FedRAMP Master Acronyms and Glossary

Version 1.4

November 20, 2017



Document Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ATE | VERSION | PAGE(S) | DESCRIPTION | AUTHOR |
| 9/10/2015 | 1.0 | All | Initial issue | FedRAMP PMO |
| 4/6/2016 | 1.1 | All | Minor corrections throughout | FedRAMP PMO |
| 8/30/2016 | 1.2 | All | Added Glossary and additional acronyms from all FedRAMP templates and documents | FedRAMP PMO |
| 4/6/2017 | 1.2 | Cover | Updated logo | FedRAMP PMO |
| 11/10/2017 | 1.3 | All | Minor corrections throughout | FedRAMP PMO |
| 11/20/2017 | 1.4 | All | Updated to latest format | FedRAMP PMO |

How to contact us

Questions about FedRAMP or this document should be directed to [info@fedramp.gov](mailto:info@fedramp.gov).

For more information about FedRAMP, visit the website at <http://www.fedramp.gov>.

TABLE OF CONTENTS

1. acronyms 1

2. glossary 9

# acronyms

Below is the master list of FedRAMP acronym definitions for all FedRAMP templates   
and documents.

Please send suggestions about corrections, additions, or deletions to [info@fedramp.gov](mailto:info@fedramp.gov).

