پیوست

شورای اجرایی (عالی) فناوری اطلاعات کشور

کمیسیون توسعه دولت الکترونیکی

چارچوب معماری سازمانی ایران

معماری مرجع امنیت

استانداردهای امنیتی حوزه رایانش ابری

نسخه ۱,۰ – اردیبهشت ماه ۱۳۹۶

پیشگفتار

با پیشرفت فناوری اطلاعات نیاز به انجام کارهای محاسباتی در همه جا و در همه زمان به‌وجود آمده است. همچنین نیازست که افراد بتوانند کارهای محاسباتی سنگین خود را بدون داشتن سخت‌افزارها و نرم‌افزارهای گران، از طریق خدمات انجام دهند. رایانش ابری آخرین پاسخ فناوری به این نیازها بوده است. با وجود این که زمان زیادی از پیدایش این علم سپری نشده‌است سازمان‌های زیادی در این حوزه فعالیت می‌کنند. در حقیقت یک ابر، ردیفی گسترده از کامپیوترهایی است که به یکدیگر متصل شده‌اند و به‌عنوان یک اکوسیستم واحد به فعالیت می‌پردازند.

رایانش ابری یک نوع از محاسبات مبتنی‌بر اینترنت می‌باشد که داده‌ها و منابع پردازشی کامپیوتر را در بین کامپیوتر و دستگاه‌های پردازشی دیگر مبتنی‌بر تقاضا به اشتراک می‌گذارد. از منظر زیرساختی، چهار دسته متفاوت با عنوان‌های ابر خصوصی، ابر عمومی، ابر ترکیبی و ابر انجمنی وجود دارد. ذخیره‌سازی ابری به کاربران این امکان را می‌دهد که از هر کجا و در هر شرایطی به داده‌های خود دسترسی پیدا کنند بنابراین این امر، مساله اعتماد به سرویس‌های ارائه دهنده فضای ابری و امنیت را با چالش مواجه نموده‌است. از این رو در این سند مقصود بر این است که استانداردهای امنیتی حوزه ابر مورد بررسی قرار گیرد تا سازمان‌ها بتوانند در این حوزه، امنیت و حریم خصوصی را برای کاربران خود فراهم آورند و در نتیجه به بهره‌وری بیشتر دست یابند.

لیست استانداردهای امنیتی حوزه رایانش ابری

شماره استاندارد	نام استاندارد
SP 500-291	NIST Cloud Computing Standards Roadmap, (2013) نقشه راه استانداردهای محاسبات ابری مؤسسه NIST
SP 500-292	NIST Cloud Computing Reference Architecture, (2011) معماری مرجع محاسبات ابری NIST
SP 500-293	US Government Cloud Computing Technology Roadmap ,(2014) نقشه راه فناوری محاسبات ابری دولت ایالات متحده
SP 500-299	NIST Cloud Computing Security Reference Architecture,(2013) معماری مرجع امنیت محاسبات ابری مؤسسه NIST
SP 800-144	Guidelines on Security and Privacy in Public Cloud Computing, (2011) راهنمای امنیت و حریم خصوصی در محاسبات ابر عمومی
SP 800-145	The NIST Definition of Cloud Computing, (2012) تعاریف NIST از محاسبات ابری
SP 800-146	Cloud Computing Synopsis and Recommendations, (2012) توصیه‌ها و مرور اجمالی بر محاسبات ابری
SP 800-125	Guide to Security for Full Virtualization Technologies, (2011) راهنمای امنیت برای فناوری‌های مجازی‌سازی کامل
Interagency Report 7904	Trusted Geolocation in the Cloud: Proof of Concept Implementation, (2015) منطقه جغرافیایی قابل اعتماد در ابر: اثبات اجرای مفاهیم
SP 800-92	Guide to Computer Security Log Management, (2006) راهنمایی برای مدیریت ثبت وقایع امنیتی کامپیوتر
SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems, Rev. 1, (2014) راهنمای استفاده از چارچوب مدیریت ریسک برای سیستم‌های اطلاعات فدرال: یک رویکرد چرخه حیات امنیت

شماره استاندارد	نام استاندارد
ISO/IEC 17788	Information technology -- Cloud computing -- Overview and vocabulary,(2014) فناوری اطلاعات- محاسبات ابری- مرور کلی و واژگان
ISO/IEC 17789	Information technology -- Cloud computing -- Reference architecture, (2014) فناوری اطلاعات- محاسبات ابری- معماری مرجع
ISO/IEC 27017	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services,(2015) فناوری اطلاعات- فنون امنیتی- کد عمل برای کنترل‌های امنیت اطلاعات بر مبنای استاندارد ISO/IEC 27002 برای خدمات ابر
ISO/IEC 27018	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, (2014) فناوری اطلاعات- فنون امنیتی- کد عمل جهت حفاظت از اطلاعات شناسایی شخصی (PII) در ابرهای عمومی که به عنوان پردازنده‌های PII عمل می‌کنند.
ISO/IEC 17826	Information technology -- Cloud Data Management Interface (CDMI), (2016) فناوری اطلاعات- رابط مدیریت داده‌های ابر
ISO/IEC 27036-2	Information technology-- Security techniques-- Information security for supplier relationships-- Part 2: Requirements, (2014) فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط عرضه‌کنندگان- بخش دوم: نیازمندی‌ها
ISO/IEC 27036-4	Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services,(2016) فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط عرضه‌کنندگان- بخش چهارم: راهنمایی برای امنیت خدمات ابر
ISO/IEC 27040	Information technology -- Security techniques -- Storage security, (2015) فناوری اطلاعات- فنون امنیتی- امنیت ذخیره‌سازی
Y.cceco	Cloud Computing Ecosystem, use cases and general requirements, (2012) اکوسیستم محاسبات ابری، موارد کاربرد و نیازمندی‌های کلی و عمومی
Y.ccic	Framework of inter-cloud computing for network and infrastructure, (2015) چارچوب محاسبات بین ابری برای شبکه و زیرساخت

