الزامات امنیتی رایانش ابری

براساس ماتریس کنترل‌های ابری (CCM)

Cloud Security Requirements (CSR)

نسخه CSR-98-0.6

مرکز آپا دانشگاه زنجان

فهرست مطالب

۱ – مروری بر مفاهیم و معماری رایانش ابری

در این بخش چارچوب و معماری رایانش ابری که براساس آن الزامات امنیتی شکل گرفته و تعریف می‌شوند به طور مختصر بیان می‌گردد. با توجه به گستردگی رایانش ابری، از منظرهای مختلفی به این موضوع توجه شده است. در حقیقت رایانش ابری یک فناوری مشتمل بر مجموعه‌ای از فناوری‌ها، مدل عملیاتی و مدل تجاری می‌باشد.

رایانش ابری فواید بالقوه‌ی فراوانی در ابعاد مختلف از جمله چابکی، استحکام و اقتصادی ایجاد کرد. سازمان‌ها با حضور رایانش ابری توانستند وظایف خود را سریع‌تر و با زمان خرابی بسیار کمتر از گذشته انجام دهند. علاوه براین از منظر امنیتی نیز امکان ارتقاء امنیت و همچنین انجام سریع‌تر طرح استمرار کسب و کار و بازگرداندن اطلاعات تخریب شده فراهم شد.

پیش از بیان الزامات امنیتی رایاناش ابری، ضروری است تعریف دقیق رایانش ابری، مدل منطقی آن، مدل مرجع و معماری و همچنین دامنه‌ی امنیتی مرتبط با آن به درستی تبیین شود.

۱-۱- تعریف رایانش ابری

براساس تعریف، رایانش ابری یک مدل عملیاتی جدید و مجموعه‌ای از فناوری‌ها برای مدیریت منابع محاسباتی اشتراکی می‌باشد. فناوری رایانش ابری به طور بالقوه با تقویت ویژگی‌هایی مانند همکاری[1]، چابکی[2]، مقایس‌پذیری و دسترس‌پذیری امکان کاهش هزینه‌ها و بهینه‌سازی محاسبات را فراهم می‌کند. انستیتوی NIST رایانش ابری را این‌گونه تعریف می‌کند: "رایانش ابری مدلی است که امکان دسترسی مناسب شبکه براساس نیاز و از همه‌ی نقاط به مخزنی از منابع محاسباتی اشتراکی را با پیکربندی‌های متعدد فراهم می‌کند به گونه‌ای که این دسترسی‌ها و امکانات می‌توانند با حداقل سربار مدیریتی و حداقل تعامل با فراهم‌کنندگان سرویس و با سرعت تهیه و در اختیار مشتریان قرار بگیرند. به عنوان مثال سرویس‌دهنده‌ها، شبکه‌ها، فضاهای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها به

[1] Collaboration

[2] Agility

عنوان منابع اشتراکی می‌توانند در بستر رایانش ابری در دسترس قرار بگیرند."

تفاوت ماهوی رایانش ابری با مجازی‌سازی سنتی در مدل ارائه‌ی سرویس است. مجازی‌سازی منابع را به صورت انتزاعی ارائه می‌دهد بدون آنکه مدلی از مخزن اشتراکی معرفی کند که در آن به صورت خودکار و براساس نیاز به مشتریان سرویس ارائه گردد. در مقابل طبیعت رایانش ابری و طراحی ذاتی آن چندمستاجری[1] می‌باشد. در این مدل چندین مصرف‌کننده مخزنی مشترک از منابع را که از همدیگر تفکیک شده و نسبت به یکدیگر ایزوله می‌باشد مورد بهره‌برداری قرار می‌دهند.

۲-۱- مدل تعریفی

انستیتوی معاهده‌ی امنیت ابر (CSA[2])، از مدل NIST به عنوان مدل استاندارد رایانش ابری استفاده می‌کند. NIST رایانش ابری را براساس پنج خصوصیت اساسی، سه مدل سرویس ابر، و چهار مدل استقرار ابر تعریف می‌کند. شکل ۱-۱ این مطلب را نشان می‌دهد.

۱-۲-۱- خصیصه‌های اساسی

منظور از خصیصه‌های اساسی، ویژگی‌هایی هستند که یک ابر را به عنوان ابر مطرح می‌کنند و نبود هر کدام از آنها، فلسفه‌ی ابر را زیرسوال می‌برد. این خصیصه‌ها عبارتند از:

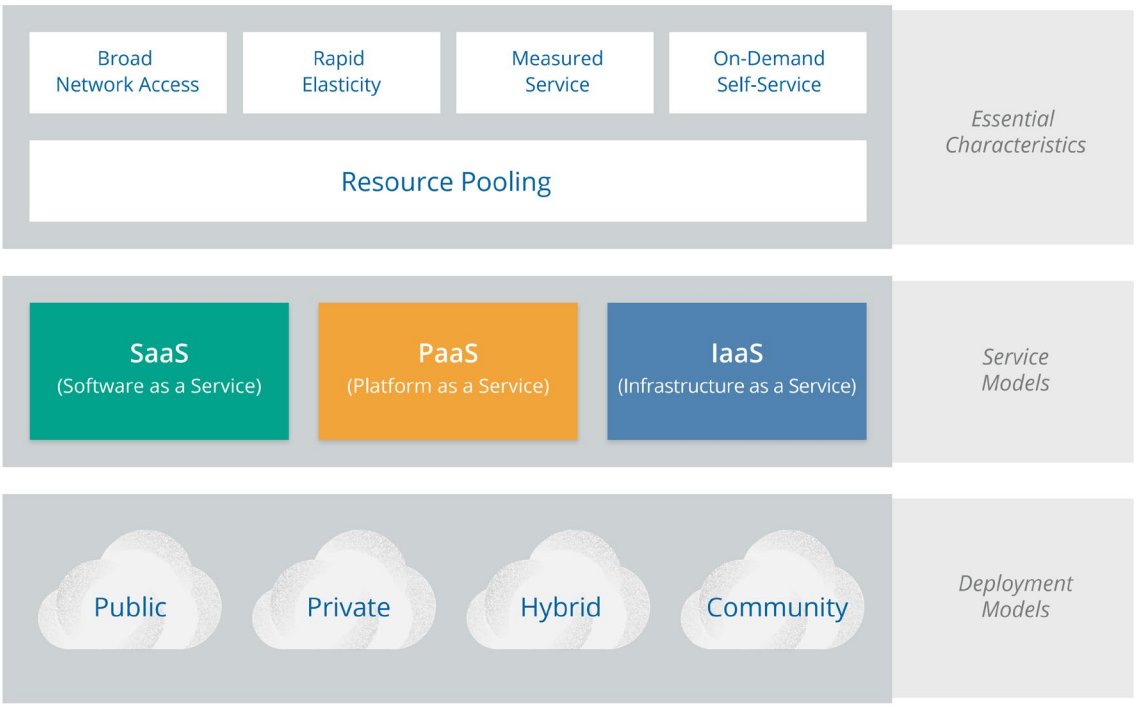
- **مخزن منبع**[3] اصلی‌ترین ویژگی مدل ابر است. فراهم‌کنندگان منابع را به صورت انتزاعی ارائه می‌دهند و آنها را در قالب یک مخزن تجمیع می‌کنند.
- مصرف‌کنندگان، منابع را از مخزن با استفاده از **سلف‌سرویس مبتنی بر نیاز**[4] تهیه می‌کنند. آنها منابع خود را بدون نیاز به تعامل با مدیران فنی و توسط خودشان مدیریت می‌کنند.

[1] Multitenant

[2] Cloud Security Alliance (CSA)

[3] Resource Pooling

[4] On-Demand Self-Service



شکل ۱-۱- مدل رایانش ابری NIST

- **دسترسی شبکه‌ی گسترده**[1] بدین معناست که همه‌ی منابع از طریق شبکه و بدون نیاز به دسترسی فیزیکی مستقیم در دسترس هستند.
- **قابلیت ارتجاعی سریع**[2] به مصرف‌کنندگان اجازه می‌دهد که منابع را به صورت خودکار و براساس نیاز گسترش دهند.
- **سرویس اندازه‌گیری**[3] آنچه را که برای مصرف‌کنندگان فراهم می‌شود به خوبی می‌سنجد.

۲-۲-۱- مدل‌های سرویس

براساس تعریف NIST سه مدل سرویس ابری تعریف می‌شود که عبارتند از:

- **نرم‌افزار به عنوان سرویس (SaaS)**[4] یک برنامه‌ی کاربردی کامل است که توسط فراهم‌کننده‌ی سرویس میزبانی و مدیریت می‌شود. مصرف‌کنندگان به آن از طریق مرورگر وب، برنامه‌ی موبایل، یا

[1] Broad Network Access
[2] Rapid Elasticity
[3] Measured Service
[4] Software as a Service (SaaS)

یک برنامه‌ی سمت مشتری سبک متصل می‌شوند.

- **سکو به عنوان سرویس (PaaS[1])**، سکوهای برنامه و توسعه مانند پایگاه داده‌ها، سکوهای اجرایی (به عنوان مثال مکانی برای اجرای پایتون، PHP و سایر کدها)، ذخیره‌سازی فایل و حتی امکان پردازشی مانند یادگیری ماشین و پردازش کلان داده را فراهم می‌کنند.
- **زیرساخت به عنوان سرویس (IaaS[2])**، امکان دسترسی به مخزن منابع مانند محاسبه، شبکه و ذخیره‌سازی را فراهم می‌کند.

۳-۲-۱- مدل‌های استقرار

مدل‌های استقرار در رایانش ابری، چهار نوع است. این مدل‌ها عبارتند از:

- **ابر عمومی[3]**: زیرساخت ابر که برای عموم و یا یک گروه بزرگ صنعتی فراهم می‌شود و متعلق به سازمانی است که سرویس‌های ابر را می‌فروشد.
- **ابر خصوصی[4]**: زیرساخت ابری که فقط برای یک سازمان عملیاتی می‌شود. این نوع ابر توسط همان سازمان یا یک شخص ثالث مدیریت می‌شود.
- **ابر جامعه[5]**: زیرساخت ابری که توسط چندین سازمان به اشتراک گذاشته می‌شود و از یک جامعه‌ی مشخصی که مسائل مشترک (از جمله ماموریت، نیازمندی‌های امنیتی و سیاست) دارند پشتیبانی می‌کند.
- **ابر ترکیبی[6]**: زیرساخت ابری که ترکیبی از چند مدل ابر (عمومی، خصوصی و جامعه) می‌باشد.

این مدل‌ها براساس کاربر رایانش ابری و اینکه چه کسانی از آن بهره می‌برند تعریف می‌شود. همانطور که دیاگرام شکل ۲-۱ نشان می‌دهد، سازمان‌هایی که رایانش ابری را مدیریت می‌کنند مدل استقرار

---

[1] Platform as a Service (PaaS)

[2] Infrastructure as a Service (IaaS)

[3] Public Cloud

[4] Private Cloud

[5] Community Cloud

[6] Hybrid Cloud

بسیار متفاوتی نسبت به ساختارهای منفرد دارند.

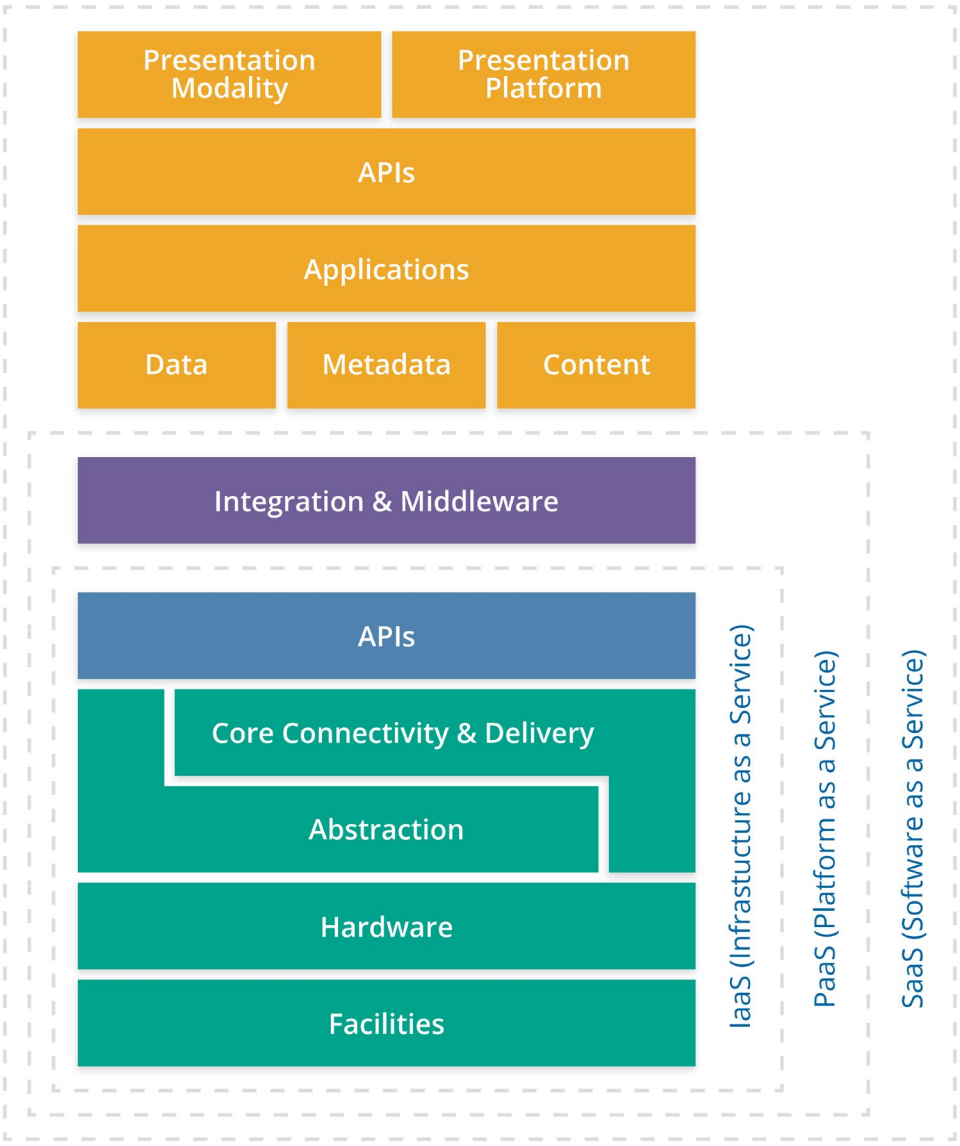
	Infrastructure Owned By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third-Party Provider	Third-Party Provider	Off-Premises	Untrusted
Private/ Community	Organization / Third-Party Provider	Organization / Third-Party Provider	On-Premises / Off-Premises	Trusted
Hybrid	Both Organization & Third-Party Provider	Both Organization & Third-Party Provider	Both On-Premises & Off-Premises	Trusted & Untrusted

[1] Management includes: governance, operations, security, compliance, etc...
[2] Infrastructure implies physical infrastructure such as facilities, compute network and storage equipment
[3] Infrastructure location is both physical relative to an organization's management umbrella and speaks to ownership versus control
[4] Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, and business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

شکل ۲-۱- دیاگرام استقرار متناسب با کاربران رایانش ابری

۳-۱- مدل‌های معماری و مرجع

هدف از این بخش ارائه‌ی مدلی برای بیان برخی اصول و موارد پایه است که بتوان توسط آنها به متخصصان امنیت جهت ارتقاء امنیت رایانش ابری کمک رساند. یکی از مدل‌های معمول، بیان رایانش ابری به صورت پشته‌ای از مدل‌های سرویس می‌باشد به گونه‌ای که SaaS روی PaaS و PaaS هم روی IaaS بنا شود. شکل ۳-۱ معماری مورد نظر را برای رایانش ابری نشان می‌دهد.



