FedRAMP Master
Acronym and Glossary

Version 1.6
07/23/2020
# DOCUMENT REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Page(s)</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/10/2015</td>
<td>1.0</td>
<td>All</td>
<td>Initial issue</td>
<td>FedRAMP PMO</td>
</tr>
<tr>
<td>04/06/2016</td>
<td>1.1</td>
<td>All</td>
<td>Addressed minor corrections throughout document</td>
<td>FedRAMP PMO</td>
</tr>
<tr>
<td>08/30/2016</td>
<td>1.2</td>
<td>All</td>
<td>Added Glossary and additional acronyms from all FedRAMP templates and documents</td>
<td>FedRAMP PMO</td>
</tr>
<tr>
<td>04/06/2017</td>
<td>1.2</td>
<td>Cover</td>
<td>Updated FedRAMP logo</td>
<td>FedRAMP PMO</td>
</tr>
<tr>
<td>11/10/2017</td>
<td>1.3</td>
<td>All</td>
<td>Addressed minor corrections throughout document</td>
<td>FedRAMP PMO</td>
</tr>
<tr>
<td>11/20/2017</td>
<td>1.4</td>
<td>All</td>
<td>Updated to latest FedRAMP template format</td>
<td>FedRAMP PMO</td>
</tr>
<tr>
<td>07/01/2019</td>
<td>1.5</td>
<td>All</td>
<td>Updated Glossary and Acronyms list to reflect current FedRAMP template and document terminology</td>
<td>FedRAMP PMO</td>
</tr>
<tr>
<td>07/01/2020</td>
<td>1.6</td>
<td>All</td>
<td>Updated to align with terminology found in current FedRAMP templates and documents</td>
<td>FedRAMP PMO</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About This Document</td>
<td>1</td>
</tr>
<tr>
<td>Who Should Use This Document</td>
<td>1</td>
</tr>
<tr>
<td>How To Contact Us</td>
<td>1</td>
</tr>
<tr>
<td>Acronyms</td>
<td>1</td>
</tr>
<tr>
<td>Glossary</td>
<td>15</td>
</tr>
</tbody>
</table>
About This Document

This document provides a list of acronyms used in FedRAMP documents and templates, as well as a glossary. There is nothing to fill out in this document.

Who Should Use This Document

This document is intended to be used by individuals who use FedRAMP documents and templates.

How To Contact Us

Questions about FedRAMP, or this document, should be directed to info@fedramp.gov.
For more information about FedRAMP, visit the website at https://www.fedramp.gov.

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.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3PAO</td>
<td>Third Party Assessment Organization</td>
</tr>
<tr>
<td>A2LA</td>
<td>American Association of Laboratory Accreditation</td>
</tr>
<tr>
<td>AA</td>
<td>Annual Assessment</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>AAL</td>
<td>Authenticator Assurance Level</td>
</tr>
<tr>
<td>AC</td>
<td>Access Control (security control family)</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants</td>
</tr>
<tr>
<td>AO</td>
<td>Authorizing Official</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>APL</td>
<td>Approved Products List (DoD)</td>
</tr>
<tr>
<td>ASHRAE</td>
<td>American Society of Heating, Refrigerating and Air-conditioning Engineers</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness and Training (security control family)</td>
</tr>
<tr>
<td>ATO</td>
<td>Authority to Operate</td>
</tr>
<tr>
<td>AU</td>
<td>Audit and Accountability (security control family)</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>BCR</td>
<td>Baltimore Cyber Range</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis / Business Impact Assessment</td>
</tr>
<tr>
<td>BOD</td>
<td>Binding Operational Directive (DHS)</td>
</tr>
<tr>
<td>BPA</td>
<td>Blanket Purchase Agreement</td>
</tr>
<tr>
<td>C&amp;A</td>
<td>Certification and Accreditation</td>
</tr>
<tr>
<td>CA</td>
<td>Security Assessment and Authorization (security control family)</td>
</tr>
<tr>
<td>CAC</td>
<td>Common Access Card</td>
</tr>
<tr>
<td>CAP</td>
<td>Corrective Action Plan</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>Completely Automated Public Turing test to tell Computers and Humans Apart</td>
</tr>
<tr>
<td>CCB</td>
<td>Change Control Board / Configuration Control Board</td>
</tr>
<tr>
<td>CDM</td>
