکان دارایی‌ها بتوانند اولویت‌بندی و مدیریت مخاطرات حوزه‌ی خود را انجام دهند. این حوزه‌ی استخراج، تبدیل و بارگذاری اطلاعات را در یک مدل داده‌ی مشترک مدیریت می‌کند.

۴ـ۱ـ۷) حوزه‌ی سرویس‌های زیرساخت

1. Information Services

حوزه‌ی سرویس‌های زیرساخت، قابلیت‌های اصلی برای پشتیبانی لایه‌های بالاتر معماری را فراهم می‌کند. این لایه‌ای از سرویس است که از برنامه‌های کاربردی ابر پشتیبانی کرده و بیشتر کاربران می‌توانند آن را ببینند. این سطح از ماشین‌های مجازی، برنامه‌های کاربردی و پایگاه‌های داده تشکیل‌شده است. سرویس‌های این حوزه عبارت‌اند از:

الف) سرویس‌های زیرساخت داخلی: سرویس‌های زیرساخت داخلی عمدتاً مرتبط با دارایی‌های فیزیکی مورداستفاده توسط تأمین‌کننده‌ی سرویس ابری برای پشتیبانی سرویس‌های مجازی است. گرچه این سرویس‌ها از دید کاربر پنهان هستند ولی پایه و اساس عملیات امن و قابل‌اطمینان هستند.

ب) سرویس‌های زیرساخت مجازی: سرویس‌های مجازی سازی در این حوزه قرار می‌گیرند. بعنوان مثال تصاویر نرم‌افزارها برای سرورهای مجازی که در سکوی مجازی‌شده روی سرور فیزیکی میزبانی می‌شوند، باید به‌صورت امن ساخته و مدیریت شوند.

پ) زیرساخت مدیریت حقوق ویژه: این زیرساخت تضمین می‌کند که کاربران دسترسی و حقوق موردنیاز برای اجرای وظایف و مسئولیت‌هایشان را با استفاده از مکانیزم‌های مدیریت دسترسی و هویت از قبیل مدیریت هویت، سرویس‌های احراز هویت، سرویس‌های صدور مجوز و مدیریت کاربردهای خاص دارا هستند.

در مرحله دوم، نگاشت بین مؤلفه‌های امنیتی و کنترل‌های استاندارد موردنظر برقرارشده است. به این منظور با توجه به ماهیت هر مؤلفه، همه‌ی ۳۵۵ مؤلفه‌ی امنیتی به کنترل امنیتی ضمیمه‌ی (الف) استاندارد، نگاشت شده‌اند. جدول (۴) نگاشت مؤلفه‌های سطح اول و سطح دوم به کنترل‌های امنیتی استاندارد مذکور را نشان می‌دهد.

۴ـ۲) نظر خبرگان در خصوص جامعیت و عملیاتی بودن الگو

به‌منظور صحه‌گذاری روند طی‌شده در تحقیق و اخذ نظرات خبرگان در خصوص الگوی ارائه‌شده، از روش دلفی و ابزار پرسش‌نامه استفاده شد. روش دلفی فرایندی ساختاریافته برای جمع‌آوری و طبقه‌بندی دانش موجود در نزد گروهی از کارشناسان و خبرگان است که از طریق توزیع پرسش‌نامه‌هایی در بین این افراد و بازخورد کنترل‌شده‌ی پاسخ‌ها و نظرات دریافتی صورت می‌گیرد. یکی از دلایل انتخاب این روش، وابسته‌نبودن این روش به تعداد خبرگان است. ازآنجاکه تعداد متخصصان و کارشناسان در دسترس در حوزه‌ی موردپژوهش زیاد نیست، لذا روش دلفی می‌تواند روش مناسبی برای اخذ نظرات باشد.

مراحل انجام‌شده برای اخذ نظرات خبرگان عبارت‌اند از:

گام اول: ابزاری که برای جمع‌آوری داده‌ها مورداستفاده قرار می‌گیرد، در مرحله‌ی نخست باید از روایی[1] برخوردار باشد. روایی بدین معناست که روش یا ابزار به‌کاررفته تا چه حدی قادر است خصوصیت موردنظر را درست اندازه‌گیری کند. برای اطمینان از روایی، سؤالات پرسش‌نامه توسط دو نفر از خبرگان بررسی و اصلاح شد.