شکل ۳-۱- معماری رایانش ابری براساس پشته‌ی مدل‌های سرویس

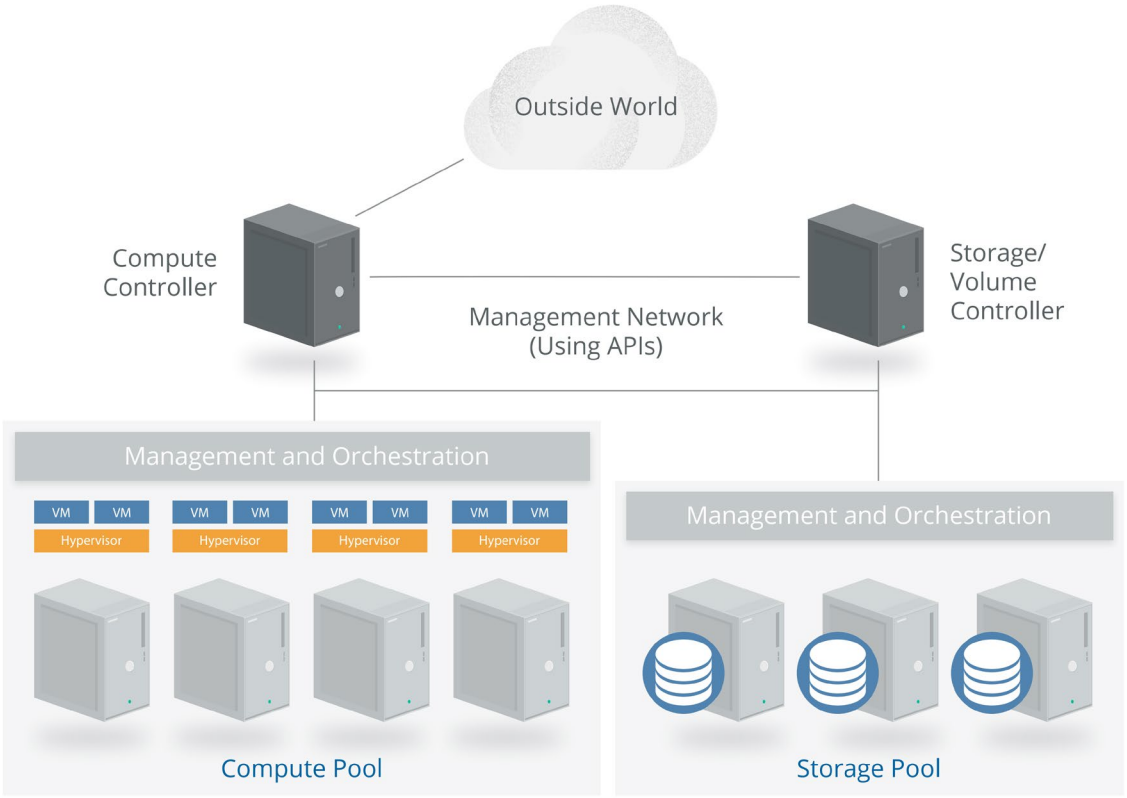
در ادامه هر کدام از مدل‌های سرویس در معماری مورد نظر تشریح می‌شوند.

۱-۳-۱- زیرساخت به عنوان سرویس (IaaS)

امکانات (Facilities) فیزیکی و سخت‌افزار (Hardware) زیرساخت، سنگ بنای IaaS می‌باشند. هر چند با رایانش ابری این منابع به صورت انتزاعی و در قالب مخزن منابع ارائه می‌شوند، اما در سطح پایه برای ساخت رایانش ابری به سخت‌افزارهای فیزیکی، شبکه‌ها و تجهیزات ذخیره‌سازی نیازمند هستیم.

توسط انتزاع (Abstraction)، همان مجازی‌سازی، منابع از محدودیت‌های فیزیکی خود خلاص

می‌شوند تا امکان ایجاد مخزن منابع فراهم شود. سپس مجموعه‌ای از ابزارهای تحویل و اتصال مرکزی (Core Connectivity & Delivery) یا همان Orchestration این منابع را به هم گره می‌زند، از آنها مخزن ایجاد می‌کند، و امکان ارائه‌ی خودکار آنها به مشتریان را فراهم می‌کند. همه‌ی این موارد توسط رابط‌های برنامه‌نویسی کاربردی (API) در معرض گذاشته می‌شود. APIها یک روش ارتباطی اصولی برای مولفه‌های درونی یک ابر می‌باشند. شکل ۴-۱ یک مثال محاسباتی ساده از معماری IaaS را نشان می‌دهد.

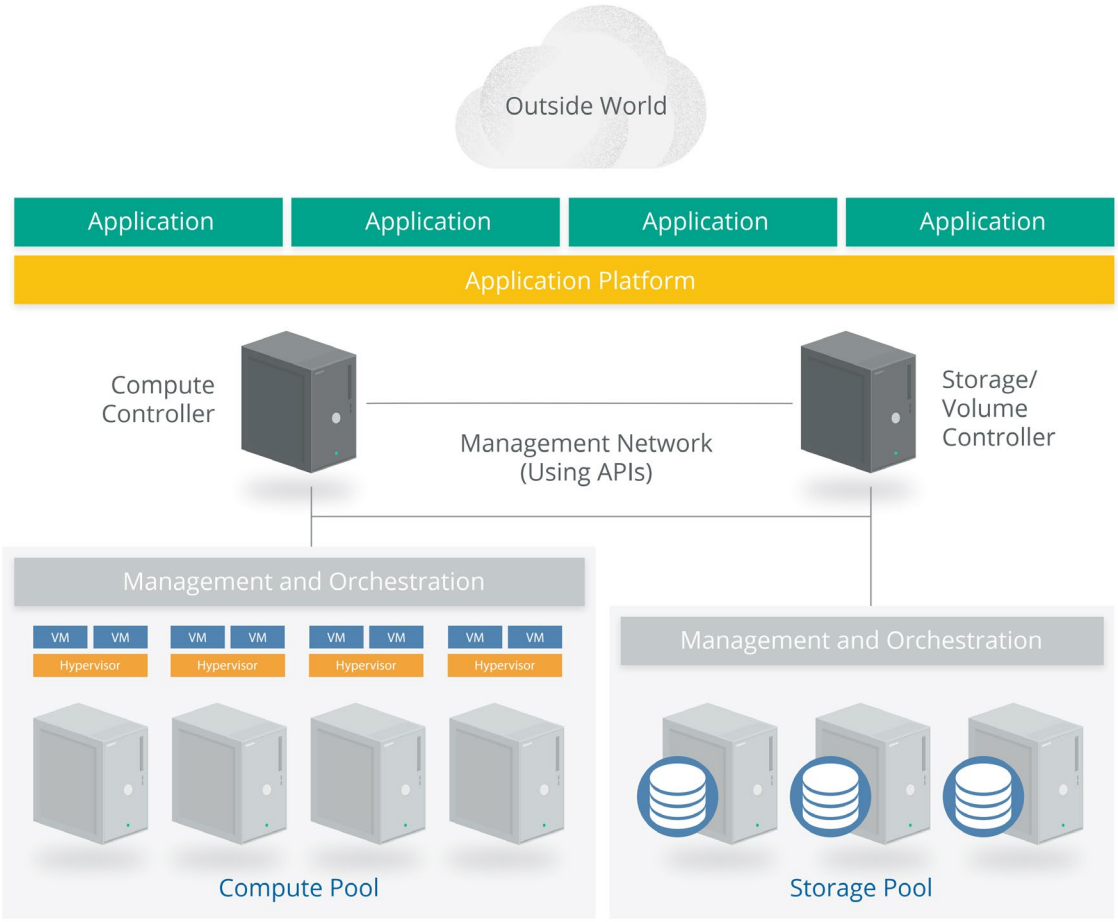


شکل ۴-۱- یک مدل معماری ساده از سکوی IaaS محاسباتی

۲-۳-۱- سکو به عنوان سرویس (PaaS)

مدل سرویس PaaS، یک لایه‌ی مازاد تجمیعی با چارچوب‌های توسعه‌ای، قابلیت‌های میان‌افزاری، و توابعی (Integration & Middleware) همچون پایگاه داده‌ها، پیام‌رسانی، و صف‌ها اضافه می‌کند. این سرویس‌ها به توسعه‌دهندگان اجازه می‌دهند که برنامه‌های خود را روی سکوی ابزارها و زبان‌های برنامه‌نویسی که توسط این پشته ارائه می‌شود بسازند. شکل ۵-۱ نمونه‌ای از معماری PaaS را که بر

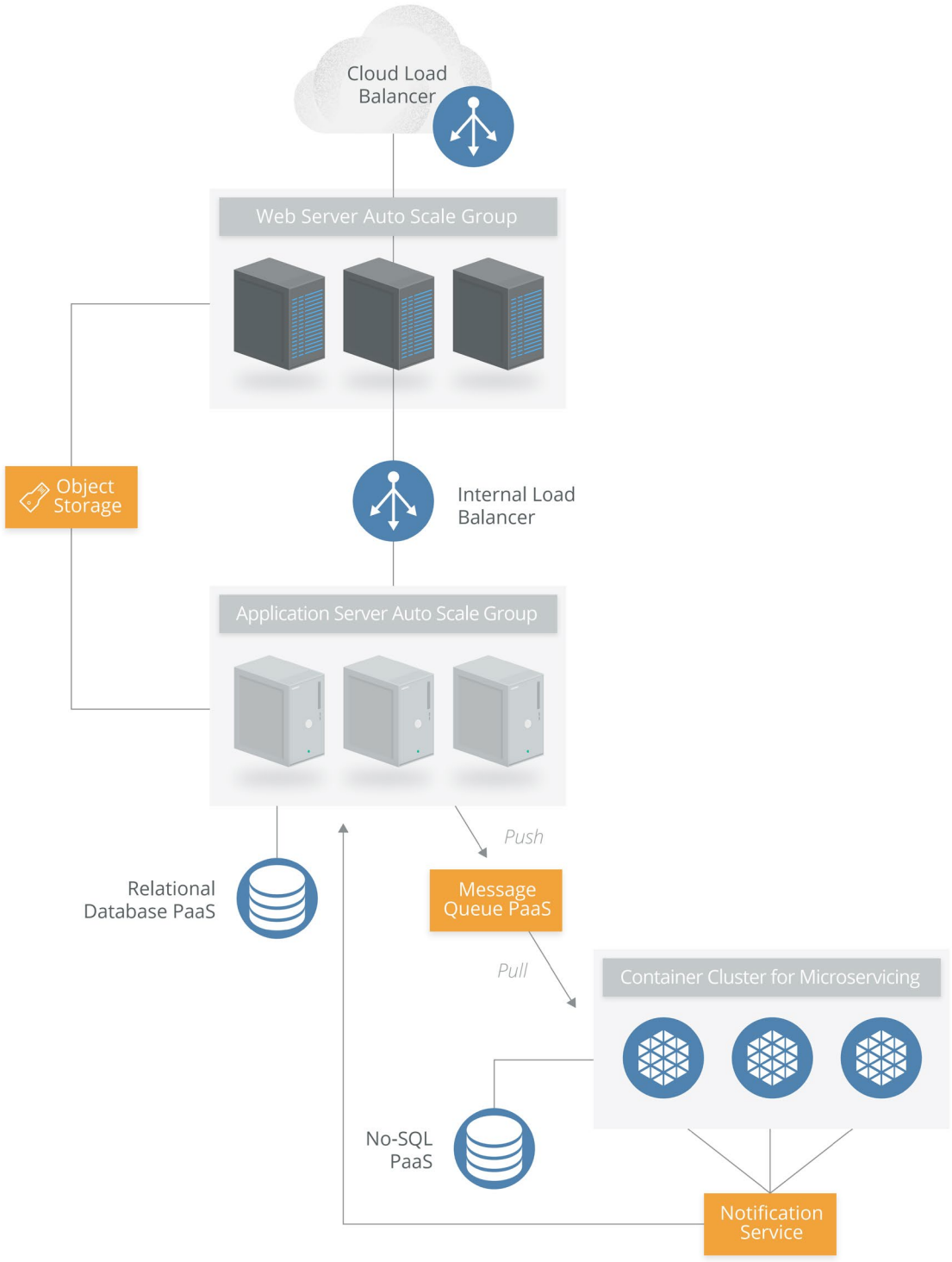
روی مدل معماری IaaS مستقر شده‌است نشان می‌دهد.



شکل ۵-۱-معماری PaaS بر روی مدل معماری IaaS

۳-۳-۱- نرم‌افزار به عنوان سرویس (SaaS)

سرویس‌های SaaS در حقیقت برنامه‌های کاربردی چندمستاجری با همه‌ی پیچیدگی‌های معماری از سکوی نرم‌افزاری می‌باشند. بسیاری از فراهم‌کنندگان سرویس SaaS، برای افزایش چابکی، مقاومت و فواید اقتصادی، آن را بر روی IaaS و PaaS بنا می‌کنند. دیاگرام معماری ارائه شده در شکل ۶-۱ یک سکوی واقعی SaaS را نشان می‌دهد.