<td>Continuous Diagnostics and Mitigation</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>Compact Disc Read-Only Memory</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Readiness Team</td>
</tr>
<tr>
<td>CI</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>CI/CD</td>
<td>Continuous Integration/Continuous Deployment</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, Integrity, Availability</td>
</tr>
<tr>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>CIM</td>
<td>Common Information Model</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CIOC</td>
<td>Chief Information Officer Council</td>
</tr>
<tr>
<td>CIRT</td>
<td>Computer Incident Response Team</td>
</tr>
<tr>
<td>CIS</td>
<td>Control Implementation Summary</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management (security control family)</td>
</tr>
<tr>
<td>CMMI</td>
<td>Capability Maturity Model Integration</td>
</tr>
<tr>
<td>CMP</td>
<td>Configuration Management Plan</td>
</tr>
<tr>
<td>CMVP</td>
<td>Cryptographic Module Validation Program</td>
</tr>
<tr>
<td>CO</td>
<td>Contracting Officer</td>
</tr>
<tr>
<td>CoLo</td>
<td>Co Location</td>
</tr>
<tr>
<td>ConMon</td>
<td>Continuous Monitoring</td>
</tr>
<tr>
<td>CONOPS</td>
<td>Concept of Operations</td>
</tr>
<tr>
<td>CONUS</td>
<td>Continental/Contiguous United States</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity of Operations Plan</td>
</tr>
<tr>
<td>COR</td>
<td>Contracting Officer’s Representative</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-The-Shelf</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning (security control family)</td>
</tr>
<tr>
<td>CPC</td>
<td>Contingency Planning Coordinator</td>
</tr>
<tr>
<td>CPD</td>
<td>Contingency Planning Director</td>
</tr>
<tr>
<td>CR</td>
<td>Change Request</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Responsibility Matrix or Customer Relationship Management</td>
</tr>
<tr>
<td>CSA</td>
<td>Cloud Security Alliance</td>
</tr>
<tr>
<td>CSIRC</td>
<td>Computer Security Incident Response Center</td>
</tr>
<tr>
<td>CSO</td>
<td>Cloud Service Offering</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma Separated Values</td>
</tr>
<tr>
<td>CTO</td>
<td>Chief Technology Officer</td>
</tr>
<tr>
<td>CTW</td>
<td>Control Tailoring Workbook</td>
</tr>
<tr>
<td>CUI</td>
<td>Controlled Unclassified Information</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures</td>
</tr>
<tr>
<td>CVSS</td>
<td>Common Vulnerability Scoring System</td>
</tr>
<tr>
<td>D&amp;A</td>
<td>Document and Assess (LI-SaaS)</td>
</tr>
<tr>
<td>DAA</td>
<td>Designated Approving Authority</td>
</tr>
<tr>
<td>DAS</td>
<td>Direct Attached Storage</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DFR</td>
<td>Detailed Finding Review</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DISA</td>
<td>Defense Information Systems Agency</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System / Domain Name Server</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>Domain Name System Security Extensions</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DoH</td>
<td>DNS over HTTPS</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DoT</td>
<td>DNS over TLS</td>
</tr>
<tr>
<td>DR</td>
<td>Deviation Request</td>
</tr>
<tr>
<td>DS</td>
<td>Database Scan</td>
</tr>
<tr>
<td>EA</td>
<td>Enterprise Architecture (OMB)</td>
</tr>
<tr>
<td>E-Authentication</td>
<td>Electronic Authentication</td>
</tr>
<tr>
<td>E-Discovery</td>
<td>Electronic Discovery</td>
</tr>
<tr>
<td>EC-Council</td>
<td>International Council of Electronic Commerce Consultants</td>
</tr>
<tr>
<td>ECSB</td>
<td>Enterprise Cloud Service Broker</td>
</tr>
<tr>
<td>ESI</td>
<td>Electronically Stored Information</td>
</tr>
<tr>
<td>FAL</td>
<td>Federation Assurance Level</td>
</tr>
<tr>
<td>FAQ</td>
<td>Frequently Asked Questions</td>
</tr>
<tr>
<td>FAR</td>
<td>Federal Acquisition Regulation</td>
</tr>
<tr>