گام دوم: در مرحله‌ی دوم سند معماری بین ۱۰ نفر خبره توزیع‌شده و نظرات به‌صورت ناشناس و بدون ارتباط با یکدیگر در قالب پرسش‌نامه و همچنین نظرات آزاد اخذشده و نظرات دارای تناقض با تعامل به اجماع رسید و پیشنهادها در الگو لحاظ شد.

گام سوم: در این گام، در جلسه‌ی مشترک با حضور همه‌ی خبرگان، الگوی اصلاح‌شده تبیین و نظرات در قالب پرسش‌نامه نهایی اخذ و تحلیل‌شده است.

ابزار مورداستفاده علاوه بر روایی، باید پایایی[2] داشته باشند. پایایی قابلیت تکرار روش یا ابزار اندازه‌گیری است.

متداول‌ترین روش برای اثبات پایایی، محاسبه‌ی ضریب آلفای کرونباخ است. هرقدر شاخص آلفای کرونباخ به یک نزدیک‌تر باشد، همبستگی درونی بین سؤالات بیشتر و درنتیجه‌ی پرسش‌ها همگن‌تر خواهند بود. کرونباخ ضریب پایایی ۴۵ درصد را کم،

1. Validity

2. Reliability

۷۵ درصد را متوسط و قابل‌قبول و ضریب ۹۵ درصد را زیاد پیشنهاد کرده است.

در این تحقیق برای سؤالات نهایی پرسش‌نامه، ضریب آلفای کرونباخ با کمک نرم‌افزار SPSS محاسبه شد. خروجی نرم‌افزار SPSS در جدول زیر نشان شده است.

Reliability Statistics	
Cronbach's Alpha	N of Items
.813	7

جدول ۵ـ۳ : ضریب آلفای کرونباخ

با توجه به نتایج به‌دست‌آمده، الگوی ارائه‌شده به‌درستی طرح‌ریزی‌شده و ضمن جامع‌بودن، به سازمان در پیاده‌سازی نظام مدیریت امنیت اطلاعات کمک می‌کند. همچنین همه‌ی خبرگان موضوع، در این زمینه توافق داشتند که تمامی الزامات نظام مدیریت امنیت اطلاعات ذکرشده در استاندارد ISO/IEC 27001:2013 و همچنین بخش عمده‌ای از اصول و راهنمایی‌های بیان‌شده در استاندارد ISO/IEC 27002:2013 با نگاه به راهنمایی‌های تکمیلی سند ISO/IEC CD 27017 در این الگو بیان‌شده است.

در تحلیل پرسش‌نامه کمترین درصد مطلوب (پنج نفر موافق، چهار نفر ممتنع و یک نفر مخالف) مربوط به مانع‌بودن مؤلفه‌های امنیتی است که به‌علت تعداد زیاد مؤلفه‌ها، صحه‌گذاری آن‌ها توسط خبرگان با تأمل انجام‌شده است.

۵) نتیجه‌گیری

امنیت در رایانش ابری از چالش‌های مهمی است که ابعاد حل‌نشده‌ی بسیاری دارد. تنوع فناوری‌های موجود در محیط رایانش ابری و نیازمندی‌های متعدد امنیتی مطرح در آن، مقوله‌ی امنیت را به موضوعی اساسی و اثرگذار در رشد و توسعه این محیط تبدیل کرده است.

شاید بتوان استقرار و کنترل امنیت در یک سازمان کوچک را بدون پیاده‌سازی نظام مدیریت امنیت اطلاعات تصور کرد، اما چنین تصوری در محیط رایانش ابری ممکن نیست. لذا توجه به استقرار یک نظام مدیریت امنیت اطلاعات براساس تجربه‌های برتر ذکرشده در استاندارد ISO/IEC 27001:2013 به‌عنوان یک راهکار امنیتی اجتناب‌ناپذیر است. در این تحقیق تلاش شد تا پیاده‌سازی نظام مدیریت امنیت اطلاعات در محیط رایانش ابری، به‌عنوان یک راهکار برای اطمینان ازلحاظ‌شدن همه جنبه‌های امنیت ارائه شود.