نام استاندارد	شماره استاندارد
Cloud Computing Reference Architecture, (2012) معماری مرجع محاسبات ابری	Y.ccra
(2015) Security framework for cloud computing, چارچوب امنیتی برای محاسبات ابری	X.ccsec (ITU-T X.1601)
Guidelines for the operational security of cloud computing, (2015) راهنمایی برای امنیت عملیاتی محاسبات ابری	X.goscc (ITU-T X.1642)
Security functional requirements for software as a service application environments,(2015) نیازمندی‌های عملکردی امنیت برای محیط کاربردی نرم‌افزار به‌عنوان خدمت[1] (SaaS)	X.sfcse (ITU-T X.1602)
Requirement of IdM in Cloud Computing, (2014) نیازمندی‌های مدیریت هویت در محاسبات ابری	X.idmcc
Trusted inter-cloud computing framework and requirements, (2015) نیازمندی‌ها و چارچوب‌های محاسبات بین ابری قابل اعتماد	QCTIC
Requirements and analysis for management interface of virtualized resources in cloud computing, (2017) نیازمندی‌ها و تحلیل‌های لازم برای رابط مدیریت منابع مجازی در محاسبات ابری	M.mivrcc
Guidelines for cloud service customer data security, (2016) دستورالعمل‌هایی برای امنیت داده‌های مشتری خدمات ابر	X.CSCdataSec (ITU-T X.1641)
Data security requirements for the monitoring service of cloud computing, (2017) نیازمندی‌های امنیت داده‌ها به‌منظور نظارت بر خدمات محاسبات ابری	X.dsms
Security requirements of public infrastructure as a service (IaaS) in cloud computing,(2018) نیازمندی‌های امنیتی زیرساخت‌های عمومی به‌عنوان یک خدمت در محاسبات ابری	X.SRIaaS
End-to-end cloud service lifecycle management requirements, (2015)	Y.e2ecslm-

[1] Software as a Service

شماره استاندارد	نام استاندارد
Req	نیازمندی‌های مدیریت چرخه حیات خدمات ابری انتها به انتها
Y.CCNaaS-arch	Cloud computing - Functional Architecture of Network as a Service, (2016)
	محاسبات ابری- معماری عملکردی شبکه به‌عنوان یک خدمت
P2301	Guide for Cloud Portability and Interoperability Profiles, (2014)
	دستورالعمل‌هایی برای مشخصات قابلیت حمل و قابلیت همکاری ابر (CPIP)
DSP0243	Open Virtualization Format Specification, (2015)
	مشخصات قالب مجازی‌سازی باز[۲] (OVF)
DSP2028	Cloud Auditing Data Federation (CADF) Use Case, (2012)
	موارد کاربرد یکپارچه‌سازی ممیزی داده ابر
	Trusted Cloud Initiative (TCI) Reference Architecture Model, (2011)
	مدل معماری مرجع طرح ابر قابل اعتماد
	Cloud Controls Matrix (CCM),(2017)
	ماتریس کنترل‌های ابر
	Top Threats to cloud computing,(2017)
	تهدیدات مهم در محاسبات ابری
	Security as a Service (SecaaS) Implementation Guidance, (2016)
	راهنمای اجرای امنیت به‌عنوان یک خدمت
	Security Guidance for Critical Areas of Focus in Cloud Computing, (2015)
	راهنمای امنیتی برای حوزه‌های بحرانی متمرکز در محاسبات ابری
	Cloud Application Management for Platforms (CAMP), (2014)
	مدیریت برنامه‌های کاربردی ابر برای پلتفرم‌ها
	Identity in the Cloud (IDCloud),(2012)
	هویت در ابر
	Topology and Orchestration Specification for Cloud Applications (TOSCA),(2016)

[۲] Open Virtualization Format

شماره استاندارد	نام استاندارد
	مشخصات توپولوژی و تنظیمات مربوط به برنامه‌های کاربردی ابر
	Cloud Authorization (CloudAuthZ),(2016)
	مجوزدهی ابر
	Public Administration Cloud Requirements (PACR), (2013)
	الزامات ابر جهت مدیریت ملی
	Cloud Data Management Interface (CDMI) specification,(2015)
	مشخصات رابط مدیریت داده‌های ابر
17826	Information technology -- Cloud Data Management Interface (CDMI), (2016)
	فناوری اطلاعات– رابط مدیریت داده‌های ابر

در ادامه هر کدام از استانداردهای فوق مختصرا شرح داده می‌شود:

- **SP 500-291: NIST Cloud Computing Standards Roadmap**

این سند به‌منظور ارایه استانداردهای موجود در زمینه محاسبات ابری منتشر شده است. چشم‌انداز این سند شامل بررسی کلی در مورد استانداردهای موجود در زمینه‌های امنیت، قابلیت حمل، قابلیت همکاری، مدل‌ها، موارد کاربرد، تحقیقات و هر آنچه که مربوط به محاسبات ابری است، می‌باشد.

- **SP 500-292: NIST Cloud Computing Reference Architecture**

تعاریف مؤسسه NIST درباره محاسبات ابری باعث می‌شود که درک روشنی از فناوری‌های محاسبات ابری و خدمات ابری ایجاد شود. این سند از سری استانداردهای NIST، معماری مرجع محاسبات ابری را ارایه می‌کند و این معماری مرجع، بر روی مواردی که خدمات ابری ارایه می‌دهند، تمرکز می‌کند و به چگونگی طراحی راه‌حل‌ها و پیاده‌سازی‌ها، نمی‌پردازد. معماری مرجع به‌منظور تسهیل فهم پیچیدگی‌های عملیاتی در محاسبات ابری، در نظر گرفته شده‌است.

- **SP 500-293: US Government Cloud Computing Technology Roadmap**

این سند، نقشه راه فناوری محاسبات ابری دولت ایالات متحده را ارایه می‌دهد. این سند به‌منظور اهداف زیر طراحی شده‌است:

- ترویج استفاده از محاسبات ابری توسط سازمان‌های فدرال و حمایت از بخش خصوصی
- کاهش عدم اطمینان از طریق فراهم کردن اطلاعات برای تصمیم‌گیرندگان
- تسهیل توسعه مدل محاسبات ابری

این سند هم‌چنین برای موارد زیر تدوین شده‌است:

- ابزاری جهت تعریف و ارتباط بین امنیت تاکتیکی و استراتژیکی با اولویت بالا، قابلیت همکاری و الزامات قابلیت حمل
- ابزاری جهت تعریف و ارتباط استانداردها، راهنمایی‌ها و فناوری‌های مربوطه
- ابزاری جهت تعریف و ارتباط لیستی از طرح‌های اقدامی مقدم[3] (PAP) که به‌منظور حمایت از توسعه استانداردها، راهنماها و فناوری‌ها توسعه داده شده‌اند.

- **SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing**

هدف از این سند، ارایه یک دید کلی از محاسبات ابری عمومی و چالش‌های حریم خصوصی و امنیت مربوط به آن می‌باشد. این سند به مسائلی در زمینه‌های تهدیدات، ریسک‌های فناوری و تدابیر حفاظتی برای محیط‌های ابر عمومی می‌پردازد و اتخاذ تصمیمات آگاهانه در مورد فناوری اطلاعات به‌منظور مقابله با این تهدیدات را امکان‌پذیر می‌سازد.