شکل ۶-۱- نمونه‌ای واقعی از سکوی SaaS

۴-۱- مدل منطقی

در سطح بالا، هر دو مدل رایانش ابری و روش‌های محاسباتی مرسوم، از یک مدل منطقی تبعیت

می‌کنند که توجه به آن باعث شناخت لایه‌های متفاوتی مبتنی بر وظیفه‌مندی می‌شود، که این مساله در تشریح تفاوت‌های دو مدل محاسباتی نیز موثر و مفید است. این مدل منطقی دارای اجزای زیر است:

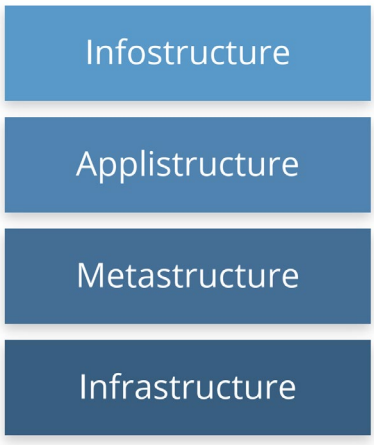
- زیرساخت: مولفه‌های مرکزی یک سیستم محاسباتی را می‌گویند که شامل "محاسبه"، "شبکه" و "ذخیره‌سازی" می‌باشد.
- متاساخت[1]: پروتکل‌ها و مکانیسم‌هایی که رابط بین لایه‌ی زیرساخت و سایر لایه‌ها را فراهم می‌کند. این لایه در حقیقت وظیفه اتصال فناوری‌ها به همدیگر را دارد و امکان مدیریت و پیکربندی را فراهم می‌کند.
- داده‌ساخت[2]: داده‌ها، اطلاعات، محتوای یک پایگاه داده، ذخیره‌سازی فایل و موارد مشابه مربوط به این لایه است.
- برنامه‌ساخت[3]: برنامه‌هایی که در ابر مستقر می‌شوند و سرویس‌های کاربردی که برای ساخت آن برنامه‌ها مورد استفاده قرار می‌گیرند در این لایه می‌گنجد.

از منظر امنیت، مکانیسم‌های امنیتی متفاوتی به هر کدام از لایه‌های منطقی نگاشت می‌شود. به عنوان مثال امنیت برنامه به لایه‌ی "برنامه‌ساخت"، امنیت داده به لایه‌ی "داده‌ساخت" و امنیت زیرساخت به لایه‌ی "زیرساخت" نگاشت می‌شود. تفاوت کلیدی رایانش ابری با مدل‌های محاسباتی مرسوم در لایه‌ی "متاساخت" می‌باشد. متاساخت ابر شامل مولفه‌های سطح مدیریت با قابلیت شبکه و دسترسی از راه دور می‌باشد. در شکل ۷-۱ لایه‌های منطقی نشان داده شده اند.

[1] Metastructure

[2] Infostructure

[3] Applistructure



شکل ۷-۱-لایه‌های منطقی مدل‌های محاسباتی

۱-۵- محدوده‌ی امنیت ابر، مسئولیت‌ها، و مدل‌ها

پس از معرفی مختصر ساختار رایانش ابری، در این بخش شاکله‌ی امنیت رایانش ابری بیان می‌شود تا براساس آن بتوان الزامات امنیتی رایانش ابری را برشمرد.

۱-۵-۱- امنیت ابر، محدوده‌ی تطبیق و مسئولیت‌ها

در حالیکه محدوده‌ی کلی امنیت و تطبیق[1] رایانش ابری تغییر نمی‌کند اما هر قسمت از ابر مسئول امنیت همان قسمت است. در نتیجه، مسئولیت‌های امنیتی در سرتاسر پشته‌ی مدل‌های سرویس و سازمان‌ها توزیع می‌شود.

- امنیت از منظر SaaS: فراهم‌کننده‌ی ابر تقریبا مسئول تمام امنیت ابر است. از این رو، کاربر ابر فقط می‌تواند نحوه‌ی استفاده از برنامه‌ها را مدیریت کند و به آنها دسترسی پیدا کند و نمی‌تواند چگونگی عملکرد برنامه‌ها را تغییر دهد. به عنوان مثال فراهم‌کننده‌ی SaaS مسئول امنیت محیطی، رخدادنگاری/نظارت/وارسی و امنیت برنامه می‌باشد در حالیکه که مصرف کننده تنها قادر به مدیریت مجوزها و حقوق کاربران است.
- امنیت از منظر PaaS: فراهم‌کننده‌ی ابر مسئول امنیت سکو می‌باشد، در حالیکه مصرف‌کننده

[1] Compliance

مسئول هر چیزی است که روی سکو پیاده‌سازی می‌شود. به عنوان مثال هنگام استفاده از پایگاه داده به عنوان سرویس، فراهم‌کننده‌ی سرویس مسئول مدیریت امنیت زیربنایی، وصله‌ها و پیکربندی هسته‌ی مرکزی است در حالیکه کاربر ابر مسئول چیزهای دیگر از جمله ویژگی‌های امنیتی مورد استفاده در پایگاه داده، مدیریت اکانت‌ها و روش‌های احراز اصالت می‌باشد.

- امنیت از منظر IaaS: مشابه با PaaS، فراهم‌کننده‌ی ابر مسئول امنیت زیربنایی زیرساخت می‌باشد، در حالیکه کاربر ابر مسئول هر چیزی است که روی زیرساخت پیاده‌سازی می‌شود. برخلاف PaaS، در این بخش بیشتر مسئولیت بر گردن سرویس‌گیرندگان می‌افتد. به عنوان مثال فراهم‌کننده‌ی IaaS با نظارت بر محیط، حملات را شناسایی می‌کند، اما مصرف‌کننده به طور کامل مسئول نحوه‌ی تعریف و پیاده‌سازی امنیت شبکه‌ی مجازی مبتنی بر ابزارهای موجود بر روی سرویس می‌باشد.

شکل ۸-۱ نحوه‌ی توزیع مسئولیت را بین سه مدل سرویس نشان می‌دهد.

شکل ۸-۱-نحوه‌ی توزیع مسئولیت‌ها بین مدل‌های سرویس

مهم‌ترین مساله‌ی امنیت در رایانش ابری عبارت است از شناخت دقیق اینکه هر کس مسئول چه بخشی از پروژه‌ی رایانش ابری می‌باشد. بنابراین رابطه‌ی امنیتی فی مابین فراهم‌کننده‌ی ابر و مصرف‌کننده مساله‌ی اساسی است.

فراهم‌کنندگان سرویس، بایستی به طور واضح کنترل‌های امنیتی داخلی و ویژگی‌های امنیتی مشتری را مستند کنند، به گونه‌ای که کاربر ابر بتواند یک تصمیم آگاهانه اتخاذ کند. همچنین فراهم‌کنندگان سرویس بایستی به طور مناسب کنترل‌های امنیتی را طراحی و پیاده‌سازی کنند.

از طرف دیگر کاربران ابر باید یک ماتریس مسئولیت‌ها برای مستندسازی اینکه چه کسی، چگونه و

با چه کنترل‌هایی پیاده‌سازی را انجام می‌دهد. انستیتوی معاهده‌ی امنیت ابر دو ابزار برای بیان الزامات امنیتی معرفی کرده است. ابزار CAIQ[1] یک قالب استاندارد برای فراهم‌کنندگان سرویس در راستای مستندسازی کنترل‌های تطبیق و امنیتی ایشان می‌باشد. ابزار دیگر CCM[2] است که فهرستی از کنترل‌های امنیتی به همراه نگاشت آنها به سایر استانداردها را ارائه می‌دهد. در این مستند الزامات امنیتی براساس کنترل‌های ارائه شده‌ی CCM بیان می‌شوند.

۲ – الزامات امنیتی مبتنی بر CCM

همانطور که بیان شد CCM فهرستی از کنترل‌های امنیتی به همراه نگاشت آنها به سایر استانداردها را ارائه می‌دهد. در این مستند الزامات امنیتی براساس کنترل‌های ارائه شده‌ی CCM بیان می‌شوند. CCM شامل دامنه‌های مختلفی است که به طور کلی به دو دسته‌ی حاکمیتی و عملیاتی تقسیم می‌شوند. دسته‌ی حاکمیتی شامل دامنه‌های است که مسائل استراتژیک و سیاست‌ها را مشخص می‌کند در حالیکه که دامنه‌های عملیاتی متمرکز بر روی مسائل امنیتی تاکتیکی و نحوه‌ی پیاده‌سازی آنها در معماری می‌باشد. ابزار CCM برای ارزیابی یک ماتریس ارائه می‌دهد که در آن دامنه‌ها به همراه الزامات هر کدام بیان می‌شوند. در ادامه دامنه‌های مختلف به همراه الزامات آنها که در ماتریس CCM نسخه 3.0.1 (آخرین نسخه تا تاریخ ۲۰۲۰/۱/۱۸) از طرف CSA ارائه شده است آمده است.

۲-۱- امنیت برنامه و رابط‌های برنامه‌نویسی

اولین بخش از ماتریس CCM بیانگر امنیت برنامه و رابط‌های برنامه‌نویسی (AIS[3]) می‌باشد. امن‌سازی برنامه‌ها و رابط‌ها که بر روی ابر اجرا یا توسعه داده می‌شوند، بسیار حائز اهمیت است. جدول زیر

[1] Consensus Assessments Initiative Questionnaire (CAIQ)

[2] Cloud Controls Matrix (CCM)

[3] Application & Interface Security (AIS)

الزامات این دامنه را مشخص می‌کند.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
AIS-01	امنیت برنامه	• بایستی برنامه‌ها و رابط‌های برنامه‌نویسی (APIها) براساس آخرین استانداردهای امنیتی مانند OWASP برای برنامه‌های تحت وب، طراحی، پیاده‌سازی، مستقر و آزمون شوند و تعهدات قانونی و نظارتی مربوطه را رعایت نمایند.
AIS-02	نیازمندی‌های دسترسی مشتریان	• بایستی قبل از دسترسی مشتری به داده‌ها، تجهیزات و سیستم‌های اطلاعاتی، الزامات امنیتی و نظارتی برای دسترسی مشتری تعریف و اجرا شود.
AIS-03	جامعیت داده	• باید رویه‌های جامعیت داده‌های ورودی و خروجی (به معنی بررسی‌های لازم در ثبت و ویرایش اطلاعات) برای جلوگیری از خطاهای پردازشی، خرابی و حذف داده‌ها در رابط‌های برنامه‌نویسی و بانک‌های اطلاعاتی پیاده‌سازی شده باشد.
AIS-04	امنیت و جامعیت داده	• برای حمایت از امنیت داده‌ها و فراهم نمودن محرمانگی، جامعیت و دسترس‌پذیری، باید سیاست‌ها و رویه‌های مناسبی تعریف و اجرا شوند تا در دسترسی به داده‌ها از طریق چندین رابط سیستمی و کارکردهای تجاری از افشاء، تغییر و از دست رفتن ناخواسته داده‌ها جلوگیری نمایند.

۲-۲- تضمین ممیزی و تطبیق

تضمین ممیزی و تطبیق (AAC[1]) با طرح‌ریزی امنیتی آغاز می‌شود و هدف از آن اطمینان از اجرای درست فرایندهای ممیزی و تطبیق با کنترل‌ها می‌باشد.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
AAC-01	طرح‌ریزی ممیزی	• طرح‌ریزی ممیزی بایستی برای تعیین مشکلات و اختلالات فرآیندهای کسب‌وکار ایجاد و انجام گیرد. • طرح‌ریزی ممیزی بایستی بر تعیین میزان موثر بودن راهکارهای امنیتی پیاده‌شده تمرکز نماید. • همه اقدام‌های ممیزی قبل از اجرا باید بررسی و مورد تایید قرار

[1] Audit Assurance & Compliance (AAC)

		گیرند.
AAC-02	ممیزی مستقل	• بررسی‌ها و ارزیابی‌های مستقل دوره‌ای حداقل به صورت سالیانه برای بررسی عدم ناسازگاری سیاست‌های اتخاذ شده، استانداردها، روال‌های اجرایی و تعهدات انجام گیرد.
ACC-03	نگاشت نظارتی سیستم اطلاعاتی	• سازمان‌ها باید یک چارچوب کنترلی که استانداردها، نظارت‌ها، قوانین و نیازمندی‌های قانونی مرتبط با الزامات کسب‌وکار را پوشش می‌دهد ایجاد و استفاده نماید. • چارچوب کنترلی بایستی به صورت حداقل سالیانه مورد بررسی قرار گیرد تا آخرین تغییرات مربوط به حوزه کسب‌وکار در آن اعمال شده باشد.