به این منظور ابتدا مجموعه‌ی کاملی از ۳۵۵ مؤلفه‌ی امنیتی شناسایی و در هفت گروه و سه سطح دسته‌بندی شد. سطوح پایین‌تر به راهکار عملیاتی و سطوح بالاتر به مفهوم چالش امنیتی نزدیک‌تر هستند. سپس نگاشت بین مؤلفه‌های امنیتی سطح اول و دوم با حوزه‌ها و اهداف کنترلی ذکرشده در ضمیمه‌ی (الف) استاندارد ISO/IEC 27001:2013 برقرار شد.

مطابق با نگاشت انجام‌شده و نظر خبرگان موضوع، الگوی ارائه‌شده تضمین می‌کند که امنیت در محیط رایانش ابری تحت کنترل بوده و درصورتی‌که به‌طور کامل پیاده‌سازی شود، تمامی حوزه‌های کنترلی ذکرشده در نظام مدیریت امنیت اطلاعات برآورده خواهد شد.

۶) منابع و مراجع

1. Mell, P. and T. Grance, SP-800-145: The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 2011.

2. Cherdantseva Y. and Hilton J.A Reference Model of Information Assurance & Security, University of Regensburg, Germany. IEEE Proceedings, 2013.

3. Corporation, I, IBM Cloud Computing Reference Architecture 3.0-Security. 2012.

4. Velte, T, A. Velte, and R. Elsenpeter, Cloud Computing, a Practical Approach: McGraw-Hill, Inc. 2010.

5. International Organization for Standardization, List of ISO Technical Committees, "http ://www.iso.org/iso/standards_development/technical_committees/"

6. ISO/IEC 27001:2013, Information Technology-Security Techniques-Information Security Management Systems-Requirements, 2013.

7. ISO/IEC 27000, Information Technology-Security Techniques-Information Security Management systems-Overview and Vocabulary, 2014.

8. ISO/IEC 27002:2013, Information Technology-Security Techniques-Code of Practice for Information Security Management,2013.

9. Voas, L.B.T.G.R.P.-C.J, SP-800-146:Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology, (Lack of Portability Between PaaS CloudsEvent-based Processor Scheduling. 2012.

10. Jansen, W. and T. Grance, NIST SP-800-144: Guidelines on Security and Privacy in Public cloud Computing. NIST Special Publication, 2011.

11. Archer, J, et al, Quick guide to the Reference Architecture (TCI-RA). Cloud-Security Alliance-CSA, 2011.

حوزه	مؤلفه‌ی امنیتی سطح بالا	مؤلفه‌ی امنیتی سطح متوسط	حوزه‌ی کنترلی ISO/IEC ۲۷۰۰۱:۲۰۱۳
حاکمیت، مدیریت ریسک و انطباق	انطباق	مدیریت انطباق	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	مدیریت تأمین‌کنندگان	الف ـ۱۵ ارتباط با تأمین‌کنندگان
حاکمیت، مدیریت ریسک و انطباق	انطباق	قراردادها	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	E-Discovery	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	آماده‌سازی قانونی پاسخ‌گویی حوادث	الف ـ۱۶ مدیریت حوادث امنیت اطلاعات
حاکمیت، مدیریت ریسک و انطباق	انطباق	طرح‌ریزی ممیزی	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	ممیزی‌های مستقل	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	ممیزی‌های شخص ثالث	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	ممیزی‌های داخلی	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	نگاشت رگولاتوری سیستم‌های اطلاعاتی	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	به روز نگه‌داشتن مجوزها و تعاملات با شرکا	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	حفاظت از مالکیت فکری	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	آزمون انطباق	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	تحلیل Forensic	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	انطباق	مدیریت ممیزی	الف ـ۱۸ انطباق