<td>FDCCI</td>
<td>Federal Data Center Consolidation Initiative</td>
</tr>
<tr>
<td>FDIC</td>
<td>Federal Deposit Insurance Corporation</td>
</tr>
<tr>
<td>FED</td>
<td>Federal Government</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>Federal Risk and Authorization Management Program</td>
</tr>
<tr>
<td>FFRDC</td>
<td>Federally Funded Research and Development Center</td>
</tr>
<tr>
<td>FICAM</td>
<td>Federal Identity, Credential, and Access Management</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>FIPS PUB</td>
<td>Federal Information Processing Standard Publication</td>
</tr>
<tr>
<td>FOC</td>
<td>Final Operating Capability</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td>FP</td>
<td>False Positive</td>
</tr>
<tr>
<td>FPS</td>
<td>Federal Protective Service</td>
</tr>
<tr>
<td>FRA</td>
<td>Federal Records Act</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GFI</td>
<td>Government Furnished Information</td>
</tr>
<tr>
<td>GIAC</td>
<td>Global Information Assurance Certification</td>
</tr>
<tr>
<td>GMT</td>
<td>Greenwich Mean Time</td>
</tr>
<tr>
<td>GSA</td>
<td>General Services Administration</td>
</tr>
<tr>
<td>GSS</td>
<td>General Support System</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HF</td>
<td>High Frequency</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host Intrusion Detection System</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HIPS</td>
<td>Host Intrusion Prevention System</td>
</tr>
<tr>
<td>HRT</td>
<td>Hardware Recovery Team</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>HSPD</td>
<td>Homeland Security Presidential Directive</td>
</tr>
<tr>
<td>HSTS</td>
<td>HTTP Strict Transport Security</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>HW</td>
<td>Hardware</td>
</tr>
<tr>
<td>IA</td>
<td>Identification and Authentication (security control family)</td>
</tr>
<tr>
<td>IA</td>
<td>Independent Auditor / Assessor</td>
</tr>
<tr>
<td>IAA</td>
<td>Inter-Agency Agreement</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>IAL</td>
<td>Identity Assurance Level</td>
</tr>
<tr>
<td>IAO</td>
<td>Independent Assessment Organizations</td>
</tr>
<tr>
<td>IAP</td>
<td>Internet Access Points</td>
</tr>
<tr>
<td>IAW</td>
<td>In Accordance With</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>IG</td>
<td>Inspector General</td>
</tr>
<tr>
<td>IOC</td>
<td>Initial Operating Capability</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPT</td>
<td>Integrated Product Team</td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response (security control family)</td>
</tr>
<tr>
<td>IRP</td>
<td>Incident Response Plan</td>
</tr>
<tr>
<td>IS</td>
<td>Information System</td>
</tr>
<tr>
<td>ISA</td>
<td>Interconnection Security Agreement</td>
</tr>
<tr>
<td>ISCP</td>
<td>Information System Contingency Plan</td>
</tr>
<tr>
<td>iSCSI</td>
<td>Internet Small Computer System Interface</td>
</tr>
<tr>
<td>ISConMon</td>
<td>Information Security Continuous Monitoring</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>ISIMC</td>
<td>Information Security and Identity Management Committee</td>
</tr>
<tr>
<td>ISO/IEC</td>
<td>International Organization for Standardization / International Electrotechnical Commission</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>ISPP</td>
<td>Information Security Policies and Procedures</td>
</tr>
<tr>
<td>ISSO</td>
<td>Information System Security Officer</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITCP</td>
<td>IT Contingency Plan</td>
</tr>
<tr>
<td>IV&amp;V</td>
<td>Independent Verification and Validation</td>
</tr>
<tr>
<td>IXP</td>
<td>Internet Exchange Point</td>
</tr>
<tr>
<td>JAB</td>
<td>Joint Authorization Board (FedRAMP)</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LI-SaaS</td>
<td>Low Impact Software as a Service</td>
</tr>
<tr>
<td>LMS</td>
<td>Learning Management System</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance (security control family)</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MAX</td>