باید توجه داشت که این سند، هیچ‌گونه خدمات محاسبات ابری خاصی، طبقه‌بندی خدمات، قرارداد خدمات، ارایه‌دهنده خدمات یا مدل استقراری را توصیه نمی‌کند. بنابراین هر سازمانی باید نیازهای خود را مورد تحلیل قرار دهد و خدمات ابر عمومی را که می‌توانند به بهترین نحو این نیازها را پوشش دهند، مورد ارزیابی، انتخاب، به‌کارگیری و نظارت قرار دهند.

---

[3] Priority Action Plans

- **SP 800-145: The NIST Definition of Cloud Computing**

این سند تعاریف مؤسسه NIST درباره محاسبات ابری را ارایه می‌دهد. محاسبات ابری یک الگوی در حال تحول است. تعاریف NIST، جنبه‌های مهم محاسبات ابری را مشخص می‌کند و به‌عنوان ابزاری جهت مقایسه خدمات ابر و استراتژی‌های توسعه در نظر گرفته می‌شود و همچنین مبنایی برای بررسی موضوعاتی از قبیل محاسبات ابری چیست تا بهترین نحوه استفاده از محاسبات ابری را فراهم می‌آورد. مدل‌های توسعه و خدمات براساس یک طبقه‌بندی ساده تعریف شده‌اند که هیچ روش توسعه، تحویل خدمت و یا عملیات کسب‌وکار بخصوصی را تعیین یا تحمیل نمی‌کنند.

- **SP 800-146: Cloud Computing Synopsis and Recommendations**

هدف از این سند، توصیف حوزه فناوری محاسبات ابری و هم‌چنین ارایه توصیه‌هایی برای تصمیم‌گیرندگان فناوری اطلاعات می‌باشد. محاسبات ابری یک زمینه در حال توسعه است و نقاط قوت و ضعف آن هنوز به‌طور کامل مورد تحقیق، مستندسازی و تست قرار نگرفته‌است. این سند، توصیه‌هایی درباره این که چگونه و در چه زمان محاسبات ابری، ابزار مناسبی محسوب می‌شوند را بیان می‌کند و محدودیت‌های دانش فعلی و زمینه‌هایی برای تجزیه و تحلیل آتی را نشان می‌دهد.

- **SP 800-125: Guide to Security for Full Virtualization Technologies**

هدف از این استاندارد، رسیدگی به نگرانی‌های موجود در زمینه فناوری‌های مجازی‌سازی کامل برای سرویس‌دهنده و نیز مجازی‌سازی دسکتاپ می‌باشد. تمامی اشکال مجازی‌سازی به جز مجازی‌سازی کامل سرویس‌دهنده و دسکتاپ خارج از محدوده این سند می‌باشد.

- **SP 800-92: Guide to Computer Security Log Management**

این توصیه‌نامه به ارایه دستورالعمل‌های کاربردی در دنیای واقعی جهت توسعه، اجرا و نگه‌داری شیوه‌های مدیریت ثبت وقایع موثر در طول یک سازمان می‌پردازد. راهنماهای ارایه شده در این سند، موضوعات مختلفی از جمله ایجاد زیرساخت مدیریت ثبت وقایع، توسعه و اجرای فرایندهای مدیریت ثبت وقایع قوی در سراسر یک سازمان را پوشش می‌دهد.

- **Interagancy Report 7904: Trusted Geolocation in the Cloud: Proof of Concept Implementation**

این سند چالش‌های امنیتی منتخب شامل مناطق جغرافیایی و فناوری‌های زیرساخت به‌عنوان یک خدمت محاسبات ابری را توصیف می‌کند. در واقع این گزارش اثباتی از پیاده‌سازی مفاهیمی[۴] را که به‌منظور رسیدگی به چالش‌های موجود طراحی شده‌اند، توصیف می‌کند. NIST IR 7904 به‌عنوان یک طرح[۵] و یا قالبی در نظر گرفته می‌شود که می‌تواند توسط جامعه امنیت عمومی به‌منظور اعتبارسنجی[۶] و پیاده‌سازی اثبات پیاده‌سازی مفاهیم توصیف شده، مورد استفاده قرار گیرد.

- **SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems**

هدف از این سند ارائه راهنمایی برای استفاده از چارچوب مدیریت ریسک در سیستم‌های اطلاعاتی فدرال شامل فعالیت‌های طبقه‌بندی امنیت، انتخاب، اجرا، ارزیابی و نظارت‌بر کنترل‌های امنیتی است. این راهنما برای موارد زیر توسعه یافته است:

- اطمینان از این که مدیریت ریسک‌های امنیتی مربوط به سیستم اطلاعاتی مطابق با اهداف کسب‌وکار سازمان است.
- اطمینان از این که نیازمندی‌های امنیت اطلاعات از جمله کنترل‌های امنیتی ضروری، در معماری سازمان و فرایندهای چرخه حیات توسعه سازمان یکپارچه شده باشد.
- برای دستیابی به اطلاعات و سیستم‌های اطلاعاتی امن‌تر در دولت فدرال، از طریق پیاده‌سازی استراتژی‌های کاهش ریسک مناسب.

---

[4] Proof of concept implementation

[5] Blueprint

[6] Validate

- **ISO/IEC 17788: Information technology -- Cloud computing -- Overview and vocabulary**

این استاندارد یک بررسی کلی از محاسبات ابری را همراه با یک مجموعه از اصطلاحات و تعاریف ارایه می‌کند. در واقع این سند یک مجموعه اصطلاحات پایه برای استانداردهای محاسبات ابری می‌باشد. ISO/IEC 17788، قابل اجرا برای تمامی سازمان‌ها به‌عنوان مثال شرکت‌های تجاری، سازمان‌های دولتی و غیره می‌باشد.

- **ISO/IEC 17789: Information technology -- Cloud computing -- Reference architecture**

این استاندارد معماری مرجع محاسبات ابری[۷] (CCRA) را مشخص می‌کند. معماری مرجع شامل نقش‌ها، فعالیت‌ها و اجزای عملکردی محاسبات ابری و هم‌چنین روابط بین آن‌ها می‌باشد.

- **ISO/IEC 27017: Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services**

این سند دستورالعمل‌هایی را برای کنترل‌های امنیت اطلاعات قابل اجرا و مناسب جهت تخصیص و استفاده از خدمات ابر با ارایه موارد زیر بیان می‌کند:

- ارایه دستورالعمل‌های اجرایی اضافه برای کنترل‌های مشخص شده در ISO/IEC 27002
- ارایه کنترل‌های اضافه همراه با راهنمایی‌هایی جهت پیاده‌سازی که به‌طور مشخص به خدمات ابری مربوط می‌شوند.