حوزه	مؤلفه‌ی امنیتی سطح بالا	مؤلفه‌ی امنیتی سطح متوسط	حوزه‌ی کنترلی ISO/IEC ۲۷۰۰۱:۲۰۱۳
حاکمیت، مدیریت ریسک و انطباق	حاکمیت	مدیریت خط‌مشی	الف ـ۵ خط‌مشی‌های امنیت اطلاعات
حاکمیت، مدیریت ریسک و انطباق	حاکمیت	آموزش و آگاهی رسانی فنی	الف ـ۷ امنیت منابع انسانی
حاکمیت، مدیریت ریسک و انطباق	حاکمیت	حاکمیت داده	الف ـ۵ خط‌مشی‌های امنیت اطلاعات
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	مدیریت ریسک فناوری اطلاعات	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	داشبورد ریسک	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	مدیریت آسیب‌پذیری	الف ـ۱۲ امنیت عملیات
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	آزمون نفوذ	الف ـ۱۲ امنیت عملیات
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	مدیریت تهدیدات	الف ـ۱۲ امنیت عملیات
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	مدیریت ریسک‌های باقی‌مانده	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	کمیته ریسک عملیاتی	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	مدیریت بحران	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	تداوم کسب‌وکار	الف ـ۱۷ جنبه‌های امنیت اطلاعات در مدیریت تداوم کسب‌وکار
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	شاخص‌های ریسک کلیدی	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	چارچوب مدیریت ریسک	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	مدیریت ریسک	مدیریت ریسک مستقل	الف ـ۱۸ انطباق
حاکمیت، مدیریت ریسک و انطباق	خط‌مشی‌ها و استانداردها	خط مبنای امنیت عملیاتی	الف ـ۵ خط‌مشی‌های امنیت اطلاعات
حاکمیت، مدیریت ریسک و انطباق	خط‌مشی‌ها و استانداردها	راهنماهای شغلی	الف ـ۷ امنیت منابع انسانی
حاکمیت، مدیریت ریسک و انطباق	خط‌مشی‌ها و استانداردها	آگاهی‌رسانی برای هر نقش	الف ـ۷ امنیت منابع انسانی
حاکمیت، مدیریت ریسک و انطباق	خط‌مشی‌ها و استانداردها	خط‌مشی‌های امنیت اطلاعات	الف ـ۵ خط‌مشی‌های امنیت اطلاعات
حاکمیت، مدیریت ریسک و انطباق	خط‌مشی‌ها و استانداردها	استانداردهای امنیتی فنی	الف ـ۵ خط‌مشی‌های امنیت اطلاعات
حاکمیت، مدیریت ریسک و انطباق	خط‌مشی‌ها و استانداردها	خط‌مشی طبقه‌بندی دارایی‌ها/ داده	الف ـ۵ خط‌مشی‌های امنیت اطلاعات
حاکمیت، مدیریت ریسک و انطباق	خط‌مشی‌ها و استانداردها	ارتباط و تعامل با رگولاتوری و تجربیات برتر	الف ـ۶ سازمان امنیت اطلاعات
سرویس‌های زیرساخت	زیرساخت مدیریت حقوق ویژه	مدیریت هویت	الف ـ۹ کنترل دسترسی
سرویس‌های زیرساخت	زیرساخت مدیریت حقوق ویژه	سرویس‌های احراز هویت	الف ـ۹ کنترل دسترسی
سرویس‌های زیرساخت	زیرساخت مدیریت حقوق ویژه	سرویس‌های صدور مجوز	الف ـ۹ کنترل دسترسی
سرویس‌های زیرساخت	زیرساخت مدیریت حقوق ویژه	مدیریت کاربردهای خاص	الف ـ۹ کنترل دسترسی
سرویس‌های پشتیبان عملیات کسب‌وکار	سرویس‌های حفاظت از زیرساخت	سرور	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	سرویس‌های حفاظت از زیرساخت	نقاط انتهایی	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	سرویس‌های حفاظت از زیرساخت	برنامه‌ی کاربردی	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	سرویس‌های حفاظت از زیرساخت	شبکه	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	امنیت منابع انسانی	خاتمه‌ی استخدام کارکنان	الف ـ۷ امنیت منابع انسانی
سرویس‌های پشتیبان عملیات کسب‌وکار	امنیت منابع انسانی	توافق‌نامه‌ی استخدام	الف ـ۷ امنیت منابع انسانی
سرویس‌های پشتیبان عملیات کسب‌وکار	امنیت منابع انسانی	گزینش و بررسی سابقه کارکنان	الف ـ۷ امنیت منابع انسانی
سرویس‌های پشتیبان عملیات کسب‌وکار	امنیت منابع انسانی	نقش‌ها و مسئولیت‌ها	الف ـ۷ امنیت منابع انسانی
سرویس‌های پشتیبان عملیات کسب‌وکار	امنیت منابع انسانی	توصیف و شرح شغل	الف ـ۷ امنیت منابع انسانی
سرویس‌های پشتیبان عملیات کسب‌وکار	امنیت منابع انسانی	آگاهی کارکنان	الف ـ۷ امنیت منابع انسانی
سرویس‌های پشتیبان عملیات کسب‌وکار	امنیت منابع انسانی	آیین کار کارکنان	الف ـ۷ امنیت منابع انسانی
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	پلت فرم مدیریت رویدادها و اطلاعات امنیتی(SIEM)	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	رویداد کاوی	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	پایش پایگاه داده	الف ـ۱۲ امنیت عملیات