۳-۲- مدیریت تداوم کسب‌وکار و انعطاف‌پذیری عملیاتی

یک چارچوب جامع امنیتی بایستی بتواند قابلیت اطمینان و تداوم سرویس را تضمین کند. بدین منظور در ماتریس CCM یک حوزه به نام BCR که به مدیریت تداوم کسب و کار و انعطاف‌پذیری عملیاتی[1] اشاره دارد تخصیص داده شده است.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
BCR-01	طرح‌ریزی تداوم کسب‌وکار	بایستی چارچوبی برای اطمینان از صحت و سازگاری در طرح‌ریزی تداوم کسب‌وکار ایجاد و مستند شود و به صورتی تدوین شود که اولویت‌های تست، نگهداشت و نیازمندی‌های امنیت اطلاعات را برآورده نماید. نیازمندی‌های مربوط به طرح‌ریزی تداوم کسب‌وکار شامل موارد زیر می‌باشد: • هدف و محدوده براساس وابستگی‌های مربوطه تعریف شده باشد. • توسط کسانی که باید استفاده کنند قابل دسترس و قابل فهم باشد. • به فرد یا افراد مشخصی که مسئولیت بررسی، بروزرسانی و تایید آنرا داشته باشند واگذار شده باشد. • خطوط تعاملی، نقش‌ها و مسئولیت‌ها تعریف شده باشد. • رویه‌های ترمیم، کارهای دستی مربوطه و اطلاعات مراجع با

[1] Business Continuity Management & Operational Resilience (BCR)

		جزئیات آورده شده باشد. • روش‌های بررسی طرح مشخص شده باشد.
BCR-02	آزمون تداوم کسب‌وکار	• طرح تداوم کسب‌وکار و پاسخگویی به رخدادهای امنیتی بایستی در دوره‌های زمانی مشخصی مورد بررسی قرار گیرد و تغییرات سازمانی و محیطی در آن اعمال شوند. • طرح‌های پاسخگویی به رخدادها بایستی مشتریان متاثر شده و سایر کسب‌وکارهای مرتبط را که زنجیره بحرانی داخلی کسب‌وکار به آنها وابسته است را شامل شود.
BCR-03	ابزار مراکز داده/ شرایط محیطی	• خدمات مربوط به ابزارهای مرکز داده و شرایط محیطی مانند برق، آب، دما، ارتباطات تلفنی و اتصال‌های اینترنتی بایستی به صورت دوره‌ای مورد نظارت، آزمون، نگهداشت و بررسی امنیتی قرار گیرند تا از خرابی‌های احتمالی یا صدمات غیرمجاز حفاظت شوند. • طرح‌های اتوماتیکی برای رفع مشکلات حاصل از خرابی‌های احتمالی درنظر گرفته شده باشد.
BCR-04	مستندسازی	مستندسازی سیستم اطلاعاتی (به معنی راهنمای مدیریت و کاربری و نمودارهای معماری سیستم) بایستی برای اهداف زیر در دسترس پرسنل مجاز قرار داشته باشد: • انجام تنظیمات، نصب و عملیاتی کردن سیستم اطلاعاتی • استفاده بهینه از ویژگی‌های امنیتی سیستم
BCR-05	مخاطرات محیطی	• حفاظت فیزیکی در برابر خطرات طبیعی و حملات عمدی شامل آتش‌سوزی، سیل، ساعقه، طوفان، زلزله، سونامی، انفجار ، حادثه هسته‌ای، فعالیت‌های آتشفشانی، خطرات بیولوژیکی، ناآرامی‌های مدنی، ریزش کوه، فعالیت تکتونیکی و اشکال دیگر فاجعه طبیعی یا انسانی باید پیش بینی، طرح ریزی و اقدامات متقابل اعمال شود.
BCR-06	مکان دستگاه‌ها	• برای کاهش خطرات ناشی از تهدیدهای فیزیکی، خطرات و احتمال دسترسی غیرمجاز، تجهیزات باید از مکان‌هایی که در معرض خطرات قرار دارند دور شوند یا توسط تجهیزات اضافی که در فاصله معقول قرار دارند، تکرار شوند.
BCR-07	نگهداری دستگاه‌ها	• برای حفظ تجهیزات، اطمینان از تداوم و در دسترس بودن عملیات باید سیاست‌ها و رویه‌هایی جهت پشتیبانی از فرآیندهای

		تجاری ایجاد شوند و و اقدامات فنی لازم انجام شوند.
BCR-08	خرابی برق دستگاه‌ها	• در برابر تهدیدهای طبیعی و انسانی باید اقدام‌های حفاظتی در مکان تجهیزات انجام گیرد تا بر اساس ارزیابی تأثیرات خاص جغرافیایی واکنش لازم را نشان دهند.
BCR-09	تحلیل تاثیر	بایستی یک روش تعریف شده و مستند برای تعیین تأثیر هرگونه اختلال بر روی سازمان (ارائه دهنده ابر، مصرف کننده ابر) وجود داشته باشد که باید موارد زیر را شامل شود: • تعیین محصولات و خدمات مهم • تعیین تمام وابستگی‌ها، از جمله فرآیندها، برنامه‌ها، شرکای تجاری و ارائه دهندگان خدمات شخص ثالث • تعیین تهدیدات مربوط به محصولات و خدمات مهم • تعیین تأثیرات ناشی از اختلالات برنامه‌ریزی شده یا غیر برنامه‌ریزی شده و نحوه تغییر در طول زمان • تعیین حداکثر دوره قابل تحمل را برای ایجاد اختلال • تعیین اولویت‌های اصلاح و ترمیم • تعیین حداقل زمان بازیابی برای از سرگیری ارائه خدمات مهم در کنار حداکثر مدت زمان تحمل اختلال در آنها • تخمین و تعیین منابع مورد نیاز برای از سرگیری ارائه خدمات
BCR-10	سیاست	• برای حصول اطمینان از برنامه‌ریزی مناسب، پشتیبانی از قابلیت‌های فناوری اطلاعات سازمان و حمایت از عملکردهای تجاری و مشتریان، باید سیاست‌ها و رویه‌هایی براساس استانداردهای قابل قبول صنعتی (مانند ITIL v4 و COBIT 5)، ایجاد شود و با تعریف فرآیندهای تجاری و اقدام‌های فنی مناسب پشتیبانی شود. • علاوه بر این، سیاست‌ها و رویه‌ها بایستی شامل نقش‌ها و مسئولیت‌های تعریف شده‌ای باشند که براساس آموزش منظم نیروی کار پشتیبانی شوند.
BCR-11	سیاست‌های حفاظت	• برای تعیین و پایبندی به دوره حفاظت از دارایی‌های حساس، بایستی سیاست‌ها و رویه‌هایی تعیین شود. • همچنین بایستی سیاست‌ها و رویه‌هایی برای پشتیبانی از فرآیندهای تجاری و اقدامات فنی مربوط به تعهدات، اقدامات

		قانونی یا نظارتی، ایجاد شوند. • اقدامات پشتیبان‌گیری و بازیابی باید به عنوان بخشی از برنامه‌ریزی تداوم کسب‌وکار درآمده و براساس آن برای اثربخشی آزمایش شوند.

۴-۲- مدیریت پیکربندی و کنترل تغییر

هدف از حوزه‌ی مدیریت پیکربندی و کنترل تغییر (CCC[1])، فرموله کردن و دستگیری از تغییرات به بهترین وجه ممکن و مدیریت پیکربندی‌های برنامه‌ها و داده‌های جدید می‌باشد.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
CCC-01	توسعه جدید/خرید	• برای حصول اطمینان از توسعه و دستیابی به داده‌های جدید، برنامه‌های فیزیکی یا مجازی، شبکه زیرساختی و مؤلفه‌های سیستم یا هر مرکز شرکتی، عملیاتی و مرکز داده، باید سیاست‌ها و رویه‌هایی تعریف شود و از پشتیبانی فرآیندهای تجاری و اقدامات فنی اجرا شده اطمینان حاصل شود. • تسهیلات از قبل توسط مسئول سازمان یا سایر نقش‌های سازمانی مجاز باید فراهم شود.
CCC-02	توسعه برون‌سپاری شده	• شرکای تجاری خارجی باید همان سیاست‌ها و رویه‌های داخلی مربوط به مدیریت تغییر، انتشار و آزمایش را رعایت کنند. (مثلاً فرآیندهای مدیریت خدمات ITIL)
CCC-03	آزمون کیفیت	• سازمان‌ها باید یک فرایند کنترل کیفیت تغییرات و فرآیند تست را دنبال نمایند (به عنوان مثال ، مدیریت خدمات ITIL) • همچنین استانداردهای مربوط به ارائه خدمات، تست و انتشار را با تاکید بر دسترسی به سیستم، محرمانه بودن و یکپارچگی سیستم‌ها و خدمات رعایت نمایند.
CCC-04	نصب نرم‌افزار غیر مجاز	• برای محدود کردن نصب نرم‌افزارهای غیرمجاز بر روی دستگاه‌های کاربران نهایی یا سازمانی (به عنوان مثال ، ایستگاه‌های کاری تعیین شده، لپ‌تاپ‌ها و دستگاه‌های تلفن همراه کاربران) باید سیاست‌ها و رویه‌هایی تعریف و اجرا شود و از طریق فرآیندهای

[1] Change Control & Configuration Management (CCC)

		تجاری و اقدامات فنی پشتیبانی شوند.
CCC-05	تغییرات محصول	• برای مدیریت مخاطرات باید سیاست‌ها و رویه‌هایی تعریف و اجرا شوند تا تغییراتی بر روی موارد زیر داشته باشند: ❖ طراحی و تنظیمات مربوط به برنامه‌های مهم و حیاتی مربوط به کسب‌وکار یا مشتری (مستاجر) و رابط سیستم (API). ❖ مؤلفه‌های شبکه و سیستم‌های زیرساختی. • اقدامات فنی لازم باید انجام شود تا قبل از استقرار اطمینان حاصل شود که کلیه تغییرات مستقیماً با درخواست تغییر ثبت شده و نیز قرارداد مشتری (مستاجر) (SLA) مطابقت دارند.

۵-۲- امنیت داده و مدیریت چرخه حیات اطلاعات

امنیت داده و مدیریت چرخه‌ی حیات (DSI[1]) که یکی از دامنه‌ها با جزئیات فراوان در ماتریس CCM می‌باشد، بر روی تمامی مسائل مرتبط با داده بحث می‌کند، از جمله اینکه چطور جریان داده‌ها مدیریت می‌شود.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
DSI-01	دسته‌بندی	• داده‌ها و اشیاء حاوی داده‌ها باید براساس نوع داده، ارزش، حساسیت داده و حساسیت سازمان، طبقه‌بندی شوند.
DSI-02	موجودی/جریان داده	• برای نگهداری، مستندسازی و حفظ جریان داده برای داده‌های مقیم (دائم یا موقت) در برنامه‌های کاربردی که در شبکه جغرافیایی توزیع شده (فیزیکی و مجازی) قرار دارند بایستی سیاست‌ها و رویه‌هایی ایجاد و با ایجاد فرآیندهای تجاری و اقدام‌های فنی پشتیبانی شوند. • این سیاست‌ها بایستی با اشخاص ثالث به منظور بررسی هرگونه تأثیر نظارتی، مقررات قانونی یا زنجیره تأمین (SLA)، و بررسی سایر ریسک‌های تجاری مرتبط با داده‌ها، به اشتراک گذاشته شوند. • در صورت درخواست، ارائه دهنده باید مشتری (مستاجر) را از تأثیر و مخاطرات، به ویژه اگر داده‌های مشتری به عنوان بخشی از

[1] Data Security & Information Lifecycle Management (DSI)

		خدمات استفاده می‌شود، مطلع سازد.
DSI-03	تراکنش‌های اقتصادی	• داده‌های مربوط به تجارت الکترونیکی که در شبکه‌های عمومی منتقل می‌شوند، باید به طور مناسب طبقه‌بندی شوند و از فعالیت‌های کلاهبرداری، افشای غیر مجاز یا تغییر محافظت شوند تا از بروز اختلافات قرارداد و مصالحه‌ی داده جلوگیری شود.
DSI-04	سیاست‌های امنیتی/ برچسب‌گذاری	• برای برچسب‌زدن، رسیدگی و امنیت‌داده‌ها و اشیاء حاوی داده‌ها باید سیاست‌ها و رویه‌های مناسبی ایجاد شود. • باید مکانیسم‌های ارث‌بری برچسب برای اشیائی که به عنوان جمع‌آوری داده‌ها عمل می‌کنند، پیاده‌سازی شود.
DSI-05	داده‌های Non-production	• داده‌های در زمان production نباید در محیط‌های Non-production همانندسازی یا استفاده شوند. هرگونه استفاده از داده‌های مشتری در محیط‌های غیرتولیدی، نیاز به تأیید صریح و مستند از کلیه مشتریانی دارد که داده‌های آنها تحت تأثیر قرار گرفته است. • همچنین باید کلیه الزامات قانونی و نظارتی را برای حفاظت از داده‌های حساس انجام داد.
DSI-06	مالکیت/شراکت	• برای کلیه داده‌ها باید مالکیت، شراکت و مسئولیت‌ها اختصاص یابد و مستندسازی و ابلاغ آنها انجام شود.
DSI-07	پاک‌سازی و انهدام امن	• برای پشتیبانی از فرآیندهای تجاری و اقدامات فنی که نیاز به پاک‌سازی ایمن و حذف کامل داده‌ها از کلیه رسانه‌های ذخیره‌سازی دارند سیاست‌ها و رویه‌های مناسبی تعریف شوند و اطمینان حاصل شود که داده‌ها به هیچ وسیله جرم‌یابی قابل بازیابی نباشد.

۶-۲- امنیت مرکز داده

امنیت مرکز داده (DCS[1])، به مباحثی همچون امنیت فیزیکی سرویس‌دهنده‌ها و مراکز داده‌ی ابر مرتبط می‌شود. این دامنه پیرامون مدیریت دارایی‌ها و کنترل دسترسی فیزیکی به سرویس‌دهنده‌ها بحث می‌کند.

[1] DataCenter Security (DCS)

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
DCS-01	مدیریت دارایی	• دارایی‌ها باید از نظر حساسیت تجاری، سطح خدماتی که از آنها انتظار می‌رود و الزامات تداوم خدمات طبقه‌بندی شوند. • فهرست کاملی از دارایی‌های مهم تجاری که در سایت‌ها و یا موقعیت‌های جغرافیایی مختلف واقع شده‌اند تهیه شود. • اطلاعات آنها در طول زمان مرتباً حفظ و بروز شود و با تعریف نقش‌ها و مسئولیت‌ها، مالکیت آنها مشخص شود.
DCS-02	نقاط دسترسی کنترل شده	• بایستی عناصر امنیتی فیزیکی (به عنوان مثال نرده‌ها، دیوارها، موانع، نگهبانان، دروازه‌ها، نظارت الکترونیکی، مکانیسم‌های احراز هویت بدنی، میزهای پذیرش و گشت‌های امنیتی) برای محافظت از سیستم‌های داده و اطلاعات حساس ایجاد شوند.
DCS-03	شناسایی تجهیزات	• شناسایی خودکار تجهیزات باید به عنوان روشی برای تأیید صحت اتصال استفاده شود. • بهتر است از فن‌آوری‌های آگاه از موقعیت مکانی برای تأیید صحت هویت اتصال تجهیزاتی که مکان آنها مشخص است استفاده شوند.
DCS-04	مجوز خارج از سایت	• مجوزهای لازم باید قبل از جابجایی یا انتقال سخت افزار، نرم‌افزار یا داده به محلی خارج از سایت اخذ شود.
DCS-05	تجهیزات خاج از سایت	• بایستی سیاست‌ها و رویه‌های لازم برای از بین بردن ایمن تجهیزات (براساس نوع تجهیز) یا پاک‌سازی کامل تجهیزاتی که در خارج از محل سازمان مورد استفاده قرار خواهند گرفت ایجاد شود. • روش مورد نظر بایستی شامل یک راه‌حل پاک کردن یا تخریب با عدم امکان بازیابی اطلاعات باشد. • پاک کردن باید شامل یک رونویسی کامل از درایو هارد دیسک‌ها و عناصر ذخیره‌سازی باشد تا اطمینان حاصل شود که درایو پاک شده برای استفاده مجدد و استقرار در خارج از سازمان آماده است.
DCS-06	سیاست	• برای حفاظت و امنیت محیط کار و ایمنی دفاتر، اتاق‌ها، تأسیسات و فضاهای محل استقرار اطلاعات حساس، باید سیاست‌ها و رویه‌های مناسبی تعریف شود و فرایندهای تجاری لازم برای پشتیبانی آنها ایجاد شود.