این توصیه‌نامه، استاندارد بین‌المللی، کنترل‌ها و راهنمایی‌های پیاده‌سازی را برای هر دو گروه ارایه‌دهنده خدمات ابر و مصرف‌کننده خدمات ابر، فراهم می‌آورد.

- **ISO/IEC 27018: Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**

این استاندارد کنترل‌ها و دستورالعمل‌هایی را به‌منظور اجرای اقداماتی جهت محافظت از اطلاعات شناسایی شخصی[۸] (PII) مطابق با اصول حریم خصوصی ارایه شده در استاندارد ISO/IEC 29100 برای محیط محاسبات ابری

---

[7] Cloud Computing Reference Architecture (CCRA)

عمومی، فراهم آورده‌است. این استاندارد به‌طور خاص دستورالعمل‌هایی را برمبنای استاندارد ISO/IEC 27002 و با توجه به در نظر گرفتن الزامات قانونی برای حفاظت از PII ارایه می‌کند.

- **ISO/IEC 17826: Information technology -- Cloud Data Management Interface (CDMI)**

این استاندارد در سال ۲۰۱۶ و با عنوان رابط مدیریت داده‌های ابر[9] (CDMI) منتشر شد که رابط‌هایی را به‌منظور دسترسی به فضای ذخیره‌سازی ابر و هم‌چنین داده‌های ذخیره‌شده در آن، مشخص می‌کند. این سند برای توسعه‌دهندگانی که در حال اجرا و یا در حال استفاده از فضای ذخیره‌سازی ابر می‌باشند، قابل پیاده‌سازی است.

- **ISO/IEC 20547-4: Information technology -- Big data reference architecture (BDRA) -- Part 4: Security and privacy fabric**

پیش‌بینی شده است که این استاندارد در سال ۲۰۱۹، منتشر شود. این سند یک استاندارد بین‌المللی است و روش‌های تأمین حریم خصوصی و امنیت پایه که در تمامی جنبه‌های BDRA اعمال می‌شود را توصیف می‌نماید. این جنبه‌ها شامل نقش داده‌های کلان، فعالیت‌ها و اجزای عملکردی می‌باشد.

- **ISO/IEC 27036-2: Information technology-- Security techniques-- Information security for supplier relationships-- Part 2: Requirements**

این استاندارد الزامات امنیت اطلاعات بنیادی را به‌منظور تعریف، پیاده‌سازی، اجرا، نظارت، بازنگری، نگه‌داری و بهبود روابط تامین‌کننده و خریدار[10]، مشخص می‌کند. این الزامات هرگونه تدارک و تامین محصولات و خدمات از جمله تولید و یا مونتاژ، مولفه‌های نرم‌افزاری و سخت‌افزاری، دانش فرایند تهیه، قرارداد ساخت، بهره‌برداری و واگذاری و خدمات محاسبات ابری را پوشش می‌دهد.

این الزامات برای تمامی سازمان‌ها صرف‌نظر از نوع فعالیت و یا گستره‌ای که دارند قابل اجرا می‌باشد. از فرایندهای پایه می‌توان به مواردی از قبیل مدیریت کسب‌وکار، مدیریت ریسک، مدیریت منابع انسانی و عملیاتی، امنیت اطلاعات و غیره اشاره کرد.

---

[8] Personally Identifiable Information

[9] Cloud Data Management Interface

[10] Acquirer

- **ISO/IEC 27036-4: Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services**

این سند راهنمایی‌هایی زیر را برای مشتریان و ارایه‌دهندگان خدمات ابر فراهم می‌کند:

- ارایه دیدی نسبت به ریسک‌های امنیت اطلاعات در ارتباط با استفاده از خدمات ابر و مدیریت آن ریسک‌ها به‌طور مؤثر.
- پاسخ‌گویی به ریسک‌های خاص به‌منظور بهره‌وری یا تخصیص خدمات ابری

دامنه این استاندارد ISO/IEC 27036-4، تعریف خطوط راهنما جهت پشتیبانی از پیاده‌سازی مدیریت امنیت اطلاعات برای استفاده از خدمات ابر می‌باشد.

- **ISO/IEC 27040: Information technology -- Security techniques -- Storage security**

این سند راهنمای فنی دقیق در مورد کاهش ریسک را با به‌کارگیری رویکرد اثبات شده در زمینه برنامه‌ریزی، طراحی، مستندسازی و پیاده‌سازی امنیت ذخیره‌سازی داده، فراهم می‌آورد.

- **ITU-T SG13 Y.cceco: Cloud Computing Ecosystem, use cases and general requirements**

هدف این استاندارد ارایه مقدمات و نیازمندی‌های کلی در زمینه اکوسیستم ابر، با تمرکز بر روی یکپارچه‌سازی و پشتیبانی از مدل محاسبات ابری و فناوری‌ها در محیط‌های مخابراتی و فناوری اطلاعات و ارتباطات[11] می‌باشد. در واقع این توصیه‌نامه به موارد زیر اشاره می‌کند:

- محاسبات ابری براساس طبقه‌بندی و تعاریف مبتنی‌بر وضعیت فعلی صنعت
- عاملان و نقش‌ها در اکوسیستم ابر
- مجموعه‌ای از مواردکاربرد مناسب ارتباطات مخابراتی
- زیرساخت‌های ابر
- موارد امنیتی مرتبط با ابر

[11] Information Communication Technology

- **ITU-T SG13 Y.ccic: Framework of inter-cloud computing for network and infrastructure**

این استاندارد بر روی استفاده از منابع شبکه و زیرساخت‌ها تمرکز دارد و همچنین چارچوب بین ابری[۱۲] را شرح می‌دهد که این چارچوب، تعداد زیادی از اپراتورهای کسب‌وکار IaaS[۱۳] و Naas[۱۴] را به هم متصل می‌نماید. Y.ccic به مسائل زیر می‌پردازد:

- توسعه موارد کاربردی
- تمایز بین کنترل ابر، مدیریت ابر و یا تعاریف روشن از آن‌ها
- هماهنگ‌سازی[۱۵] اصطلاحات و مدل داده منبع شبکه با همکاری سازمان ISO

- **ITU-T SG13 Y.ccra: Cloud Computing Reference Architecture**

دامنه و هدف این پروژه، توسعه معماری مرجع محاسبات ابری مبتنی‌بر سه سند زیر می‌باشد:

- پیش‌نویس نسخه جدید Y.CCRA با عنوان معماری مرجع محاسبات ابری منتشر شده توسط ITU-T Q.27/13.
- بخش ۶,۱ پیش‌نویس جدید Y.CCEco با عنوان محاسبات ابری: اکوسیستم، مواردکاربرد و نیازمندی‌های کلی- عاملان[۱۶] و نقش‌های یک اکوسیستم ابر، منتشر شده توسط ITU-T Q.26/13
- سند ISO/IEC WD 17789 با عنوان معماری مرجع محاسبات ابری (آخرین سند در N0680) منتشر شده توسط گروه کاری۳[۱۷].