Table – Master Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| **3PAO** | Third Party Assessment Organization |
| **A2LA** | American Association of Laboratory Accreditors |
| **AC** | Access Control (SSP Table 13 1 Summary of Required Security Controls) |
| **ACL** | Access Control List |
| **AO** | Authorizing Official |
| **API** | Application Programming Interface |
| **APL** | Approved Products List (DOD list) |
| **ASHRAE** | American Society of Heating, Refrigerating and Air-conditioning Engineers (see PE-14) |
| **AT** | Awareness and Training |
| **ATO** | Authorization To Operate |
| **AU** | Audit and Accountability (SSP Table 13 1 Summary of Required Security Controls) |
| **BCP** | Business Continuity Plan |
| **BIA** | Business Impact Analysis / Business Impact Assessment |
| **C&A** | Certification & Accreditation |
| **CA** | Security Assessment and Authorization (SSP Table 13 1 Summary of Required Security Controls) |
| **CAP** | Corrective Action Plan |
| **CapEx** | Capital Expense |
| **CAPTCHA** | Completely Automated Public Turing test to tell Computers and Humans Apart |
| **CCB** | Change Control Board |
| **CDM** | Continuous Diagnostics and Mitigation |
| **CERT** | Computer Emergency Response Team |
| **CI** | Configuration Item |
| **CIDR** | Classless Inter-Domain Routing |
| **CIOC** | Chief Information Officer Council |
| **CIRT** | Consumer Incident Response Team |
| **CIS** | Control Implementation Summary / Control Information Summary |
| **CISO** | Chief Information Security Officer |
| **CLI** | Command Line Interface |
| **CM** | Configuration Management (SSP Table 13 1 Summary of Required Security Controls) |
| **CMP** | Configuration Management Plan |
| **CMVP** | Cryptographic Module Validation Program |
| **CO** | Contracting Officer |
| **ConMon** | Continuous Monitoring |
| **CONOPS** | Concept of Operations |
| **COOP** | Continuity of Operations Plan |
| **COR** | Contracting Officer’s Representative |
| **COTS** | Commercial Off-The-Shelf |
| **CP** | Contingency Planning (SSP Table 13 1 Summary of Required Security Controls) |
| **CPD** | Contingency Planning Director |
| **CR** | Change Request |
| **CRM** | Customer Relationship Management |
| **CSIRC** | Computer Security Incident Response Center |
| **CSP** | Cloud Service Provider |
| **CTW** | Control Tailoring Workbook |
| **CUI** | Confidential Unclassified Information |
| **DAA** | Designated Approving Authority |
| **DAS** | Direct Attached Storage |
| **DDoS** | Distributed Denial of Service (DDoS) |
| **DHS** | Department of Homeland Security |
| **DMZ** | Demilitarized Zones [SC-7 (13)] |
| **DNS** | Domain Name System |
| **DoD** | Department of Defense |
| **E-Authentication** | Electronic Authentication |
| **EC-Council** | International Council of Electronic Commerce Consultants |
| **ECSB** | Enterprise Cloud Service Broker |
| **FDCCI** | Federal Data Center Consolidation Initiative |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **FIPS** | Federal Information Processing Standards |
| **FIPS 199** | Federal Information Processing Standard Publication 199 |
| **FIPS PUB** | Federal Information Processing Standard Publication |
| **FIPS PUB 199** | Federal Information Processing Standard Publication |
| **FISMA** | Federal Information Security Management Act of 2014 |
| **FOC** | Final Operating Capability |
| **FOIA** | Freedom of Information Act |
| **FTP** | File Transfer Protocol |
| **GIAC** | Global Information Assurance Certification |
| **gov** | Government |
| **GSA** | General Services Administration |
| **GSS** | General Support System |
| **GUI** | Graphical User Interface |
| **HIDS** | Host Intrusion Detection System |
| **HIPAA** | Health Insurance Portability and Accountability Act (of 1996) |
| **HIPS** | Host Intrusion Prevention System |
| **HSM** | Hardware Security Module |
| **HSPD** | Homeland Security Presidential Directive |
| **HSPD 12** | Homeland Security Presidential Directive 12 |
| **HTTP** | Hyper Text Transport Protocol |
| **IA** | Identification and Authentication |
| **IAA** | Inter-Agency Agreement |
| **IaaS** | Infrastructure as a Service (Model) |
| **IAP** | Internet Access Points [SC-7 (13)] |
| **IATO** | Interim Authorization to Operate |
| **ID** | Identification |
| **IEC** | International Electrotechnical Commission |
| **IG** | Inspector General / Implementation Guidance |
| **IOC** | Initial Operating Capability |
| **IP** | Internet Protocol |
| **IPv4** | Internet Protocol version 4 |
| **IPv6** | Internet Protocol version 6 |
| **IR** | Incident Response |
| **ISCP** | This Information Technology Contingency Plan |
| **iSCSI** | Internet Small Computer System Interface |
| **ISIMC** | Information Security and Identity Management Committee |
| **ISO** | International Organization for Standardization |
| **ISO/IEC** | International Organization for Standardization / International Electrotechical Commission |
| **ISP** | Internet Service Provider |
| **ISPP** | Information Security Policies and Procedures |
| **ISSO** | Information System Security Officer |
| **IT** | Information Technology |
| **ITCP** | IT Contingency Plan |
| **JAB** | (FedRAMP) Joint Authorization Board |