DCS-07	مجوزدهی ناحیه‌ای	• ورود و خروج از مناطق امن باید توسط مکانیسم‌های کنترل دسترسی فیزیکی محدود و کنترل شود تا اطمینان حاصل شود که فقط افراد مجاز امکان دسترسی دارند.
DCS-08	ورود افراد غیرمجاز	• ورود و خروج افراد غیرمجاز مانند نیروهای خدماتی و سایر کارکنان غیرمجاز که ممکن است وارد محوطه شوند باید تحت نظارت و کنترل قرار گیرد و در صورت امکان از محل ذخیره‌ی داده‌ها و پردازش آنها جدا شوند تا از افشای غیرمجاز داده‌ها و ضرر جلوگیری شود.
DCS-09	دسترسی کاربر	• دسترسی فیزیکی به دارایی‌های اطلاعاتی و توابع آنها بایستی برای کاربران و پرسنل پشتیبانی محدود شود.

۷-۲- مدیریت کلید و رمزنگاری

رمزنگاری یکی از بزرگ‌ترین بخش‌های امنیت ابر است. در این راستا در ماتریس CCM، حوزه‌ی مدیریت کلید و رمزنگاری (EKM[1]) امکان اعمال سیاست‌هایی برای تنظیم درست محیط رمزنگاری و مدیریت کلیدها با تاثیر حداکثری فراهم می‌کند.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
EKM-01	حق مالکیت	• کلیدها باید دارای مالکان قابل شناسایی باشند • بایستی سیاست‌های مدیریت کلید وجود داشته باشد.
EKM-02	تولید کلید	• برای مدیریت کلیدهای رمزنگاری در رمزنگاری سرویس، سیاست‌ها و رویه‌هایی ایجاد شود (به عنوان مثال ، مدیریت چرخه عمر از تولید کلید تا ابطال و جایگزینی، زیرساخت‌های کلید عمومی، طراحی پروتکل رمزنگاری و الگوریتم‌های مورد استفاده، کنترل دسترسی برای ایجاد کلیدهای خاص و تبادل و ذخیره‌سازی از جمله تفکیک کلیدهای مورد استفاده برای داده یا جلسات رمزگذاری شده). • در صورت درخواست، ارائه دهنده باید به مشتری (مستاجر) از تغییرات درون سیستم رمزنگاری اطلاع دهد، به ویژه اگر داده‌های مشتری (مستاجر) به عنوان بخشی از خدمات استفاده شود و

[1] Encryption and Key Management (EKM)

		مشتری (مستاجر) مسئولیت مشترکی در مورد اجرای کنترل داشته باشد.
EKM-03	حفاظت از داده‌های حساس	• برای استفاده از پروتکل‌های رمزگذاری در حفاظت از داده‌های حساس، باید سیاست‌ها و رویه‌های مناسبی تعریف شود و فرآیندهای تجاری و اقدامات فنی لازم برای پشتیبانی آن تعریف شود. • طبق قوانین و مقررات، محل‌هایی که برای حفاظت از داده‌های حساس باید مورد توجه قرار گیرد شامل موارد زیر می‌باشند: (۱)محل ذخیره‌سازی داده‌ها (به عنوان مثال سرورهای پرونده، پایگاه‌داده‌ها و ایستگاه‌های کاری کاربر نهایی)، (۲)محل استفاده از داده‌ها (حافظه)، و (۳)محل انتقال داده‌ها (به عنوان مثال رابط‌های سیستم، شبکه‌های عمومی و پیام‌های الکترونیکی که داده‌ها از طریق آنها ارسال شده‌اند).
EKM-04	دسترسی و ذخیره‌سازی	• لازم است از بسترهای نرم‌افزاری و الگوریتم‌های مناسب برای رمزگذاری داده‌ها (مانند AES-256) در قالب‌های باز/تاییدشده و الگوریتم‌های استاندارد استفاده شود. • کلیدها نباید در ابر ذخیره شوند (یعنی در ارائه دهنده ابر مورد نظر)، بلکه توسط مصرف کننده ابر یا ارائه دهنده، در قالب مدیریت کلید قابل اعتماد تولید شوند. • مدیریت کلید و استفاده از آن باید به صورت وظایف جداگانه‌ای باشند.

۸-۲- مدیریت مخاطره و قانون‌گذاری

آنچه که تا اینجا بدان پرداخته شده‌است عمدتا نیازمندیهای امنیتی پایه می‌باشد. در بسیاری از موارد، الزامات امنیتی مبتنی بر سیاست‌های داخلی آن تجارت نمی‌باشند و عوامل خارجی مانند الزامات قانونی و تنظیمات و مقررات حاکمیتی نیز در آنها موثر است. این بخش از الزامات در CCM تحت عنوان مدیریت مخاطره و قانون‌گذاری (GRM[1]) بیان شده‌است.

[1] Governance and Risk Management (GRM)

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
GRM-01	الزامات اولیه	• الزامات امنیتی اولیه باید برای محصول توسعه یافته یا خریداری شده، سازمانی یا مدیریت شده، فیزیکی یا مجازی، برنامه‌های کاربردی و سیستم زیرساختی و مؤلفه‌های شبکه که مطابق با تعهدات قانونی و مقررات قابل اجرا هستند، ایجاد شود. • تغییر تنظیمات اولیه تجهیزات و نرم‌افزارها، باید براساس سیاست‌ها و رویه‌های مدیریت تغییرات و قبل از مراحل استقرار انجام شود تا اعمال و استفاده از آنها مجاز باشد. • تطبیق با الزامات اولیه امنیتی، باید حداقل سالانه مورد ارزیابی مجدد قرار گیرد، مگر اینکه در دوره‌های مشخصی براساس نیازهای تجاری ایجاد و مجاز شده باشد.
GRM-02	تخمین مخاطره با تمرکز بر داده	• تخمین مخاطرات مرتبط با نیازهای حاکمیتی داده‌ها باید در فواصل زمانی برنامه‌ریزی شده‌ای انجام شود و موارد زیر را در نظر گیرد: ❖ آگاهی از مکان ذخیره‌سازی داده‌های حساس در سراسر برنامه‌ها، پایگاه‌داده‌ها، سرورها و زیرساخت‌های شبکه ❖ تعهد با دوره‌های نگهداری تعیین شده ❖ الزام به معدوم نمودن داده‌های منقضی شده ❖ طبقه‌بندی و محافظت از داده‌ها در برابر استفاده غیر مجاز، دسترسی، از بین رفتن، تخریب و جعل
GRM-03	دیدگاه مدیریتی	• مدیران، وظیفه آگاهی و پیروی از سیاست‌ها و رویه‌های امنیتی و استانداردهای مربوط به حوزه مسئولیت خود را دارند.
GRM-04	برنامه مدیریتی	• یک برنامه مدیریت امنیت اطلاعات (ISMP) باید تدوین، مستندسازی، تصویب و اجرا شود که شامل اقدام‌های اداری، فنی و فیزیکی برای محافظت از تجهیزات و داده‌ها در مقابل از دست دادن، سوء استفاده، دسترسی غیرمجاز، افشاء، تغییر و تخریب باشد. برنامه امنیتی بایستی شامل موارد زیر باشد، اما به آنها محدود نمی‌شود و به ویژگی‌های تجاری نیز مربوط می‌شوند: مدیریت ریسک، سیاست امنیتی، سازمان امنیت اطلاعات، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی و محیطی، ارتباطات و مدیریت عملیات، کنترل دسترسی، توسعه و نگهداری

		سیستم‌های اطلاعاتی
GRM-05	مشارکت/ پشتیبانی مدیریتی	• مدیریت اجرایی باید اقدام‌های رسمی را برای پشتیبانی از امنیت اطلاعات به صورت مستندشده و تعهدآور انجام دهد و اطمینان حاصل کند که اقدام‌ها به افراد مشخصی منتسب شده باشند.
GRM-06	سیاست	• سیاست‌ها و رویه‌های امنیت اطلاعات باید تنظیم و برای بررسی و ارزیابی در اختیار کلیه پرسنل داخلی مرتبط و کسب‌وکارهای خارجی مرتبط قرار گیرد. • سیاست‌های امنیت اطلاعات باید توسط رئیس سازمان تجاری (یا نقش و مسئول معتبر دیگر کسب و کار) تایید شود و به وسیله یک طرح تجاری استراتژیک و یک طرح مدیریت امنیت اطلاعات که مشخص کننده نقش‌ها و مسئولیت‌های امنیت اطلاعات می‌باشد پشتیبانی شود.
GRM-07	اجرای سیاست	• بایستی برای کارمندانی که سیاست‌ها و رویه‌های امنیتی را نقض کرده‌اند، یک سیاست رسمی انضباطی و مجازاتی تعیین شود. • کارمندان باید آگاه شوند که در صورت بروز تخلف چه اقدامی می‌تواند انجام شود و اقدام‌های انضباطی در سیاست‌ها و رویه‌ها باید بیان شود.
GRM-08	تاثیر سیاست بر تخمین مخاطره	• بایستی نتایج تخمین مخاطرات به صورت بروزرسانی سیاست‌های امنیتی، رویه‌ها، استانداردها و کنترل‌های امنیتی اعمال شوند و از مفید و مؤثر بودن آنها اطمینان حاصل شود.
GRM-09	بازبینی سیاست‌ها	• رئیس سازمان تجاری (یا نقش و مسئول معتبر دیگر) باید سیاست امنیت اطلاعات را در فواصل زمانی برنامه‌ریزی شده یا در صورت تغییر در سازمان مورد بررسی قرار دهد تا از تداوم و همبستگی آن با استراتژی امنیتی، اثربخشی، صحت، اهمیت و مطابقت آن با تعهدات قانونی یا نظارتی اطمینان حاصل نماید.
GRM-10	تخمین‌های مخاطره	• مطابق با چارچوب جامع سازمانی، تخمین‌های رسمی مخاطرات بایستی حداقل به صورت سالیانه یا در فواصل برنامه‌ریزی شده (و در صورت هرگونه تغییر در سیستم‌های اطلاعاتی) انجام شود. • احتمال و تأثیر همه خطرات شناسایی شود و با استفاده از روش‌های کیفی و کمی، باید احتمال و تأثیر آنها در مقایسه با خطرات اصلی و تاثیرگذار مشخص شود.

		• کلیه مخاطرات به صورت مشخصی دسته‌بندی شوند.
GRM-11	چارچوب مدیریت مخاطره	• خطرات باید تا حد قابل قبول کاهش یابد. سطوح پذیرش براساس معیارهای مخاطره باید برای بازه‌های زمانی مجزا تهیه شود و بعد از تأیید ذینفعان ایجاد و مستند شود.

۹-۲- امنیت منابع انسانی

سیاست‌های امنیتی و الزامات آن، زمانی موثر و کارآمد هستند که توسط کسانی که درگیر فرایندها هستند به درستی پیاده‌سازی شوند. در این راستا یک دامنه‌ی کنترلی برای امنیت منابع انسانی (HRS[1]) در CCM درنظر گرفته شده‌است.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
HRS-01	بازگرداندن اموال	• پس از خاتمه خدمت پرسنل یا پایان یافتن روابط تجاری خارجی، کلیه اموال متعلق به سازمان باید در مدت زمان مشخصی برگردانده شوند.
HRS-02	سوءپیشینه	• مطابق قوانین کشوری، مقررات، اخلاق حرفه‌ای و محدودیت‌های پیمانکاری، کلیه کاندیداهای استخدام، پیمانکاران و اشخاص ثالث متناسب با طبقه‌بندی داده‌ای که دسترسی خواهند داشت، بایستی مورد تأیید و تایید عدم سوء پیشینه قرار گیرند.
HRS-03	تعهدنامه‌های استخدام	• بایستی تعهدنامه‌های استخدام شامل مقررات و موارد مربوط به پیروی از سیاست‌های حاکمیتی و امنیت اطلاعات تعیین شده باشد و برای همه انواع استخدام (شامل کارمند تمام وقت یا پاره وقت یا مشروط) قبل از شروع به کار پرسنل و قبل از دسترسی به امکانات، منابع و اموال شرکت، این تعهدنامه‌ها توسط کارمندان تازه استخدام شده امضا شود.
HRS-04	اتمام کارمندی	• نقش‌ها و مسئولیت‌های مربوط به اجرای پایان خدمت یا تغییر در جایگاه استخدامی باید تعیین، مستندسازی و ابلاغ شود.
HRS-05	مدیریت دستگاه موبایل	• برای مدیریت مخاطرات مربوط به اجازه دسترسی دستگاه‌های تلفن همراه به منابع سازمانی باید سیاست‌ها و رویه‌های مناسبی تعریف شود و فرآیندهای تجاری و اقدامات فنی لازم برای

[1] Human Resource Security (HRS)