- **ITU-T SG17 X.ccsec (ITU-T X.1601): Security framework for cloud computing**

این سند یک چارچوب امنیت سطح بالا را برای محاسبات ابری توصیف می‌کند که به تجزیه و تحلیل تهدیدات و چالش‌های امنیتی در محیط محاسبات ابری می‌پردازد و قابلیت‌های امنیتی را توصیف می‌کند که می‌تواند این تهدیدات را کاهش و چالش‌های امنیتی را برطرف کند. یک چارچوب جهت تعیین این که کدام یک از این

---

[12] Inter-Cloud

[13] Internet as a Service

[14] Network as a Service

[15] Synchronization

[16] Actor

[17] WG3

قابلیت‌های امنیتی برای کاهش تهدیدات امنیتی و رسیدگی به چالش‌های امنیتی در محاسبات ابری مورد نیاز خواهند بود، ارایه می‌شود.

- **ITU-T SG17 X.goscc (ITU-T X.1642): Guidelines for the operational security of cloud computing**

این توصیه‌نامه راهنمایی‌های امنیت عملیاتی را برای محاسبات ابری فراهم می‌آورد که شامل راهنمای توافق‌نامه سطح خدمات[۱۸] (SLA) و همچنین حفظ و بررسی امنیت به صورت روزانه برای محاسبات ابری می‌باشد. مخاطبان هدف این توصیه‌نامه، ارایه‌دهندگان خدمات ابر مانند اپراتورهای مخابراتی سنتی، ISP ها[۱۹] و ICP[۲۰] ها می‌باشند

- **ITU-T SG17 X.sfcse (ITU-T X.1602): Security functional requirements for software as a service application environments**

این توصیه‌نامه یک توصیف عملکردی عمومی را برای محیط برنامه کاربردی نرم‌افزار به‌عنوان خدمت سرویس‌گرای امن[۲۱] فراهم می‌آورد که مستقل از نوع شبکه، سیستم‌عامل، میان‌افزار، محصولات و یا راه‌حل‌های خاص می‌باشد. هم‌چنین این سند مستقل از هر نوع خدمت، مدل خاص سناریو، فرضیات و یا راه‌حلی ارایه شده است. در کل، این سند یک رویکرد ساخت‌یافته را جهت تعریف، طراحی و اجرای قابلیت‌های سرویس‌گرای امن و قابل مدیریت[۲۲] در محیط محاسبات ابری مخابراتی، توصیف می‌کند.

- **ITU-T SG17 X.idmcc: Requirement of IdM in Cloud Computing**

تمرکز این توصیه‌نامه بر روی هماهنگ‌سازی خدمات مخابراتی در محیط محاسبات ابری می‌باشد. ذکر این نکته ضروری است که این توصیه‌نامه ابتدا بر روی موارد کاربرد و تحلیل نیازمندی‌ها و با در نظر گرفتن امکانات موجود در صنعت شروع به کار کرد و اکنون در مورد نحوه هماهنگ‌سازی خدمات مخابراتی و خدمات اینترنتی مبتنی‌بر زیرساخت مدیریت هویت مشترک در محیط‌های محاسبات ابری متمرکز شده‌است.

---

18 service level agreement

19 Internet Service Provider

20 Internet Cloud Provider

21 secure service oriented Software as a Service

22 Manageable

- **ITU-T SG13 Q19 Y. CTIC: : Trusted inter-cloud computing framework and requirements**

این استاندارد در سال ۲۰۱۵ و با عنوان نیازمندی‌ها و چارچوب محاسبات بین ابری قابل اعتماد منتشر شد. این سند چارچوب محاسبات بین ابری قابل اعتماد و موارد کاربردی مبتنی‌بر چارچوب مشخص شده در ITU-T Rec. Y.3511 را مشخص می‌کند. دامنه این استاندارد شامل موارد زیر می‌باشد:

- اهداف محاسبات بین ابری قابل اعتماد
- الزاماتی به‌منظور برقراری امنیت بین ابری قابل اعتماد
- الزاماتی به‌منظور مدیریت[۲۳] بین ابری قابل اعتماد
- الزاماتی به‌منظور انعطاف‌پذیری[۲۴] بین ابری قابل اعتماد

- **ITU-T JRG-CCM M.mivrcc : Requirements and analysis for management interface of virtualized resources in cloud computing**

این توصیه‌نامه نیازمندی‌ها و تحلیل‌ها را برای رابط مدیریت بین سیستم پشتیبان عملیاتی ابر[۲۵] (COSS) و عامل مدیریت منابع مجازی‌شده[۲۶] (VRM)، مشخص می‌کند. این توصیه‌نامه متدولوژی مشخصات رابط توصیف شده در سند ITU-T M.3020 را مورد توجه قرار می‌دهد.

در این توصیه‌نامه عامل VRM جهت مدیریت و نظارت‌بر جنبه‌های توابع کنترلی و انتزاعی درون منابع و لایه شبکه معماری مرجع محاسبات ابری[۲۷](CCRA) در نظر گرفته می‌شود. COSS یک سیستم مدیریت یکپارچه را در راستای مدیریت جهانی ارایه می‌دهد که قابلیت‌های مدیریتی مرتبط با عملیات مورد نیاز جهت مدیریت و کنترل خدمات ابری پیشنهاد شده به مشتری را پیاده‌سازی می‌کند.

---

23 Governance

24 Resiliency

25 Cloud Operational Support System

26 Virtualized Resource Management

27 Cloud Computing Reference Architecture

در این توصیه‌نامه نیازمندی‌های عملکردی به‌منظور رابط مدیریت مشخص شده‌است که شامل مدیریت تنظیمات، مدیریت خطا و مدیریت عملکرد می‌باشد. در بخش تجزیه و تحلیل این سند، مدل اطلاعات مشروح[۲۸]، تمامی عملکردها را در سراسر رابط مدیریت فراهم می‌آورد.