حوزه	مؤلفه‌ی امنیتی سطح بالا	مؤلفه‌ی امنیتی سطح متوسط	حوزه‌ی کنترلی ISO/IEC ۲۷۰۰۱:۲۰۱۳
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	پایش برنامه‌های کاربردی Honey Pot	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	پایش نقطه‌ی انتهایی	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	وابستگی رویدادها	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	پایش ابر	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	رویدادنگاری ایمیل	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	جاسوسی سایبری	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	مدیریت تهدیدات	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	پورتال مرکز عملیات امنیت (SOC)	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	سرویس‌های امنیت (برون‌سپاری شده) مدیریت‌شده	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	پایگاه دانش	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	محافظت از اعتبار و برند	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	Anti-Phishing	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	دفاع داخل شبکه‌ی زمان واقعی ـ پروتکل	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	خودکار امنیت محتوی (SCAP)	الف ـ۱۲ امنیت عملیات
سرویس‌های پشتیبان عملیات کسب‌وکار	پایش امنیت	الگوی رفتاری کاربر	الف ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	حفاظت از داده‌ها	مدیریت چرخه‌ی عمر داده	الف ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	حفاظت از داده‌ها	جلوگیری از نشت داده	الف ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	حفاظت از داده‌ها	حفاظت از حق مالکیت فکری	الف ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	حفاظت از داده‌ها	سرویس‌های رمزنگاری	الف‌ـ۱۰ رمزنگاری
عملیات و پشتیبانی فناوری اطلاعات	عملیات فناوری اطلاعات	طرح بازگشت از حادثه	الف‌ـ۱۶ مدیریت حوادث امنیت اطلاعات
عملیات و پشتیبانی فناوری اطلاعات	عملیات فناوری اطلاعات	طرح بازگشت از حادثه	الف‌ـ۱۶ مدیریت حوادث امنیت اطلاعات
عملیات و پشتیبانی فناوری اطلاعات	عملیات فناوری اطلاعات	حاکمیت فناوری اطلاعات	الف‌ـ۱۶ مدیریت حوادث امنیت اطلاعات
عملیات و پشتیبانی فناوری اطلاعات	عملیات فناوری اطلاعات	مدیریت منابع	الف‌ـ۸ مدیریت دارایی
عملیات و پشتیبانی فناوری اطلاعات	عملیات فناوری اطلاعات	دفتر مدیریت پروژه	الف‌ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	تحویل سرویس	مدیریت سطح سرویس	الف‌ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	تحویل سرویس	تحلیل بازگشت‌پذیری فناوری اطلاعات	الف‌ـ۱۷ جنبه‌های امنیت اطلاعات در مدیریت تداوم کسب‌وکار
عملیات و پشتیبانی فناوری اطلاعات	تحویل سرویس	مدیریت دارایی‌ها	الف‌ـ۸ مدیریت دارایی
عملیات و پشتیبانی فناوری اطلاعات	تحویل سرویس	پایش عملکرد برنامه‌های کاربردی	الف‌ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	پشتیبانی سرویس	مدیریت پیکربندی	الف‌ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	پشتیبانی سرویس	مدیریت حوادث	الف‌ـ۱۶ مدیریت حوادث امنیت اطلاعات
عملیات و پشتیبانی فناوری اطلاعات	پشتیبانی سرویس	مدیریت مسئله	الف‌ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	پشتیبانی سرویس	مدیریت دانش	الف‌ـ۱۲ امنیت عملیات
عملیات و پشتیبانی فناوری اطلاعات	پشتیبانی سرویس	مدیریت تغییرات	الف‌ـ۱۴ اکتساب،توسعه و نگهداری سامانه
عملیات و پشتیبانی فناوری اطلاعات	پشتیبانی سرویس	مدیریت Release	الف‌ـ۱۴ اکتساب،توسعه و نگهداری سامانه
سرویس‌های ارائه	نوع سرویس	سکوی سرویس مصرف‌کننده	الف‌ـ۱۳ امنیت ارتباطات
سرویس‌های ارائه	نوع سرویس	سکوی سرویس سازمانی	الف‌ـ۱۳ امنیت ارتباطات
سرویس‌های ارائه	سکوی ارائه	نقاط انتهایی	الف‌ـ۱۳ امنیت ارتباطات
سرویس‌های ارائه	سکوی ارائه	نقاط انتهایی	الف‌ـ۱۳ امنیت ارتباطات
سرویس‌های ارائه	سکوی ارائه	Speech Recognition(IVR)	الف‌ـ۱۳ امنیت ارتباطات
سرویس‌های ارائه	سکوی ارائه	Handwriting(ICR)	الف‌ـ۱۳ امنیت ارتباطات