		پشتیبانی آن ایجاد شود. • ممکن است نیاز به اجرای کنترل‌های تضمین امنیت بالاتری باشد و سیاست‌ها و رویه‌های مجزایی برای استفاده از این دستگاه‌ها تدوین و ابلاغ شود (به عنوان مثال آموزش‌های امنیتی خاص، احراز هویت قوی‌تر، کنترل حق دسترسی و نظارت بر دستگاه).
HRS-06	تعهدنامه‌های عدم افشای اطلاعات	• الزامات تعهدنامه‌های مربوط به عدم افشاء یا محرمانه بودن، منعکس‌کننده نیازهای سازمان برای حفاظت از داده‌ها و جزئیات عملیاتی می‌باشد و باید در فواصل زمانی برنامه‌ریزی شده شناسایی، بررسی و بروزرسانی شوند و به امضای همه کارکنان برسد.
HRS-07	نقش‌ها و مسئولیت‌ها	• نقش و مسئولیت‌های پیمانکاران، کارمندان و کاربران شخص ثالثی که با منابع داده‌ای و اموال سازمان در ارتباط هستند باید مستند و ابلاغ گردد.
HRS-08	استفاده قابل قبول از تکنولوژی	• برای تعیین مجوزها و شرایط لازم برای استفاده از دستگاه‌های کاربری متعلق به پرسنل یا مدیریت سازمان (به عنوان مثال، ایستگاه‌های کاری، لپ‌تاپ‌ها و دستگاه‌های تلفن همراه) برای دسترسی به زیرساخت‌های شبکه و اجزاء سیستم باید سیاست‌ها و رویه‌های مناسبی تعریف شود و فرآیندهای تجاری و اقدامات فنی لازم برای پشتیبانی آن ایجاد شود. • علاوه بر آن، به منظور پشتیبانی بهتر از کاربران، بایستی تعریف مجوزها و شرایط لازم برای استفاده از دستگاه‌های تلفن همراه شخصی (BYOD) و برنامه‌های مرتبط با دسترسی به منابع سازمانی موردنظر برای کاربران در نظر گرفته شده و فراهم شود.
HRS-09	آگاهی بخشی و آموزش	• برای کلیه پیمانکاران، کاربران شخص ثالث و کارمندان سازمان یک برنامه آموزشی در زمینه آگاهی امنیتی درنظر گرفته شود و در صورت لزوم به صورت اجباری باشد. • کلیه افراد دارای دسترسی به داده‌های سازمانی باید آموزش‌های مناسب و مداومی را در خصوص حساسیت‌های سازمانی، فرآیندها و سیاست‌های مربوط به عملکرد حرفه‌ای خود داشته باشند.
HRS-10	مسئولیت‌های کاربران	کلیه پرسنل باید از نقش‌ها و مسئولیت‌های خود آگاه باشند: • آگاهی و پیروی از سیاست‌ها و رویه‌های تعیین شده و تعهدات

		مربوط به رعایت قوانین و نظارت‌های سازمان. • ایجاد و مدیریت یک محیط کاری امن و ایمن براساس نیازهای سازمانی
HRS-11	فضای کاری	• بایستی سیاست‌ها و رویه‌ها به گونه‌ای تنظیم شوند که یک فضای کاری امن ایجاد شود • اسناد حساس و صورت جلسات از دسترس مستقیم سایر افراد خارج شوند (مثلاً روی میزکاری رها نشوند) • پس از یک دوره مشخص داده‌ها و اسناد اضافی غیرفعال شوند.

۱۰-۲-مدیریت دسترسی و هویت

مدیریت دسترسی، همواره یکی از بخش‌های بزرگ و برجسته در امنیت ابر می‌باشد. مدیریت دسترسی و هویت (IAM[1]) شامل ۱۳ کنترل و الزام امنیتی می‌باشد.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
IAM-01	دسترسی به ابزار ممیزی	• دسترسی و استفاده از ابزارهای ممیزی که با سیستم‌های اطلاعاتی سازمان ارتباط برقرار می‌کنند باید بطور مناسب تفکیک شوند و دسترسی‌ها محدود شود تا از افشای نامناسب و دستکاری داده‌های لاگ جلوگیری شود.
IAM-02	چرخه‌حیات مجوزها / مدیریت شرط‌ها	برای اطمینان از احراز هویت، اعمال مجوزها و مدیریت دسترسی پرسنل داخلی و مشتریان (مستاجران) در دسترسی به داده‌ها، تجهیزات (فیزیکی و مجازی)، رابط‌های برنامه، زیرساخت‌های شبکه‌های و مؤلفه‌های سیستمی باید سیاست‌ها و رویه‌های مناسبی تعریف شود و فرآیندهای تجاری و اقدامات فنی لازم برای پشتیبانی از آن ایجاد شود. این سیاست‌ها، رویه‌ها و اقدامات باید موارد زیر را شامل شود: • رویه‌ها، نقش‌ها و مسئولیت‌های لازم برای تأمین و بازپس‌گیری مجوزهای دسترسی به حساب کاربران مشخص شود و از قاعده حداقل امتیاز بر اساس نیازهای کاری پیروی شود.

[1] Identity and Access Management (IAM)

		• ملاحظات ویژه در خصوص موارد خاص کاری و تضمین احراز هویت چند عاملی انجام گیرد. (به عنوان مثال، رابطهای مدیریتی، تولید کلید، دسترسی از راه دور، تفکیک وظایف، دسترسی اضطراری، امکان استقرار در مناطق جغرافیایی توزیع شده و تعدد پرسنل برای سیستم‌های مهم درنظر گرفته شود) • بخش‌بندی دسترسی‌ها به جلسات و داده‌های کاری کاربران در معماری‌های چند عامله برای شخص ثالث (به عنوان مثال برای ارائه دهنده خارجی یا مشتریان دیگر) • تعیین روش‌های بررسی قابل اعتماد و مدیریت دسترسی‌های سرویس به سرویس (API) و روش‌های پردازش اطلاعات (به عنوان مثال SSO) • مدیریت چرخه اعتبار حساب کاربری از لحظه ایجاد تا ابطال • ذخیره‌سازی حساب‌ها و شناسه‌ها و در صورت امکان استفاده مجدد از آنها • استفاده از قواعد احرازهویت، مجوزدهی و حسابرسی (AAA) برای دسترسی به داده‌ها و جلسات (به عنوان مثال رمزگذاری چند عاملی، منقضی شدنی و غیر مشترک) • مجوزدهی و قابلیت پشتیبانی و کنترل دسترسی مشتری (مستاجر) بر اساس احرازهویت، مجوزدهی و حسابرسی (AAA) برای دسترسی به داده‌ها و جلسات • پیروی از الزامات قانونی یا نظارتی قابل اعمال
IAM-03	دسترسی به درگاه‌های پیکربندی	• بایستی دسترسی کاربر به درگاه‌های تشخیص و پیکربندی محدود به افراد مجاز و برنامه‌های کاربردی باشد.
IAM-04	سیاست‌ها و رویه‌ها	• بایستی برای ذخیره‌سازی و مدیریت اطلاعات هویتی مربوط به اشخاصی که به زیرساخت‌های فناوری اطلاعات دسترسی پیدا می‌کنند و میزان دسترسی آنها، سیاست‌ها و رویه‌هایی ایجاد شود. • باید سیاست‌هایی برای کنترل دسترسی به منابع شبکه براساس هویت کاربر تدوین شود.
IAM-05	تفکیک وظایف	• برای محدود کردن دسترسی کاربر طبق تفکیک وظایف مشخص شده و همچنین به منظور تعیین مخاطرات مرتبط با تضاد منافع کاربران، باید سیاست‌ها و رویه‌های مناسبی تعریف شود و

		فرآیندهای تجاری و اقدامات فنی لازم برای پشتیبانی آن ایجاد شود.
IAM-06	محدودیت دسترسی به کد منبع	• دسترسی به برنامه‌های توسعه یافته سازمان، کد منبع برنامه‌ها یا هر شکل دیگری از منابع که شامل قوانین مالکیت معنوی می‌باشند و استفاده از نرم‌افزارهای اختصاصی باید طبق قانون حداقل دسترسی و براساس نیاز مطابق با سیاست‌ها و رویه‌های دسترسی کاربر تعیین شده و به طور مناسب محدود شود.
IAM-07	دسترسی شخص ثالث	• بایستی شناسایی، ارزیابی و اولویت‌بندی خطرات ناشی از فرآیندهای تجاری که نیاز به دسترسی به سیستم‌ها و داده‌های سازمان دارند برای به حداقل رساندن، نظارت و سنجش احتمال خطر و تأثیر دسترسی غیرمجاز انجام شوند. • بررسی‌های جبران خسارت براساس روش‌های تحلیل ریسک باید قبل از فراهم کردن دسترسی انجام شود.
IAM-08	منابع قابل اعتماد	• بایستی سیاست‌ها و رویه‌های مناسبی برای ذخیره‌سازی مجوزها و دسترسی به هویت‌ها که برای احراز هویت استفاده خواهند شد، تعریف شوند. • اطمینان حاصل شود که دسترسی به اطلاعات هویت‌ها فقط به کاربران و برنامه‌هایی که براساس نیازهای اجرایی لازم هست و براساس قانون کمترین دسترسی ممکن اعطا شده باشد.
IAM-09	مجوز دسترسی کاربران	• اختصاص دسترسی کاربران (به عنوان مثال کارمندان، پیمانکاران، مشتریان (مستاجر)، شرکای تجاری) به داده‌ها و برنامه‌های متعلق یا مدیریت شده سازمان (فیزیکی و مجازی)، سیستم‌های زیربنایی و مؤلفه‌های شبکه بایستی با تایید مدیریت سازمان قبل از دسترسی به آنها مطابق با سیاست‌ها و رویه‌های تعیین شده انجام شود. • در صورت درخواست مشتری، ارائه دهنده باید در خصوص دسترسی کاربران به اطلاعات مشتری (مستاجر)، به او اطلاع دهد به ویژه اگر داده‌های مشتری به عنوان بخشی از سرویس در حال استفاده باشد یا مشتری در خصوص تعیین کنترل دسترسی‌ها مسئولیت مشترکی داشته باشد.
IAM-10	بازبینی دسترسی	• دسترسی کاربران باید برای مناسب بودن مجوزها، در فواصل

	کاربران	زمانی برنامه‌ریزی شده‌ای، توسط مدیران سازمان یا سایر افراد مسئول بررسی و مجدداً مورد تأیید قرار گیرد و بر اساس قانون اعطای حداقل دسترسی‌ها براساس نیازهای شغلی انجام گیرد. • برای تخلفات دسترسی شناسایی شده، باید از سیاست‌ها و رویه‌های تعریف شده‌ای برای اصلاح دسترسی کاربران استفاده شود.
IAM-11	لغو دسترسی‌های کاربران	• (ابطال یا اصلاح) دسترسی کاربر به داده‌ها و برنامه‌های متعلق یا مدیریت شده (فیزیکی و مجازی) سازمان، سیستم‌های زیرساختی و مؤلفه‌های شبکه، بایستی طبق سیاست‌ها و رویه‌های تعیین شده و براساس تغییر وضعیت کاربر در زمان مناسبی اعمال شود. (به عنوان مثال در زمان خاتمه کار یا خاتمه رابطه تجاری، تغییر شغل یا انتقال). • در صورت درخواست مشتری، ارائه دهنده باید این تغییرات را به مشتری (مستاجر) اطلاع دهد، به ویژه اگر داده‌های مشتری به عنوان بخشی از سرویس در حال استفاده باشد یا مشتری در خصوص تعیین کنترل دسترسی‌ها مسئولیت مشترکی داشته باشد.
IAM-12	اعتبارات شناسه کاربران	بایستی اعتبار حساب کاربران داخلی یا مشتریان (مستاجران) به شرح زیر محدود شود و از احراز هویت، مجوزها و مدیریت دسترسی‌ها مطابق با سیاست‌ها و رویه‌های تعیین شده اطمینان حاصل شود: • تعیین روش‌های بررسی قابل اعتماد و مدیریت دسترسی‌های سرویس به سرویس (API) و روش‌های پردازش اطلاعات (به عنوان مثال SSO) • مدیریت چرخه اعتبار حساب کاربری از لحظه ایجاد تا ابطال • ذخیره‌سازی حساب‌ها و شناسه‌ها و در صورت امکان استفاده مجدد از آنها • استفاده از قواعد احرازهویت، مجوزدهی و حسابرسی (AAA) برای دسترسی به داده‌ها و جلسات (به عنوان مثال رمزگذاری چند عاملی، منقضی شدنی و غیر مشترک)
IAM-13	دسترسی برنامه‌های کاربردی	• برنامه‌های کاربردی که قادر به کنترل بالقوه سیستم، اشیاء، شبکه، ماشین مجازی و کنترل‌های برنامه هستند باید محدود

		شوند.

۱۱-۲-امنیت زیرساخت و مجازی‌سازی

با توجه به اینکه بسیاری از محیط‌های رایانش ابری توسط فناوری‌های مجازی‌سازی ایجاد می‌شوند، بنابراین ایجاد دامنه‌ی امنیت زیرساخت و مجازی‌سازی (IVS[1]) برای بیان الزامات امنیتی مرتبط با آن در رایانش ابری ضروری است.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
IVS-01	لاگ ممیزی/ تشخیص نفوذ	• سطوح امنیتی بالاتری برای تضمین ذخیره‌سازی، نگهداری و مدیریت چرخه حیات لاگ‌های ممیزی، رعایت تعهدات قانونی یا نظارتی و فراهم نمودن حسابرسی دقیق دسترسی‌های کاربران در تشخیص رفتارهای مشکوک شبکه و تشخیص عدم صحت فایل‌ها و فراهم نمودن توانایی تشخیص جرم در صورت نقض امنیت لازم است.
IVS-02	تشخیص تغییرات	• ارائه دهنده‌ی سرویس باید صحت کلیه ماشین‌های مجازی را در همه زمان‌ها تضمین کند. • هر تغییری که در هر ماشین مجازی ایجاد شده باشد باید وارد لاگ شود و یک هشدار، بدون در نظر گرفتن نوع وضعیت اجرایی آنها (مثلاً خفته ، خاموش یا در حال اجرا) اعلام شود. • هرگونه تغییر یا انتقال یک ماشین مجازی و اعتبارسنجی صحت آن باید بلافاصله از طریق روش‌های الکترونیکی (به عنوان مثال از طریق پورتال یا اعلام هشدار) در دسترس مشتریان قرار گیرد.
IVS-03	همگام‌سازی زمان	• برای همگام‌سازی ساعت‌های سیستم در کلیه سیستم‌های پردازش اطلاعات، بایستی از یک منبع زمانی خارجی معتبر که مورد توافق متقابل قرار گرفته شده باشد، استفاده شود تا ردیابی و بازسازی زمان‌های فعالیت را تسهیل کند.
IVS-04	مستندسازی	• در دسترس بودن، کیفیت و ظرفیت کافی منابع باید برنامه‌ریزی،

[1] Infrastructure & Virtualization Security (IVS)