<td>MAX.gov (Secure Repository)</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi-Factor Authentication</td>
</tr>
<tr>
<td>MOA</td>
<td>Memorandum of Agreement</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MP</td>
<td>Media Protection (security control family)</td>
</tr>
<tr>
<td>MSSP</td>
<td>Managed Security Service Provider</td>
</tr>
<tr>
<td>MT</td>
<td>Manual Test</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>MTIPS</td>
<td>Managed Trusted IP Service</td>
</tr>
<tr>
<td>N/A</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>NARA</td>
<td>National Archives and Records Administration</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NDA</td>
<td>Non-Disclosure Agreement</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Network Basic Input/Output System</td>
</tr>
<tr>
<td>NFPA</td>
<td>National Fire Protection Association</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-Governmental Organization</td>
</tr>
<tr>
<td>NIAP</td>
<td>National Information Assurance Partnership</td>
</tr>
<tr>
<td>NIS</td>
<td>Network Information System</td>
</tr>
<tr>
<td>NISP</td>
<td>National Industrial Security Program</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NIST SP</td>
<td>NIST Special Publication</td>
</tr>
<tr>
<td>NNTP</td>
<td>Network News Transfer Protocol</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
</tr>
<tr>
<td>NPPD</td>
<td>National Protection and Programs Directorate (DHS)</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>NTTAA</td>
<td>National Technology Transfer and Advancement Act</td>
</tr>
<tr>
<td>NVD</td>
<td>National Vulnerability Database</td>
</tr>
<tr>
<td>NVI</td>
<td>NAT Virtual Interface</td>
</tr>
<tr>
<td>ODAL</td>
<td>Outage and Damage Assessment Lead</td>
</tr>
<tr>
<td>OEP</td>
<td>Occupant Emergency Plan</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>OGC</td>
<td>Office of the General Counsel</td>
</tr>
<tr>
<td>OIG</td>
<td>Office of the Inspector General</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>OR</td>
<td>Operational Requirement</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSINT</td>
<td>Open Source Intelligence</td>
</tr>
<tr>
<td>OSCAL</td>
<td>Open Security Controls Assessment Language</td>
</tr>
<tr>
<td>OSCP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>P&amp;P</td>
<td>Policies and Procedures</td>
</tr>
<tr>
<td>PA</td>
<td>Provisional Authorization</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>P-ATO</td>
<td>Provisional Authority to Operate</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry (Data Security Standard)</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>PDS</td>
<td>Protective Distribution System</td>
</tr>
<tr>
<td>PE</td>
<td>Physical and Environmental Protection (security control family)</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Assessment</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PL</td>
<td>Planning (security control family)</td>
</tr>
<tr>
<td>PL</td>
<td>Public Law</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>PLC</td>
<td>Procurement and Logistics Coordinator</td>
</tr>
<tr>
<td>PM</td>
<td>Program Management</td>
</tr>
<tr>
<td>PMO</td>
<td>Program Management Office</td>
</tr>
<tr>
<td>POA&amp;M</td>
<td>Plan of Action and Milestones</td>
</tr>
<tr>
<td>POC</td>
<td>Point of Contact</td>
</tr>
<tr>
<td>POSIX</td>
<td>Portable Operating System Interface</td>
</tr>
<tr>
<td>PS</td>
<td>Personnel Security (security control family)</td>
</tr>
<tr>
<td>PTA</td>
<td>Privacy Threshold Analysis</td>
</tr>
<tr>
<td>PTR</td>
<td>Penetration Test Report</td>
</tr>
<tr>
<td>PUB</td>
<td>Publication</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>QC</td>
<td>Quality Control</td>
</tr>
<tr>
<td>QM</td>