- **ITU-T X.CSCdataSec (ITU-T X.1641) : Guidelines for cloud service customer data security**

این توصیه‌نامه راهنمایی‌هایی را به‌منظور تأمین امنیت داده‌های مشتری خدمات ابر در زمانی که یک CSP[۲۹] نسبت به حصول اطمینان در مورد این که داده با مکانیسم‌های امنیتی مناسب مورد استفاده قرار گرفته باشد مسئول است، به‌کار می‌رود. هم‌چنین این توصیه‌نامه، کنترل‌های امنیتی را برای داده‌های مشتری خدمات ابر در مراحل مختلف از چرخه کامل داده را مشخص می‌نماید. این کنترل‌های امنیتی خاص ممکن است به‌عنوان نیازهای امنیتی برای تغییرات داده‌های مشتری خدمات ابر نیز مورد استفاده قرار بگیرد.

- **ITU-T X.dsms : Data security requirements for the monitoring service of cloud computing**

این سند نیازمندی‌های امنیت داده را به‌منظور نظارت بر خدمات محاسبات ابری از جمله نظارت بر نیازمندی‌های حوزه داده، نظارت بر چرخه حیات داده، الزامات امنیتی نظارت‌بر اکتساب داده و الزامات امنیتی نظارت‌بر نحوه ذخیره‌سازی داده‌ها را تجزیه و تحلیل می‌کند.

نظارت بر چرخه حیات داده‌ها شامل ایجاد داده، ذخیره داده، استفاده از داده، مهاجرت داده، ارایه داده، تخریب داده و پشتیبان‌گیری از داده می‌باشد. نظارت بر اکتساب داده‌ها، نیازمندی‌های امنیتی فناوری‌های اکتساب را تعیین می‌کند و هم‌چنین نظارت بر ذخیره‌سازی داده‌ها نیز نیازمندی‌های امنیتی را برای CSP و به‌منظور ذخیره‌سازی داده‌ها، مشخص می‌نماید.

---

[28] Detailed information model

[29] Cloud Service Provider

- **X.SRIaaS: Security requirements of public infrastructure as a service (IaaS) in cloud computing**

این سند در سال ۲۰۱۸ منتشر خواهد شد. زیرساخت به‌عنوان یک خدمت (IaaS)، یکی از گروه‌های خدمات ابری می‌باشد. خدمات مجازی‌شده و محیط‌های IaaS نسبت به زیرساخت‌ها و برنامه‌های کاربردی فناوری اطلاعات سنتی با چالش‌ها و تهدیدات بیشتری مواجه هستند. هدف این توصیه‌نامه، مستندسازی نیازمندی‌های امنیتی IaaS عمومی می‌باشد. در واقع این سند به‌منظور بهبود سطح امنیت کلی در تمام مراحل برنامه‌ریزی، ساخت و نیز مراحل عملیاتی بسترها و خدمات IaaS، به‌کار می‌رود. این سند، هم‌چنین مکمل فعالیت‌های استانداردسازی امنیتی مرتبط با شبکه‌های مبتنی‌بر نرم‌افزار به‌خصوص استاندارد X.sdnsec، می‌باشد.

- **ITU-T JRG-CCM Y.e2ecslm-Req : End-to-end cloud service lifecycle management requirements**

این سند با عنوان الزامات مدیریت چرخه حیات خدمات ابری انتها به انتها، منتشر شده است. این توصیه‌نامه الزامات عملکردی چرخه حیات را جهت جنبه‌های مدیریت خدمات سرویس‌های ابر، مشخص می‌نماید. مدیریت چرخه حیات خدمات ابر شامل مدیریت رویداد، مدیریت سیاست، مدیریت اطلاعات مربوط به نقش، آماده‌سازی برنامه‌های کاربردی و خدمات، مدیریت منابع و مدیریت محتوا می‌باشد.

- **ITU-T SG13 Q18 Y.CCNaaS-arch : Cloud computing - Functional Architecture of Network as a Service**

این سند با عنوان معماری کاربردی شبکه به‌عنوان یک خدمت (NaaS) در حیطه محاسبات ابری، منتشر شده است. این توصیه‌نامه، معماری کاربردی NaaS را که شامل قابلیت‌ها، اجزای عملکردی و هم‌چنین رویه‌ها و نقاط مرجع مبتنی‌بر نیازمندی‌های عملکردی مشخص‌شده در سند Y.3512 می‌باشد را توصیف می‌کند. حوزه این سند شامل موارد زیر می‌باشد:

- بررسی کلی از معماری عملکردی NaaS
- قابلیت‌های NaaS
- اجزای عملکردی NaaS
- نقاط مرجع بین اجزای عملکردی NaaS
- رویه‌هایی برای مواردکاربرد معمول NaaS

- **IEEE P2301: Guide for Cloud Portability and Interoperability Profiles**

این استاندارد دستورالعمل‌هایی را برای مشخصات قابلیت حمل و قابلیت همکاری ابر[30] (CPIP) ارایه می‌دهد. این راهنما توصیه‌هایی را برای شرکای اکوسیستم محاسبات ابر (از جمله، فروشندگان ابر، ارایه‌دهندگان خدمات و کاربران) را قادر می‌سازد تا برمبنای استانداردها و در حوزه‌هایی مانند رابط‌های برنامه کاربردی، رابط‌های قابلیت حمل، رابط‌های مدیریت، رابط‌های قابلیت همکاری، قالب‌های فایل و قوانین عملکرد، انتخاب‌های درستی داشته باشند. در واقع هدف از این راهنما کمک به تولیدکنندگان و کاربران در توسعه، ساخت، استفاده از محصولات و خدمات محاسبات ابری می‌باشد که منجر به افزایش قابلیت حمل، قابلیت اشتراک[31] و قابلیت همکاری سیستم‌های محاسبات ابری می‌شود.

- **DSP0243: Open Virtualization Format Specification**

این استاندارد یک قالب باز، قابل حمل، امن، کارآمد و توسعه‌پذیر را به‌منظور بسته‌بندی و توزیع نرم‌افزار برای اجرا در ماشین‌های مجازی را ارایه می‌دهد. این قالب در واقع یک استاندارد طراحی شده به‌منظور رسیدگی به قابلیت همکاری و استقرار ابزارهای مجازی می‌باشد. امکان به‌کارگیری و استقرار ساده و نیز بدون خطای ابزارهای مجازی در سرتاسر بسترهای مجازی متعدد، با استفاده از این استاندارد قابل اعمال است.