حوزه	مؤلفه‌ی امنیتی سطح بالا	مؤلفه‌ی امنیتی سطح متوسط	حوزه‌ی کنترلی ISO/IEC ۲۷۰۰۱:۲۰۱۳
سرویس‌های برنامه کاربردی	اتصال و یکپارچه‌سازی	واسطهای برنامه‌نویسی	الف_۱۴ اکتساب،توسعه و نگهداری سامانه
سرویس‌های برنامه کاربردی	چرخه حیات دانش امنیتی	الگوهای طراحی امنیت	الف_۱۲ امنیت عملیات
سرویس‌های برنامه کاربردی	چرخه حیات دانش امنیتی	الگوهای حمله	الف_۱۲ امنیت عملیات
سرویس‌های برنامه کاربردی	چرخه حیات دانش امنیتی	نمونه کدها	الف_۱۲ امنیت عملیات
سرویس‌های برنامه کاربردی	چرخه حیات دانش امنیتی	چارچوب امنیت برنامه کاربردی-ACEGI	الف_۱۲ امنیت عملیات
سرویس‌های برنامه کاربردی	اتصال و یکپارچه‌سازی	یکپارچه‌سازی میان‌افزارها	الف_۱۲ امنیت عملیات
سرویس‌های برنامه کاربردی	اتصال و یکپارچه‌سازی	برقراری اتصال و تحویل	الف_۱۲ امنیت عملیات
سرویس‌های برنامه کاربردی	اتصال و یکپارچه‌سازی	انتزاع (زبان ارتباطی مشترک)	الف_۱۲ امنیت عملیات
سرویس‌های برنامه کاربردی	فرایندهای توسعه	تضمین کیفیت نرم‌افزار	الف_۱۴ اکتساب،توسعه و نگهداری سامانه
سرویس‌های برنامه کاربردی	فرایندهای توسعه	امنیت مرور کد	الف_۱۴ اکتساب،توسعه و نگهداری سامانه
سرویس‌های برنامه کاربردی	فرایندهای توسعه	پویش آسیب‌پذیری برنامه کاربردی	الف_۱۲ امنیت عملیات
سرویس‌های برنامه کاربردی	فرایندهای توسعه	آزمون استرس و حجم کاری قابل بارگذاری	الف_۱۲ امنیت عملیات
سرویس‌های اطلاعاتی	مدیریت داده‌های امنیتی تولید شده	حفظ سوابق	الف_۱۸ انطباق
سرویس‌های اطلاعاتی	سرویس‌های گزارش دهی	داشبورت داشبورد	الف_۱۶ مدیریت حوادث امنیت اطلاعات
سرویس‌های اطلاعاتی	سرویس‌های گزارش دهی	داده‌کاوی	الف_۱۶ مدیریت حوادث امنیت اطلاعات
سرویس‌های اطلاعاتی	سرویس‌های گزارش دهی	ابزارهای گزارش‌گیری	الف_۱۶ مدیریت حوادث امنیت اطلاعات
سرویس‌های اطلاعاتی	سرویس‌های گزارش دهی	هوش کسب‌وکار	الف_۱۶ مدیریت حوادث امنیت اطلاعات