| **LAN** | Local Area Network |
| **LMS** | Learning Management System |
| **MA** | Maintenance (SSP Table 13 1 Summary of Required Security Controls) |
| **MAS** | Multiple Award Schedule |
| **MAX** | MAX.gov (Secure Repository) |
| **mil** | Military |
| **MOU** | Memorandum of Understanding |
| **MP** | Media Protection (SSP Table 13 1 Summary of Required Security Controls) |
| **MSSP** | Managed Security Service Provider |
| **MT** | Manual Test |
| **MTIPS** | Managed Trusted IP Service |
| **N/A** | Not Applicable |
| **NARA** | National Archives and Records Administration |
| **NAS** | Network Attached Storage |
| **NAT** | Network Address Translation |
| **NFPA** | National Fire Protection Association |
| **NGO** | Non-Governmental Organization |
| **NIAP** | National Information Assurance Partnership [IA-2 (11)] |
| **NISP** | National Industrial Security Program |
| **NIST** | National Institute of Standards and Technology |
| **NIST-SP** | NIST Special Publication |
| **NLA** | No Logical Access (SSP Table 9 1 Personnel Roles and Privileges) |
| **NNTP** | Network News Transfer Protocol |
| **NP** | Non-Privileged (SSP Table 9 1 Personnel Roles and Privileges) |
| **NPPD** | National Protection and Programs Directorate (of DHS) |
| **NTP** | Network Time Protocol |
| **NVI** | NAT Virtual Interface |
| **ODAL** | Outage and Damage Assessment Lead |
| **OEP** | Occupant Emergency Plan |
| **OIG** | Office of the Inspector General |
| **OMB** | Office of Management and Budget |
| **OpEx** | Operating Expense |
| **OR** | Operational Requirement |
| **OSINT** | Open Source Intelligence |
| **OWASP** | Open Web Application Security Project |
| **P** | Privileged (SSP Table 9 1 Personnel Roles and Privileges) |
| **PA** | Provisional Authorization |
| **PaaS** | Platform as a Service (Model) |
| **P-ATO** | Provisional Authorization to Operate |
| **PDF** | Portable Document Format |
| **PDS** | Protective Distribution System |
| **PE** | Physical and Environmental Protection (SSP Table 13 1 Summary of Required Security Controls) |
| **PIA** | Privacy Impact Assessment |
| **PII** | Personally Identifiable Information |
| **PIV** | Personal Identity Verification |
| **PKI** | Public Key Infrastructure [SC-7 (13)] |
| **PL** | Planning (SSP Table 13 1 Summary of Required Security Controls) |
| **PL** | Public Law |
| **PLC** | Procurement and Logistics Coordinator |
| **PM** | Program Management |
| **PMO** | Program Management Office |
| **POA&M** | Plan of Action and Milestones |
| **POC** | Point of Contact |
| **PS** | Personnel Security (SSP Table 13 1 Summary of Required Security Controls) |
| **PTA** | Privacy Threshold Analysis |
| **PTR** | Penetration Test Report |
| **PUB** | Publication |
| **QA** | Quality Assurance |
| **QC** | Quality Control |
| **QM** | Quality Management |
| **R1** | Revision 1 |
| **RA** | Risk Assessment |
| **RBAC** | Role-Based Access Control |
| **Rev** | Revision |
| **RFC** | Request for Change |
| **RFI** | Request for Information |
| **RFP** | Request for Proposal |
| **RIP** | Routing Information Protocol |
| **RMF** | Risk Management Framework |
| **RoB** | Rules of Behavior |
| **ROE** | Rules of Engagement |
| **RTO** | Recovery Time Objective |
| **SA** | System and Services Acquisition (SSP Table 13 1 Summary of Required Security Controls) |
| **SA** | Security Assessment |
| **SaaS** | Software as a Service |
| **SAF** | Security Assessment Framework |
| **SAML** | Security Assertion Markup Language |
| **SAN** | Storage Area Networks |
| **SAP** | Security Assessment Plan |
| **SAR** | Security Assessment Report |
| **SAS** | Security Assessment Support |
| **SC** | System and Communications Protection (SSP Table 13 1 Summary of Required Security Controls) |
| **SCSI** | Small Computer System Interface |
| **SDLC** | System Development Life Cycle |
| **SI** | System and Information Integrity (SSP Table 13 1 Summary of Required Security Controls) |
| **SLA** | Service Level Agreement |
| **SME** | Subject Matter Expert |
| **SMS** | Short Message Service |
| **SMTP** | Simple Mail Transfer Protocol |
| **SOP** | Standard Operating Procedure |
| **SORN** | System of Records Notice |
| **SP** | Service Processor (SSP Table 11 1 System Interconnections) |
| **SP** | Special Publication |
| **SQL** | Structured Query Language |
| **SSL** | Secure Sockets Layer |
| **SSO** | Single Sign-On |
| **SSP** | System Security Plan |
| **TCP** | Transmission Control Protocol |
| **TFTP** | Trivial FTP |
| **TIC** | Trusted Internet Connection |
| **TICAP** | Trusted Internet Connection Access Providers |
| **TLS** | Transport Layer Security |
| **TP** | Test Plan |
| **TR** | Technical Representative |
| **TR-R** | Technical Representative’s Representative |
| **TTS** | Technology Transformation Services |
| **US** | United States |
| **UDP** | User Diagram Protocol |
| **UPS** | Uninterruptable Power Supply |
| **URL** | uniform resource locator |
| **USC** | United States Code |
| **US-CERT** | United States Computer Emergency Readiness Team |
| **UUCP** | Unix-to-Unix Copy Protocol |
| **V2** | Version 2 |
| **VLAN** | Virtual Local Area Network |
| **VPN** | Virtual Private Network (SSP Table 11 1 System Interconnections) |