- **DSP2028: Cloud Auditing Data Federation (CADF) Use Case**

این سند به‌منظور ارایه مجموعه‌ای از مواردکاربرد در دنیای واقعی جهت فراهم کردن برخی از ملاحظات برای ممیزی منابع مبتنی‌بر ابر در نظر گرفته می‌شود. این ملاحظات شامل نوع داده، منابع و تعاملات مورد انتظار توسط نهادهای مسئول به‌منظور ممیزی انطباق سیستم‌ها، برنامه‌های کاربردی و داده‌های میزبانی شده در توسعه ابر می‌باشد. این نهادها شامل مدیران برنامه‌های کاربردی و داده، مأموران امنیتی و حسابرسان شرکت‌ها، فروشندگان ابزار و خدمت در اکوسیستم ممیزی ابر می‌باشند.

---

[30] Cloud Portability and Interoperability Profiles

[31] Commonality

- **Trusted Cloud Initiative (TCI) Reference Architecture Model**

طرح امن و قابل اعتماد محیط‌های مبتنی بر ابر، یک رویکرد جامع برای معماری زیرساخت‌های امن ابر که در سال ۲۰۱۱ و توسط سازمان CSA، منتشر شد را ارایه می‌دهد. TCIچهار مدل معماری استاندارد صنعتی TOGAF، ITIL، SABSA و Jericho را به کار می‌گیرد و بهترین الگوهای معماری را به‌منظور ایجاد یک رویکرد جامع برای امنیت ابر، ترکیب می‌نماید.

معماری مرجع TCI، متدولوژی و مجموعه‌ای از ابزارها می‌باشد که طراحان امنیت، طراحان سازمان و متخصصان مدیریت ریسک را قادر می‌سازد تا یک مجموعه‌ای از راه‌حل‌ها را ارایه دهند. معماری باید با توجه به نیازمندی‌های کسب‌وکار مورد هدایت قرار گیرد. در مورد TCI این نیازمندی‌ها از یک ماتریس کنترل هدایت شده[۳۲] با استفاده از موارد زیر به‌دست می‌آیند:

- چارچوب‌های استاندارد مانند ISO-27002
- استانداردهای امنیت داده صنعت کارت پرداخت[۳۳]
- چارچوب ممیزی فناوری اطلاعات مانند COBIT
- به‌طور کلی مدل‌های تحویل ابر مانند SaaS، PaaS و IaaS

- **Cloud Controls Matrix (CCM)**

این ماتریس یک چارچوب کنترل امنیت برای ارایه‌دهنده خدمات ابر و مصرف‌کننده آن خدمات می‌باشد و در سال ۲۰۱۷، جدیدترین نسخه آن منتشر شد. استفاده از ماتریس کنترل CSA و کنترل‌های ISO 27017 به‌منظور تسهیل تطابق‌پذیری[۳۴] در ابر صورت می‌پذیرد. اولین بار، چارچوب کنترل، به‌طور خاص به‌منظور مدیریت ریسک در زنجیره تأمین ابر[۳۵]، طراحی شد. این ماتریس به موارد زیر می‌پردازد:

- چالش‌های درون و برون سازمانی به‌منظور برقراری مداوم امنیت اطلاعات
- ارایه یک نقطه تکیه‌گاه و زبان مشترک به‌منظور سنجش وضعیت تطابق‌پذیری و امنیت
- ارایه یک چشم‌انداز وسیع به‌منظور برقراری مقررات حریم خصوصی و استانداردهای امنیتی

---

32 Control matrix guided

33 Payment Card Industry Data Security Standard

34 Compliance

35 Cloud Supply Chain

این ماتریس هم‌چنین یک بنیادی را برای استانداردها و گواهی‌های جدید صنعت، فراهم می‌آورد. حوزه‌های فعالیت CCM شامل موارد زیر می‌باشد:

- انطباق (CO)
- مدیریت و کنترل داده[۳۶] (DG)
- تسهیل‌سازی امنیت (FS)
- منابع انسانی (HR)
- امنیت اطلاعات (IS)
- مسائل قانونی[۳۷] (LG)
- مدیریت عملیات (OM)
- مدیریت ریسک (RM)
- انعطاف‌پذیری[۳۸] (RS)
- معماری امنیت

➢ **Top Threats to cloud computing**

هدف از انتشار این سند، ارایه زمینه‌های مورد نیاز جهت کمک به سازمان‌ها می‌باشد تا بتوانند در زمینه مدیریت ریسک با توجه به استراتژی‌های به‌تصویب رسیده در ابر، تصمیمات را به درستی اتخاذ نمایند. در اصل این سند باید همراه با سند راهنمای امنیت برای مناطق بحرانی متمرکز در محاسبات ابری، مورد استفاده قرار گیرد. حوزه فعالیت این سند شامل تهدیدات زیر می‌باشد:

- سوءاستفاده[۳۹] و استفاده نادرست[۴۰] از محاسبات ابری
- رابط‌های برنامه‌نویسی برنامه‌های کاربردی غیر ایمن
- کارمندان داخلی بدخواه

---

36 Data Governance

37 Legal

38 Resiliency

39 Abuse

40 Nefarious Use

- آسیب‌پذیری‌های فناوری‌های به اشتراک گذاشته‌شده
- نشت و یا از دست دادن داده
- ربودن[41] ترافیک، خدمات و حساب کاربری
- مشخصات ریسک ناشناخته

➢ **Security as a Service (SecaaS) Implementation Guidance**

این راهنمای اجرا به‌عنوان بهترین رویه برای طراحی، پیاده‌سازی، ارزیابی شناسایی و مدیریت دسترسی و به‌طور خاص آن مواردی که درون محاسبات ابری اعمال می‌شوند، می‌باشد. در واقع این راهنما به تصمیمات فنی و کسب‌وکار که باید توسط سازمان‌ها و به‌منظور پیاده‌سازی اجزای امنیت به‌عنوان یک خدمت مدیریت دسترسی و هویت و به‌عنوان بخشی از محیط ابر، مورد استفاده قرار می‌گیرد، می‌پردازد.

➢ **Security Guidance for Critical Areas of Focus in Cloud Computing**

این سند چهارده حوزه کاری را شامل می‌شود. این حوزه‌های کاری با استانداردهای صنعتی و بهترین رویه‌ها، برابری می‌کنند. این سند در واقع به‌عنوان یک عامل مهم در مدیریت استراتژیک خدمات ابر عمل می‌کند. چهارده حوزه کاری شامل موارد زیر می‌باشد:

- حوزه ۱: چارچوب معماری محاسبات ابری؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.
- حوزه ۲: مدیریت ریسک سازمان و دولت؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.
- حوزه ۳: مسائل حقوقی: قراردادها و تشخیص‌های الکترونیکی[42]؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.
- حوزه ۴: مدیریت ممیزی و تطابق‌پذیری؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.
- حوزه ۵: امنیت داده و مدیریت اطلاعات؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.
- حوزه ۶: قابلیت حمل و قابلیت همکاری
- حوزه ۷: امنیت مرسوم[43]، تدوام کسب‌وکار و بازیابی فاجعه؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.