سرویس‌های زیرساخت	زیرساخت داخلی	امنیت تجهیزات	الف_۱۱ امنیت فیزیکی و محیطی
سرویس‌های زیرساخت	زیرساخت داخلی	مدیریت ریسک محیطی	الف_۱۱ امنیت فیزیکی و محیطی
سرویس‌های زیرساخت	زیرساخت داخلی	سرویس‌های ذخیره‌سازی	الف_۱۱ امنیت فیزیکی و محیطی
سرویس‌های زیرساخت	زیرساخت داخلی	سرویس‌های شبکه	الف_۱۱ امنیت فیزیکی و محیطی
سرویس‌های زیرساخت	زیرساخت داخلی	سرویس‌های شبکه	الف_۱۱ امنیت فیزیکی و محیطی
سرویس‌های زیرساخت	زیرساخت داخلی	نگهداری تجهیزات	الف_۱۱ امنیت فیزیکی و محیطی
سرویس‌های زیرساخت	زیرساخت داخلی	سرورها	الف_۱۱ امنیت فیزیکی و محیطی
سرویس‌های زیرساخت	زیرساخت داخلی	نقاط انتهایی	الف_۱۱ امنیت فیزیکی و محیطی
سرویس‌های زیرساخت	زیرساخت داخلی	سرویس‌های دسترس‌پذیری	الف_۱۱ امنیت فیزیکی و محیطی
سرویس‌های زیرساخت	زیرساخت مجازی	مجازی‌سازی کلاینت و دسک تاپ	الف_۱۲ امنیت عملیات /الف_۱۳ امنیت ارتباطات
سرویس‌های زیرساخت	زیرساخت مجازی	مجازی‌سازی برنامه کاربردی	الف_۱۲ امنیت عملیات /الف_۱۳ امنیت ارتباطات
سرویس‌های زیرساخت	زیرساخت مجازی	فضای کاری مجازی	الف_۱۲ امنیت عملیات /الف_۱۳ امنیت ارتباطات
سرویس‌های زیرساخت	زیرساخت مجازی	مجازی‌سازی ذخیره‌سازی	الف_۱۲ امنیت عملیات /الف_۱۳ امنیت ارتباطات
سرویس‌های زیرساخت	زیرساخت مجازی	مجازی‌سازی سرور	الف_۱۲ امنیت عملیات /الف_۱۳ امنیت ارتباطات
سرویس‌های زیرساخت	زیرساخت مجازی	شبکه	الف_۱۲ امنیت عملیات /الف_۱۳ امنیت ارتباطات
سرویس‌های زیرساخت	زیرساخت مجازی	مجازی‌سازی پایگاه داده	الف_۱۲ امنیت عملیات /الف_۱۳ امنیت ارتباطات
سرویس‌های زیرساخت	زیرساخت مجازی	مجازی‌سازی تجهیزات موبایل	الف_۱۲ امنیت عملیات /الف_۱۳ امنیت ارتباطات
سرویس‌های زیرساخت	زیرساخت مجازی	مجازی‌سازی کارت هوشمند	الف_۱۲ امنیت عملیات /الف_۱۳ امنیت ارتباطات

جدول ۴: نگاشت مؤلفه‌های امنیتی سطح اول و دوم به حوزه‌های کنترلی ISO/IEC 27001:2013