# 

# glossary

Below is the master list of FedRAMP glossary terms for all FedRAMP templates.

Please send suggestions about corrections, additions, or deletions to [info@fedramp.gov](mailto:info@fedramp.gov).

Table – Master Glossary

|  |  |
| --- | --- |
| term | meaning |
| **Agency Authorization to Operate** | An Agency ATO is an authorization that is issued by a Federal Department, Office, or Agency. |
| **Cloud Access** | To make contact with or gain access to Cloud Services. |
| **Cloud Auditor** | A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation. |
| **Cloud Broker** | An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers. |
| **Cloud Carrier** | The intermediary that provides connectivity and transport of cloud services between Cloud Providers and Cloud Consumers. |
| **Cloud Consumer** | Person or organization that maintains a business relationship with, and uses services from, Cloud Service Providers. |
| **Cloud Distribution** | The process of transporting cloud data between Cloud Providers and Cloud Consumers. |
| **Cloud Provider** | Person, organization or entity responsible for making a service available to service consumers. |
| **Cloud Service Management** | Cloud Service Management includes all the service-related functions that are necessary for the management and operations of those services required by or proposed to customers. |
| **Community Cloud** | The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. |
| **Configured by Customer** | A control here the customer needs to apply a configuration in order to meet the control requirement. |
| **Data Portability** | The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. |
| **FedRAMP Authorization Package** | Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. This includes, as a minimum, the Security Plan, Security Assessment Report, Plan of Action and Milestones and a Continuous Monitoring Plan. |
| **FedRAMP Authorized** | TBD, after differences are settled. |
| **FedRAMP In-Process** | FedRAMP In-Process is a designation for Applicants that are in the JAB P-ATO or Agency ATO [authorization application] paths. |
| **FedRAMP P-ATO** | FedRAMP Provisional Authorization to Operate.  A provisional authorization is an initial statement of risk and approval of an authorization package by the JAB pending the issuance of a final authorization to operate by the Executive department or agency acquiring the cloud service. |
| **FedRAMP Ready** | FedRAMP Ready is a designation which is intended to demonstrate a CSP's ability to complete the full FedRAMP authorization process. It is a mandatory step in pursuing a JAB P-ATO authorization and is optional for those pursuing an Agency-based FedRAMP Authorization. To be listed as FedRAMP Ready, CSPs work with a 3PAO to submit a Readiness Assessment Report which must be reviewed and approved by the FedRAMP PMO. |
| **Fixed Endpoints** | A physical device, fixed in its location that provided a man/machine interface to cloud services and applications. A fixed endpoint typically uses one method and protocol to connect to cloud services and applications. |
| **Hybrid Cloud** | The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). |
| **Information System Security Officer (ISSO)** | The FedRAMP ISSO refers to the ISSO who reviews security packages intended for the JAB. |
| **Infrastructure as a Service (IaaS)** | The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). |
| **Inherited from  pre-existing Authorization** | A control that is inherited from another CSP Name system that has already received an Authorization. |
| **Interoperability** | The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions. |
| **Joint Authorization Board** | The JAB consists of the CIOs of the DOD, GSA, and the DHS. |
| **Joint Authorization Board Provisional Authorization to Operate** | A FedRAMP JAB P-ATO is a FedRAMP Provisional Authorization to Operate issued by the JAB. |
| **Metering** | Provide a measuring capability at some level of abstraction appropriate to the type of service (e.g, storage, processing, bandwidth, and active user accounts). |
| **Mobile Endpoints** | A physical device, often carried by the user that provided a man/machine interface to cloud services and applications. A Mobile Endpoint may use multiple methods and protocols to connect to cloud services and applications. |
| **Monitoring and Reporting** | Discover and monitor the virtual resources, monitor cloud operations and events, and generate performance reports. |
| **Performance Audit** | Systematic evaluation of a cloud system by measuring how well it conforms to a set of established performance criteria. |
| **Physical Resource Layer** | Includes all the physical resources used to provide cloud services, most notably, the hardware and the facility. |
| **Platform as a Service** | The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. |