<td>Quality Management</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment (security control family)</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Adjustment</td>
</tr>
<tr>
<td>RAR</td>
<td>Readiness Assessment Report</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-Based Access Control</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Change</td>
</tr>
<tr>
<td>RFI</td>
<td>Request for Information</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Proposal</td>
</tr>
<tr>
<td>RFQ</td>
<td>Request for Quotation</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>RMF</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>ROB</td>
<td>Rules of Behavior</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>ROE</td>
<td>Rules of Engagement</td>
</tr>
<tr>
<td>ROI</td>
<td>Return On Investment</td>
</tr>
<tr>
<td>RP</td>
<td>Relying Party</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>SA</td>
<td>System and Services Acquisition (security control family)</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAF</td>
<td>Security Assessment Framework</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SAP</td>
<td>Security Assessment Plan</td>
</tr>
<tr>
<td>SAR</td>
<td>Security Assessment Report</td>
</tr>
<tr>
<td>SAS</td>
<td>Security Assessment Support</td>
</tr>
<tr>
<td>SC</td>
<td>System and Communications Protection (security control family)</td>
</tr>
<tr>
<td>SC</td>
<td>Security Coordinator</td>
</tr>
<tr>
<td>SCAP</td>
<td>Security Content Automation Protocol</td>
</tr>
<tr>
<td>SCR</td>
<td>Significant Change Request</td>
</tr>
<tr>
<td>SCSI</td>
<td>Small Computer System Interface</td>
</tr>
<tr>
<td>SD</td>
<td>Secure Digital</td>
</tr>
<tr>
<td>SDLC</td>
<td>System Development Life Cycle</td>
</tr>
<tr>
<td>SI</td>
<td>System and Information Integrity (security control family)</td>
</tr>
<tr>
<td>SIA</td>
<td>Security Impact Analysis</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SME</td>
<td>Subject Matter Expert</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SO</td>
<td>System Owner</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Center</td>
</tr>
<tr>
<td>SOC</td>
<td>System and Organization Controls (AICPA)</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SORN</td>
<td>System of Records Notice</td>
</tr>
<tr>
<td>SP</td>
<td>Service Processor</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SRT</td>
<td>Software Recovery Team</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>SSP</td>
<td>System Security Plan</td>
</tr>
<tr>
<td>SDO</td>
<td>Standards Developing Organization</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>TAA</td>
<td>Trade Agreements Act</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial FTP</td>
</tr>
<tr>
<td>TIC</td>
<td>Trusted Internet Connection</td>
</tr>
<tr>
<td>TICAP</td>
<td>Trusted Internet Connection Access Providers</td>
</tr>
<tr>
<td>TLD</td>
<td>Top Level Domain</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TOS</td>
<td>Terms of Service</td>
</tr>
<tr>
<td>TP</td>
<td>Test Plan</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>TR</td>
<td>Technical Representative / Reviewer</td>
</tr>
<tr>
<td>TT</td>
<td>Telecommunications Team</td>
</tr>
<tr>
<td>TTS</td>
<td>Technology Transformation Services</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra-High Frequency</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USGCB</td>
<td>United States Government Configuration Baseline</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>USC</td>
<td>United States Code</td>
</tr>
<tr>
<td>US-CERT</td>
<td>United States Computer Emergency Readiness Team</td>
</tr>
<tr>
<td>UTC</td>
<td>Universal Time Coordinated</td>
</tr>
<tr>
<td>UUCP</td>
<td>Unix-to-Unix Copy Protocol</td>
</tr>
<tr>
<td>VD</td>
<td>Vendor Dependency</td>
</tr>
<tr>
<td>VHF</td>
<td>Very High Frequency</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over Internet Protocol</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