---

41 Hijacking

42 Electronic Discovery

- حوزه ۸: عملیات مرکز داده
- حوزه ۹: پاسخ‌گویی به حادثه؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.
- حوزه ۱۰: امنیت برنامه کاربردی؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.
- حوزه ۱۱: رمزنگاری و مدیریت کلید؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.
- حوزه ۱۲: مدیریت دسترسی؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.
- حوزه ۱۳: مجازی‌سازی؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۷ انجام شده‌است.
- حوزه ۱۴: امنیت به‌عنوان یک خدمت؛ آخرین به‌روز رسانی این حوزه در سال ۲۰۱۶ انجام شده‌است.

➢ Cloud Application Management for Platforms (CAMP)

سند CAMP مؤسسه OASIS در سال ۲۰۱۴ منتشر شد و یک پروتکل تعاملی و سازگاری را ارایه می‌دهد که مجریان ابر می‌توانند از آن برای گسترش برنامه‌های کاربردی خود استفاده کنند. این سند مصنوعات و رابط‌های برنامه‌های کاربردی را تعریف می‌کند که بایستی توسط پلتفرم به‌عنوان یک خدمت ابر به‌منظور مدیریت ایجاد، اجرا، نظارت و وصله برنامه‌های کاربردی در ابر ارایه شود. همچنین CAMP، واسطی را برای تأمین خود خدمتی[۴۴]، نظارت و کنترل، فراهم می‌آورد.

➢ Identity in the Cloud (IDCloud)

کمیته فنی IDCloud موسسه OASIS بر روی پیشبرد استفاده از استانداردهای مدیریت هویت در زمینه محاسبات ابری تمرکز دارد. این امر باعث تولید یک مجموعه از موارد کاربرد مربوط به استفاده از هویت و شناسایی در ابر می‌شود. در واقع هدف از این سند هماهنگی تعاریف، اصطلاحات و واژگان هویت در زمینه محاسبات ابری و توسعه مشخصات استانداردهای باز به‌منظور استقرار، تأمین و مدیریت هویت می‌باشد.

---

[43] Traditional Security

[44] Self-Service

- **Topology and Orchestration Specification for Cloud Applications (TOSCA)**

TOSCA یک استاندارد ابر باز جدید و مهم است که یک اکوسیستم منحصربه‌فرد را فراهم می‌آورد. کمیته فنی TOSCA در مؤسسه OASIS بر روی بهبود قابلیت حمل برنامه‌های کاربردی و خدمات ابر در سراسر چرخه حیات آن‌ها، مطالعه می‌کنند. TOSCA، شرح سازگاری برنامه‌های کاربردی و زیرساخت خدمات ابر، روابط بین بخش‌های خدمات و رفتار عملیاتی این خدمات (به عنوان مثال، توسعه، وصله) را مستقل از منبع ایجاد خدمت و هر ارایه‌دهنده خاص ابر و یا میزبانی وب، فراهم خواهد کرد.

- **Cloud Authorization (CloudAuthZ)**

کمیته فنی CloudAuthZ مدل‌های بهینه‌ای را به‌منظور مدیریت مجوزها و حقوق دسترسی در زمینه‌های SaaS، PaaS، IaaS، توسعه می‌دهد. CloudAuthZ، یک مجموعه از ویژگی‌ها و حقوق دسترسی ضمنی را جهت ارایه به نقاط اجرایی، بصورت بی‌درنگ، فراهم می‌کند. با CloudAuthZ، تصمیمات مجوزدهی می‌توانند با استفاده از داده‌هایی مانند اینکه کاربران کجا هستند، چه‌کاری را انجام می‌دهند، از چه تجهیزاتی استفاده می‌کنند و غیره ، اتخاذ شوند. این تصمیمات می‌توانند منجر به ورود کاربران به ابر و یا مانع ورود آن‌ها شوند.

- **Public Administration Cloud Requirements (PACR)**

دولت‌ها در حال بررسی انتقال بسیاری از سیستم‌های فناوری اطلاعات و ارتباطات به ابر و نیز تأسیسات و خدمات محاسبات توزیع‌شده از راه دور، می‌باشند. البته ماهیت این سیستم‌های جدید نیازمند بعضی از بازبینی‌ها در سیاست‌های عمومی و الزامات پاسخ‌گویی دولت به توابع فناوری اطلاعات و ارتباطات می‌باشد. این استاندارد، الزامات عملیاتی محاسبات ابری را برای ادارات دولتی و به‌منظور فراهم‌آوری تدارکات، تضمین قابلیت ممیزی، آزمون انطباق‌پذیری و معیارهای اکتساب[۴۵]، توسعه می‌دهد.

- **Cloud Data Management Interface (CDMI) specification**

CDMI یک استاندارد انجمن صنعت شبکه‌های ذخیره‌سازی (SNIA)[۴۶] است که یک رابطی را برای دسترسی به مخازن داده ابر و مدیریت داده‌های ذخیره شده در آن را مشخص می‌کند. این استاندارد بین المللی توسط توسعه‌دهندگان، کسانی که مخازن داده ابری را پیاده‌سازی یا استفاده می‌کنند، به‌کار می‌رود. این رابط مدیریت یک

---

[45] Acquisition criteria

[46] Storage Networking Industry Association

واسط عملکردی را تعریف می‌کند که برنامه‌های کاربردی از طریق آن قادرند عملیاتی مانند ایجاد، بازیابی، به‌روزرسانی و حذف عناصر داده از فضای ذخیره‌سازی ابر را انجام دهند.

به‌عنوان بخشی از این رابط، مشتری قادر به کشف قابلیت‌های مخازن ابر پیشنهاد شده و استفاده از این رابط به‌منظور مدیریت داده‌هایی می‌باشد که در این مکان واقع شده‌اند. علاوه‌بر این، فراداده می‌تواند بر روی عناصر داده از طریق این رابط قرار بگیرد.

- **Information technology -- Cloud Data Management Interface (CDMI)**

سازمان SNIA به کمک سازمان ISO/IEC این استاندارد را با هدف استانداردسازی در زمینه فناوری اطلاعات و مخازن ابری منتشر نمود. استاندارد بین‌المللی CDMI رابطی را به‌منظور دسترسی به مخازن ابر و مدیریت اطلاعات ذخیره‌شده در آن، تعریف می‌کند. این سند برای توسعه‌دهندگانی که کار اجرا و استفاده از مخازن ابر را بر عهده دارند، قابل به‌کارگیری می‌باشد.