	سیستم‌های اطلاعاتی	تهیه و اندازه‌گیری شود تا عملکرد سیستم مورد نیاز مطابق با تعهدات قانونی و مقررات مربوطه ارائه شود. پیش‌بینی ظرفیت‌های مورد نیاز آینده برای کاهش خطر اضافه بار سیستم لازم می‌باشد.
IVS-05	مدیریت آسیب‌پذیری	• پیاده‌سازها باید اطمینان حاصل کنند که ابزارها یا خدمات ارزیابی آسیب‌پذیری امنیتی، شرایط فناوری‌های مجازی‌سازی مورد استفاده را شامل می‌شوند (یعنی برای سیستم‌های مجازی‌سازی مناسب باشند).
IVS-06	امنیت شبکه	• برای محدود کردن و نظارت بر ترافیک بین اتصالات قابل اعتماد و غیر قابل اعتماد، باید طراحی و تنظیمات مناسبی برای محیط‌های شبکه و ماشین‌های مجازی در نظر گرفته شوند. • این تنظیمات بایستی حداقل سالانه مورد بازبینی قرار گیرد و طبق یک روش مستند شده برای استفاده در کلیه خدمات، پروتکل‌ها، درگاه‌ها و با تغییرکنترل‌ها اعمال شود.
IVS-07	کنترل‌های پایه و مقاوم‌سازی سیستم	• همه‌ی سیستم عامل‌ها باید مقاوم‌سازی شوند به گونه‌ای که فقط درگاه‌ها، پروتکل‌ها و خدمات لازم را برای تأمین نیازهای تجاری فراهم کنند. • از کنترل‌کننده‌های فنی مانند: آنتی ویروس، ناظر یکپارچگی فایل‌ها و لاگ به عنوان بخشی از استاندارد کاری اولیه استفاده شود.
IVS-08	محیط‌های عملیاتی/غیرعملیاتی	• برای جلوگیری از دسترسی غیرمجاز یا تغییر در اطلاعات، محیط‌های تولید و غیرتولید باید از هم جدا شوند. جداسازی محیط‌ها ممکن است شامل موارد زیر باشد: فایروال‌های بازرسی، منابع تأیید صحت دامنه / قلمرو • تفکیک وظایف برای کارکنانی که به این محیط‌ها به عنوان بخشی از وظایف شغلی خود دسترسی دارند، بایستی انجام شود.
IVS-09	قطعه‌بندی (Segmentation)	• برنامه‌های چند مستاجره (مشترک بین چند مشتری) متعلق یا مدیریت شده توسط سازمان (فیزیکی و مجازی) و سیستم زیرساختی و اجزای شبکه باید به گونه‌ای که دسترسی کاربر و مشتری (مستاجر) به طور مناسب از سایر مستاجران تفکیک شود طراحی، توسعه، استقرار و پیکربندی شود. در این برنامه‌ها ملاحظات زیر باید لحاظ شود:

		❖ سیاست‌ها و رویه‌ها تعیین شده باشد. ❖ جداسازی دارایی‌های مهم اقتصادی و داده‌های حساس کاربران که نیاز به کنترل‌های قوی‌تر و سطح بالاتری از تضمین را لازم داشته باشند. ❖ رعایت تعهدات قانونی و مقررات مربوط به الزامات مربوطه
IVS-10	امنیت و حفاظت از داده ماشین مجازی	• در هنگام انتقال سرورهای فیزیکی، برنامه‌ها یا داده‌ها به سرورهای مجازی، بایستی از کانال‌های ارتباطی ایمن و رمزگذاری شده استفاده شود و در صورت امکان از یک شبکه مجزا از شبکه‌های سطح تولید استفاده شود.
IVS-11	مقاوم‌سازی فوق‌ناظر (Hypervisor)	• دسترسی به کلیه عملکردهای مدیریتی فوق‌ناظر یا کنسول‌های مدیریتی برای سیستم‌هایی که میزبان سیستم‌های مجازی هستند باید براساس اصل کمترین مجوز برای پرسنل انجام شود. • سیستم‌های مجازی از طریق کنترل‌کننده‌های فنی (به عنوان مثال، تأیید هویت دو مرحله‌ای، اقدام‌های ممیزی، فیلتر آدرس IP، فایروال‌ها و ارتباطات کپسوله شده TLS) حفاظت گردد.
IVS-12	امنیت شبکه بی‌سیم	برای محافظت از محیط‌های شبکه بی‌سیم، باید سیاست‌ها و رویه‌های مناسبی تعریف شود و از فرآیندهای تجاری و اقدامات فنی برای پشتیبانی از آنها استفاده شود. از جمله این اقدام‌ها می‌توان به موارد زیر اشاره نمود: • فایروال‌های ورودی برای محدود کردن ترافیک غیر مجاز، پیاده‌سازی و تنظیم شود. • تنظیمات امنیتی با رمزگذاری قوی برای تأیید اعتبار و انتقال انجام گیرد • تنظیمات پیش فرض تجهیزات (به عنوان مثال کلیدهای رمزگذاری، گذرواژها و رشته‌های SNMP) با مقادیر مناسبی جایگزین شوند. • دسترسی کاربر به دستگاه‌های شبکه بی‌سیم محدود به پرسنل مجاز باشد. • قابلیت تشخیص وجود دستگاه‌های شبکه بی‌سیم غیر مجاز برای قطع به موقع از شبکه استفاده شده باشد.
IVS-13	معماری شبکه	• با بررسی معماری شبکه بایستی محیط‌های پرخطر و

		جریان‌داده‌هایی را که ممکن است دارای مخاطرات قانونی باشند، شناسایی کرد. • اقدامات فنی باید به کار گرفته شود و از تکنیک‌های دفاع در عمق (به عنوان مثال تجزیه و تحلیل بسته‌ها، کنترل ترافیک و سیاه چاله‌ها) برای تشخیص و پاسخ به موقع در برابر حملات مبتنی بر شبکه در ارتباط با الگوهای ترافیکی و حملات انکار سرویس (DDoS) استفاده شود.

۱۲-۲-قابلیت حمل و تعامل‌پذیری

قابلیت حمل و تعامل (IPY[1])، الزامات امنیتی مرتبط با نحوه‌ی استفاده از APIها و ارتباطات بین سرویس‌ها را بیان می‌کند.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
IPY-01	APIها	• ارائه دهنده خدمات ابری باید از APIهای باز و منتشر شده برای اطمینان از پشتیبانی از قابلیت همکاری بین مؤلفه‌ها و تسهیل برنامه‌های مهاجرت استفاده کند.
IPY-02	درخواست داده	• کلیه داده‌های دارای ساختار و بدون ساختار باید در صورت درخواست در قالب‌های استاندارد تجاری (به عنوان مثال doc.، xls.، pdf.) در اختیار قرار گیرد.
IPY-03	مشروعیت و سیاست	• بایستی سیاست‌ها، رویه‌ها و شرایط توافق شده متقابلی بین فراهم کننده‌ها به منظور برآورده کردن نیازهای مشتریان (مستاجران) برای کاربردهای سرویس به سرویس (API) و قابلیت همکاری در پردازش اطلاعات و قابلیت حمل برنامه‌های توسعه داده شده و تبادل، استفاده و یکپارچه‌سازی اطلاعات تعریف و اجرا شود.
IPY-04	پروتکل‌های شبکه استاندارد	• ارائه دهنده باید از پروتکل‌های شبکه استاندارد و ایمن برای دریافت و ارائه داده‌ها و مدیریت خدمات استفاده کند. • باید سندی را در اختیار مصرف‌کنندگان (مستاجرین) قرار دهد تا جزئیات مربوط به استانداردهای تعامل و تبادلی را که لازم دارند ارائه دهد.

[1] Interoperability & Portability (IPY)

IPY-05	مجازی‌سازی	• ارائه دهنده باید برای کمک به اطمینان از قابلیت همکاری از یک سکوی مجازی‌سازی صنعتی و قالب‌های استاندارد مجازی‌سازی (به عنوان مثال OVF) استفاده کند. • ارائه دهنده باید تغییرات سفارشی را که برای هر یک از ناظرینی که فعال می‌باشد و کلیه روش‌های مجازی‌سازی خاص استفاده شده را به صورت مستند شده در دسترس مشتری قرار دهد.

۱۳-۲-امنیت موبایل

با توجه به گستردگی تجهیزات موبایل، تدوین الزامات امنیتی موبایل (MOS[1]) برای سیستم‌های ابری لازم و ضروری است.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
MOS-01	ضدبدافزارها	• آموزش آگاهی از ضدبدافزارها، مخصوص دستگاه‌های تلفن همراه، باید در آموزش‌هایی که ارائه دهنده‌های خدمات برای آگاهی‌رسانی درباره امنیت اطلاعات ارائه می‌نمایند وجود داشته باشد.
MOS-02	فروشگاه‌های برنامه‌ها	• بایستی لیست مستند شده‌ای از فروشگاه‌های تأیید شده برای برنامه‌های دستگاه‌های تلفن همراه یا فراهم‌کننده‌های ذخیره‌سازی داده‌ها ارائه شود.
MOS-03	برنامه تاییدشده	• شرکت‌های مورد نظر باید دارای سیاست مستند شده‌ای باشند و ممنوعیت نصب برنامه‌های تأیید نشده یا برنامه‌های تأیید شده‌ای که از فروشگاه‌هایی که از قبل شناسایی و تایید نشده بدست می‌آیند، را مشخص نمایند.
MOS-04	نرم‌افزار تایید شده برای BYOD	• بایستی سیاست BYOD (دستگاه‌های موبایل شخصی) و پشتیبانی از آموزش‌های آگاهی‌رسانی، به صورت روشنی برنامه‌های تأیید شده، فروشگاه‌های تایید شده برای برنامه‌ها و افزونه‌هایی که ممکن است برای استفاده در BYOD مورد استفاده قرار گیرد را بیان کنند.

[1] Mobile Security (MOS)

MOS-05	آموزش و آگاهی‌بخشی	• ارائه دهنده باید سیاست مستندشده مشخصی در ارتباط با دستگاه تلفن همراه داشته باشد که شامل یک تعریف مستندشده برای دستگاه‌های تلفن همراه و استفاده‌های مجاز از آنها و پیش‌نیازهای استفاده از دستگاه‌های تلفن همراه باشد. • ارائه دهنده می‌بایست سیاست و الزامات را از طریق برنامه آگاهی‌بخشی و آموزش امنیتی شرکت ارائه و به آن اطلاع کارکنان و مشتریان برساند.
MOS-06	خدمات مبتنی بر ابر	• کلیه سرویس‌های مبتنی بر ابر که توسط دستگاه‌های تلفن همراه شرکت یا دستگاه‌های موبایل شخصی مورد استفاده قرار می‌گیرند، بایستی برای استفاده و ذخیره‌سازی اطلاعات تجاری شرکت از قبل تأیید شده باشند.
MOS-07	سازگاری	• شرکت باید یک پروسه اعتبارسنجی برنامه کاربردی مستند برای آزمایش دستگاه تلفن همراه، سیستم عامل و مشکلات سازگاری برنامه داشته باشد.
MOS-08	تایید صلاحیت دستگاه	• سیاست BYOD باید شرایط مربوط به دستگاه و شرایط لازم برای استفاده از دستگاه‌های موبایل شخصی را تعریف کند.
MOS-09	موجودی دستگاه‌ها	• بایستی لیستی از همه دستگاه‌های تلفن همراهی که برای ذخیره‌سازی و دسترسی به داده‌های شرکت استفاده می‌شوند تهیه و نگهداری شود. • هر تغییری در وضعیت این دستگاه‌ها (به عنوان مثال سیستم عامل و سطح وصله امنیتی، گمشده شدن یا خراب شدن آنها و تغییر در فردی که از آنها استفاده می‌کند) باید در لیست موجودی آنها اعمال و مورد بررسی قرار گیرد.
MOS-10	مدیریت دستگاه	• باید یک روش متمرکز مدیریت دستگاه‌های تلفن همراه که کلیه دستگاه‌های تلفن همراه مجاز برای ذخیره‌سازی، انتقال یا پردازش داده‌های مشتری را تحت نظر داشته باشد مستقر شود.
MOS-11	رمزنگاری	• سیاست‌های مربوط به استفاده از دستگاه تلفن همراه باید الزام به استفاده از رمزنگاری برای کل دستگاه یا برای داده‌های حساسی که در دستگاه‌های تلفن همراه ذخیره می‌شوند را مشخص نماید و از طریق کنترل‌های تکنولوژیکی اجرا و اجبار نماید.
MOS-12	روت‌کردن دستگاه	• سیاست‌های مربوط به استفاده از دستگاه تلفن همراه باید دور زدن

		کنترل‌های امنیتی داخلی (build-in) در دستگاه‌های تلفن همراه را ممنوع کند (به عنوان مثال root کردن دستگاه‌ها را ممنوع نماید) • این ممنوعیت باید از طریق کنترل‌های تشخیصی و پیشگیری بر روی دستگاه‌ها یا از طریق یک سیستم مدیریتی متمرکز (به عنوان مثال مدیریت دستگاه تلفن همراه) اعمال شود.
MOS-13	قانون (Legal)	• سیاست‌های BYOD شامل بیان واضح انتظارات مربوط به حفظ حریم خصوصی، الزامات حقوقی، کشف الکترونیکی و موارد قانونی است. • سیاست‌های BYOD باید به صورت روشن انتظارات مربوط به از دست دادن داده‌های غیر شرکتی را در صورت نیاز به پاک کردن دستگاه بیان کند.
MOS-14	صفحه قفل	• دستگاه‌های BYOD و دستگاه‌های متعلق به شرکت بایستی به گونه‌ای تنظیم شوند که فعال‌سازی قفل خودکار به صورت اجباری باشد و الزام آن باید از طریق کنترل‌های فنی اجرا شود.
MOS-15	سیستم عامل‌ها	• تغییرات در سیستم‌عامل دستگاه‌های همراه، سطح وصله امنیتی و برنامه‌های کاربردی موجود در آنها باید از طریق فرآیندهای مدیریت تغییر شرکت انجام شود.
MOS-16	رمزعبورها	• سیاست‌های رمز عبور، قابل استفاده برای دستگاه‌های تلفن همراه، باید از طریق کنترل‌های فنی بر روی کلیه دستگاه‌های شرکت یا دستگاه‌های تأیید شده برای استفاده دستگاه‌های موبایل شخصی، مستند و اجرا شوند. • این سیاست‌ها باید تغییر طول رمز عبور / پین و الزام‌های تأیید اعتبار را ممنوع کند.
MOS-17	سیاست	سیاست‌های دستگاه تلفن همراه باید کاربر BYOD را به تهیه نسخه پشتیبان از داده‌ها، ممنوعیت استفاده از فروشگاه‌های برنامه تأیید نشده و استفاده از نرم‌افزارهای ضدبدافزار (در صورت پشتیبانی) الزام کند.
MOS-18	حذف از دور	• کلیه دستگاه‌های تلفن همراهی که به شکل شخصی یا به صورت واگذار شده از طرف شرکت مجاز به استفاده شده‌اند، بایستی قابلیت پاک کردن کل دستگاه یا اطلاعات مربوط به شرکت از راه

		دور توسط پرسنل IT شرکت را داشته باشند.
MOS-19	وصله‌های امنیتی	• دستگاه‌های تلفن همراه متصل به شبکه‌های شرکت، یا ذخیره‌کننده و دارنده دسترسی به اطلاعات شرکت، باید مجوز تایید نرم‌افزار و نسخه را از راه دور مجاز سازند. • کلیه دستگاه‌های تلفن همراه باید جدیدترین وصله‌های مرتبط با امنیت را که توسط شرکت سازنده نرم‌افزار انتشار داده شده باشند یا توسط پرسنل تایید شده‌ای مشخص شده باشند را نصب نمایند و پرسنل مجاز IT باید بتوانند این بروزرسانی‌ها را از راه دور انجام دهند.
MOS-20	کاربران	• سیاست‌های BYOD بایستی سیستم‌ها و سرورهای مجاز برای استفاده یا دسترسی از طریق دستگاه‌های موبایل شخصی را مشخص نمایند.