| **Portability** | 1. The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. 2. The ability of software or of a system to run on more than one type or size of computer under more than one operating system. See POSIX. 3. Of equipment, the quality of being able to function normally while being conveyed. |
| **Privacy** | Information privacy is the assured, proper, and consistent collection, processing, communication, use and disposition of disposition of personal information (PI) and personally identifiable information (PII) throughout its life cycle. |
| **Privacy-Impact Audit** | Systematic evaluation of a cloud system by measuring how well it conforms to a set of established privacy-impact criteria. |
| **Private Cloud** | The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. |
| **Provided by Customer** | A control where the customer needs to provide additional hardware or software in order to meet the control requirement. |
| **Provisioning/ Configuration** | Process of preparing and equipping a cloud to allow it to provide services to its users. |
| **Public Cloud** | The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. |
| **Rapid Provisioning** | Automatically deploying cloud system based on the requested service/resources/capabilities. |
| **Resource Abstraction and Control Layer** | Entails software elements, such as hypervisor, virtual machines, virtual data storage, and supporting software components, used to realize the infrastructure upon which a cloud service can be established. |
| **Resource Change** | Adjust configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud. |
| **Security** | Refers to information security. "Information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. |
| **Security Audit** | Systematic evaluation of a cloud system by measuring how well it conforms to a set of established security criteria. |
| **Service Aggregation** | An aggregation brokerage service combines multiple services into one or more new services. It will ensure that data is modeled across all component services and integrated as well as ensuring the movement and security of data between the service consumer and multiple providers. |
| **Service Arbitrage** | Cloud service arbitrage is similar to cloud service aggregation. The difference between them is that the services being aggregated are not fixed. Indeed the goal of arbitrage is to provide flexibility and opportunistic choices for the service aggregator, e.g., providing multiple email services through one service provider or providing a credit-scoring service that checks multiple scoring agencies and selects the best score. |
| **Service Consumption** | A Cloud Broker in the act of using a Cloud Service. |
| **Service Deployment** | All of the activities and organization needed to make a cloud service available. |
| **Service Intermediation** | An intermediation broker provides a service that directly enhances a given service delivered to one or more service consumers, essentially adding value on top of a given service to enhance some specific capability. |
| **Service Provider Corporate** | A control that originates from the CSP Name corporate network. |
| **Service Provider Hybrid** | A control that makes use of both corporate controls and additional controls specific to a particular system at the CSP Name. |
| **Service Provider System Specific** | A control specific to a particular system at the CSP Name and the control is not part of the service provider corporate controls. |
| **Shared** | A control that is managed and implemented partially by the CSP Name and partially by the customer. |
| **Support Team** | The FedRAMP support team is the group of individuals that responds to info@fedramp.gov. |
| **Threat** | An adversarial force or phenomenon that could impact the availability, integrity, or confidentiality of an information system and its networks including the facility that houses the hardware and software. |
| **Threat Actor** | An entity that initiates the launch of a threat agent is referred to as a threat actor. |
| **Threat Agent** | An element that provides the delivery mechanism for a threat. |
| **Validation and Verification** | [The PMBOK guide](https://en.wikipedia.org/wiki/A_Guide_to_the_Project_Management_Body_of_Knowledge), a standard adopted by [IEEE](https://en.wikipedia.org/wiki/IEEE), defines them as follows in its 4th edition:[[2]https://en.wikipedia.org/wiki/Verification\_and\_validation - cite\_note-pmboked4-2](https://en.wikipedia.org/wiki/Verification_and_validation#cite_note-pmboked4-2)  "Validation. The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers. Contrast with verification."  "Verification. The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process. Contrast with validation." |
| **Vulnerability** | An inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact in the protection of the confidentiality, integrity, or availability of the system (application and associated data). |