۱۴-۲-مدیریت حوادث امنیتی، کشف و جرم‌یابی

هر چند پیش‌گیری یکی از بهترین رویکردها در امنیت ابر است، اما در بسیاری از موارد نقض‌های امنیتی رخ می‌دهد. دامنه‌ی مدیریت حوادث، کشف الکترونیکی و جرم‌یابی (SEF[1]) الزامات امنیتی ضروری را برای شرایط نقض امنیتی بیان می‌کند.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
SEF-01	نگهداری اطلاعات تماس/مجوزها	• باید اطلاعات تماس با مقامات مجاز ذیربط، مقامات قانون محلی و ملی و سایر مقامات قضایی تهیه، حفظ و به طور مرتب به روز شوند. • برای اطمینان، بایستی امکان تماس مستقیمی برای مواقع ضروری فراهم شود تا در صورت نیاز به انجام اقدام‌های جرم‌یابی، امکان هماهنگی سریع وجود داشته باشد.
SEF-02	مدیریت حوادث	• برای ردیابی حوادث مربوط به امنیت و اطمینان از مدیریت به موقع و کامل حادثه، بایستی مطابق با سیاست‌ها و رویه‌های

[1] Security Incident Management, E-Discovery, & Cloud Forensics (SEF)

		وزارت ارتباطات و فناوری اطلاعات، سیاست‌ها و رویه‌های لازم ایجاد شوند و فرآیندهای تجاری و اقدامات فنی لازم برای پشتیبانی از اجرای آنها ایجاد شود.
SEF-03	گزارش حوادث	• بایستی کارکنان و شراکای تجاری خارج از شرکت باید از مسئولیت‌های خود در خصوص گزارش به موقع وقایع امنیتی اطلاعات آگاه باشند. • کارکنان و شراکای تجاری خارج از شرکت باید در صورت بروز حوادث امنیتی، کلیه وقایع امنیتی اطلاعات را به موقع گزارش دهند. • رویدادهای امنیت اطلاعات باید از طریق کانال‌های ارتباطی از پیش تعریف شده و به موقع و رعایت تعهدات قانونی و نظارتی مربوطه گزارش شوند.
SEF-04	آماده‌سازی قانونی پاسخ به حوادث	• برای اقدامات قانونی بعد از حادثه امنیت اطلاعاتی، نیاز به تعریف رویه‌های جرم‌یابی مناسب، از جمله زنجیره حضانت، برای جمع‌آوری و ارائه شواهد لازم می‌باشد. • پس از اعلام و اخطار لازم، برای مشتریان و سایر شرکای تجاری خارج از شرکت که تحت تأثیر نقض امنیت قرار گرفته اند، همانطور که در تحقیقات قانونی مجاز است فرصت مشارکت برای آنها درنظر گرفته شود.
SEF-05	معیارهای پاسخ به حوادث	• بایستی سازوکارهایی برای نظارت و تعیین کمیت، انواع، حجم و هزینه حوادث امنیتی اطلاعات ایجاد شود.

۱۵-۲-مدیریت زنجیره تامین، شفافیت و مسئولیت‌پذیری

مدیریت زنجیره‌ی تامین، شفافیت و مسئولیت‌پذیری (STA[1])، مجموعه‌ای توامان از الزامات امنیتی سرراست و پیچیده می‌باشد. به این دلیل سرراست است که وظایف مورد نیاز برای تکمیل و استانداردهای مورد نیاز برای اجرا به روشنی بیان شده‌اند. اما از این جهت پیچیده هستند که برآورده کردن تمامی استانداردهای خواشته شده به طور همزمان کار راحتی نمی‌باشد.

[1] Supply Chain Management, Transparency, & Accountability (STA)

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
STA-01	کیفیت و صحت داده	• ارائه دهندگان باید برای بهبود کیفیت داده و چالش‌های مرتبط با آن، با همکاری شرکای زنجیره تأمین ابر خود بررسی و راهکار ارائه کنند. • ارائه دهندگان باید کنترل‌هایی را برای کاهش دسترسی و مهار مخاطرات امنیتی داده برای کلیه پرسنلی که در زنجیره تأمین مشارکت دارند از طریق تفکیک مناسب وظایف، دسترسی مبتنی بر نقش و دسترسی در کمترین حدممکن طراحی و اجرا کنند.
STA-02	گزارش‌دهی رویداد	• ارائه دهنده بایستی اطلاعات مربوط به حوادث امنیتی را به صورت دوره‌ای و از طریق روش‌های الکترونیکی (به عنوان مثال پرتال‌ها) در اختیار همه مشتریان و ارائه دهندگانی که از آن حادثه تاثیر پذیرفته‌اند قرار دهد.
STA-03	خدمات شبکه/زیرساخت	• رابط سیستم به سیستم (API ها) برنامه‌هایی که بر مشتری تاثیرگذار هستند و از نظر تجاری اهمیت دارند، زیرساخت‌های شبکه و مؤلفه‌های سیستم، باید مطابق با سرویس مورد توافق و توانایی‌های تعیین شده، طراحی، توسعه و مستقر شوند. • در طراحی، توسعه و استقرار آنها همچنین سیاست‌ها و رویه‌های حکومتی در حوزه IT و مدیریت خدمات باید درنظر گرفته شود.
STA-04	ارزیابی داخلی ارائه دهنده	• ارائه دهنده باید ارزیابی‌های داخلی سالانه‌ای برای اطمینان از تعیین مطابقت و اثربخش بودن سیاست‌ها و رویه‌های خود و میزان پشتیبانی از معیارها و مقیاس‌ها انجام دهد.
STA-05	توافقات زنجیره تامین	موافقت‌نامه‌های زنجیره تأمین بین ارائه‌دهندگان و مشتریان (مستاجرین) باید حداقل مقررات و شرایط مورد توافق متقابل را شامل شود: • محدوده روابط تجاری و خدمات ارائه شده را مشخص نماید (به عنوان مثال نحوه و میزان دریافت داده، تبادل و استفاده از اطلاعات، مجموعه ویژگی‌ها و امکانات، پرسنل و شبکه‌های زیرساختی و اجزای سیستم برای ارائه خدمات و پشتیبانی، نقش‌ها و مسئولیت‌های ارائه دهنده و مشتری (مستاجر) و هرگونه روابط تجاری تحت نظارت یا برون سپاری شده، موقعیت جغرافیایی فیزیکی خدمات میزبانی شده و هرگونه ملاحظه مربوط

		به رعایت مقررات شناخته شده را درنظر بگیرد) • الزامات امنیتی اطلاعات، مهم‌ترین موردی است که در تعامل طولانی مدت بین ارائه دهنده خدمات و مشتری (مستاجر) تاثیرگذار می‌باشد و به جزئیات فرآیندهای تجاری و پشتیبانی مربوطه و اقدامات فنی انجام شده برای پیاده نمودن مدیریت مخاطرات، تعهدات قانونی و نظارتی و رعایت مقررات در کلیه روابط تجاری اشاره می‌نماید. • اطلاع‌رسانی و دریافت مجوزهای اولیه توسط ارائه دهنده برای هرگونه تغییر که بر خدمات مشتری (مستاجر) تاثیرگذار می‌باشد. • اطلاع رسانی به موقع حوادث امنیتی به کلیه مشتریان (مستاجرین) و سایر شرکای تجاری که تحت تأثیر قرار گرفته‌اند. • ارزیابی و تأیید مستقل تطبیق با مفاد توافق‌نامه و اصطلاحات بدون ایجاد خطر غیرقابل قبول در فرآیندهای تجاری. • شرایط انقضای تعامل تجاری و نحوه برخورد با داده‌های مشتری (مستاجر) • نیازمندی‌های مشتری در ارتباط با رابط و برنامه سرویس به سرویس (API) و قابلیت حمل، تبادل، ماندگاری و استفاده از اطلاعات
STA-06	بازبینی حاکمیتی زنجیره تامین	• ارائه‌دهندگان باید فرایندهای مدیریت ریسک و فرآیندهای حاکمیتی شرکای خود را بررسی کنند تا روش‌های اجرایی سازگار و هماهنگ باشند و خطراتی که ممکن است از دیگر اعضای زنجیره تأمین بر ابر تاثیر گذارد را مشخص نمایند.
STA-07	سنجه‌های زنجیره تامین	• بایستی سیاست‌ها و رویه‌هایی برای بررسی مداوم موافقت‌نامه‌های خدمات بین ارائه دهندگان و مشتریان (مستاجرین) در سراسر زنجیره تأمین (بالادست / پایین دست) تعریف و اجرا شود. • بررسی‌ها باید حداقل سالانه انجام شود و هرگونه عدم مطابقت با توافق‌نامه‌های ایجاد شده را شناسایی کند. • بررسی‌ها باید به اقداماتی برای رسیدگی به مشکلات سطح خدمات یا تناقضات ناشی از روابط نامناسب تأمین کننده منجر شود.
STA-08	تخمین شخص ثالث	• ارائه‌دهندگان باید با انجام بررسی سالانه، امنیت اطلاعات را در

		سراسر زنجیره تأمین اطلاعات خود تضمین کنند. این بررسی شامل کلیه شرکاء و ارائه دهندگان شخص ثالث است که زنجیره تأمین اطلاعات به آنها بستگی دارد.
STA-09	ممیزی شخص ثالث	• ارائه‌دهندگان شخص ثالث باید مطابقت با موارد مندرج در توافق‌نامه‌ها را از بابت امنیت اطلاعات و حفظ محرمانگی، کنترل دسترسی، تعریف خدمات و سطح تحویل شده را نشان دهند. • گزارش‌ها، سوابق و خدمات شخص ثالث حداقل برای کنترل و حفظ مطابقت با موارد مندرج در توافق‌نامه‌های ارائه خدمات باید حداقل سالانه تحت نظارت و بررسی قرار گیرند.

۱۶-۲-مدیریت آسیب‌پذیری و تهدید

آخرین بخش از الزامات و کنترل‌های امنیتی CCM، مدیریت آسیب‌پذیری و تهدید (TVM[1]) می‌باشد. این دامنه بیانگر الزامات مرتبط با برنامه‌های ضدبدافزار، مدیریت آسیب‌پذیری و وصله‌ها و سنجه‌های امنیتی کدهای متحرک می‌باشد.

شناسه	عنوان الزام امنیتی	شرح الزام امنیتی
TVM-01	نرم‌افزار ضدویروس/ضدمخرب	• برای جلوگیری از اجرای بدافزار در دستگاه‌های کاربر نهایی متعلق به سازمان یا مدیریت شده (یعنی ایستگاه‌های کاری خارج از شرکت، لپ تاپ و دستگاه‌های تلفن همراه) و شبکه‌های زیربنایی IT و اجزای سیستم، بایستی سیاست‌ها و رویه‌های لازم ایجاد شوند و فرآیندهای تجاری و اقدامات فنی لازم برای پشتیبانی از اجرای آنها ایجاد شود.
TVM-02	مدیریت آسیب‌پذیری/ وصله	• برای شناسایی به موقع آسیب پذیری‌ها در برنامه‌های سازمان یا تحت مدیریت آن ، زیرساخت شبکه و مؤلفه‌های سیستم و اطمینان از موثر بودن کنترل‌های امنیتی، بایستی سیاست‌ها و رویه‌های لازم ایجاد شوند و فرآیندهای تجاری و اقدامات فنی لازم برای پشتیبانی از اجرای آنها ایجاد شود (به عنوان مثال ارزیابی دوره‌ای آسیب‌پذیری شبکه و آزمون نفوذ نرم‌افزارها انجام گیرد).

[1] Threat & Vulnerability Management (TVM)

		• باید مدل مبتنی بر ریسک برای اولویت‌بندی اصلاح نقاط آسیب‌پذیر شناسایی شده استفاده شود. • تغییرات باید از طریق یک فرآیند مدیریت تغییر در کلیه بخش‌ها، تغییرات پیکربندی یا تغییراتی در نرم‌افزار داخلی سازمان ایجاد شود. • در صورت درخواست، ارائه دهنده باید سیاست‌ها و رویه‌های مربوطه و نقاط ضعف شناسایی شده را به مشتری (مستاجر) اطلاع دهد. به ویژه اگر داده‌های مشتری (مستاجر) تحت تاثیر این سیاست‌ها قرار داشته باشد یا مشتری (مستاجر) نسبت به اجرای کنترل مسئولیت مشترکی داشته باشد.
TVM-03	کد متحرک	• برای جلوگیری از اجرای کد متحرک غیرمجازی که به عنوان نرم‌افزار بین سیستم‌ها و از طریق شبکه قابل اعتماد یا غیر قابل اعتماد منتقل می‌شود بایستی سیاست‌ها و رویه‌های لازم ایجاد شوند و فرآیندهای تجاری و اقدامات فنی لازم برای پشتیبانی از اجرای آنها ایجاد شود. • باید از اجرای کد متحرک غیرمجاز، در دستگاه‌های کاربر نهایی متعلق به سازمان یا مدیریت شده (یعنی ایستگاه‌های کاری خارج از شرکت، لپ تاپ و دستگاه‌های تلفن همراه) و شبکه‌های زیربنایی IT و اجزای سیستم جلوگیری شود.