# 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.

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Authority to Operate</td>
<td>An authorization that is issued by a federal department, office, or agency</td>
</tr>
<tr>
<td>Cloud Access</td>
<td>To make contact with or gain access to a cloud service</td>
</tr>
<tr>
<td>Cloud Auditor</td>
<td>A party that can conduct independent assessment of cloud services, information system operations, and/or performance and security of the cloud implementation</td>
</tr>
<tr>
<td>Cloud Broker</td>
<td>An entity that manages the use, performance, and delivery of cloud services and negotiates relationships between Cloud Providers and Cloud Consumers</td>
</tr>
<tr>
<td>Cloud Carrier</td>
<td>The intermediary that provides connectivity and transport of cloud services between Cloud Service Providers and Cloud Consumers</td>
</tr>
<tr>
<td>Cloud Consumer</td>
<td>Person or organization that maintains a business relationship with, and uses services from, Cloud Service Providers</td>
</tr>
<tr>
<td>Cloud Distribution</td>
<td>The process of transporting cloud data between Cloud Service Providers and Cloud Consumers</td>
</tr>
<tr>
<td>Cloud Provider</td>
<td>A person, organization or entity responsible for making a service available to service consumers</td>
</tr>
<tr>
<td>Cloud Service Management</td>
<td>Includes all the service-related functions that are necessary for the management and operations of those services required by or proposed to customers</td>
</tr>
<tr>
<td>Community Cloud</td>
<td>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.</td>
</tr>
<tr>
<td>Configured by Customer</td>
<td>A control where the customer needs to apply a configuration in order to meet the control requirement</td>
</tr>
<tr>
<td><strong>Container</strong></td>
<td>A container consists of an entire runtime environment: an application, plus all its dependencies, libraries and other binaries, and configuration files needed to run it, bundled into one package.</td>
</tr>
<tr>
<td><strong>CSA STAR Certification</strong></td>
<td>The CSA STAR Certification is a third party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001 management system standard together with the CSA Cloud Controls Matrix, a specified set of criteria that measures the capability levels of the cloud service.</td>
</tr>
<tr>
<td><strong>Data Portability</strong></td>
<td>The ability to transfer data from one system to another without being required to recreate or re-enter data descriptions or to modify significantly the application being transported.</td>
</tr>
<tr>
<td><strong>Digital Authentication</strong></td>
<td>The process of establishing confidence in user identities presented digitally to a system, which was previously referred to as Electronic Authentication (E-Authentication)</td>
</tr>
<tr>
<td><strong>FedRAMP Accelerated</strong></td>
<td>A FedRAMP initiative to reduce the decision time for applications for a JAB P-ATO to six months. FedRAMP Accelerated is now the JAB Authorization Process. See FedRAMP Accelerated, A Case Study for Change Within Government.</td>
</tr>
<tr>
<td><strong>FedRAMP Authorization Package</strong></td>
<td>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 System Security Plan (SSP) and its attachments, a Security Assessment Report (SAR), a Plan of Action and Milestones (POA&amp;M) and a Continuous Monitoring Plan.</td>
</tr>
<tr>
<td><strong>FedRAMP Connect</strong></td>
<td>The process facilitated by the FedRAMP PMO by which CSPs are evaluated against the prioritization criteria and recommended to the JAB and CIO Council to work toward a JAB P-ATO</td>
</tr>
<tr>
<td><strong>FedRAMP In-Process</strong></td>
<td>FedRAMP In-Process is a designation provided to CSPs that are actively working toward a FedRAMP Authorization with either the JAB or a federal agency</td>
</tr>
<tr>
<td><strong>FedRAMP P-ATO</strong></td>
<td>A FedRAMP Provisional Authority to Operate is an initial statement of risk and approval of an authorization package by the JAB, pending the issuance of a final Authority to Operate by the executive department or agency acquiring the cloud service.</td>
</tr>
<tr>
<td><strong>FedRAMP Ready</strong></td>
<td>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 (RAR) which must be reviewed and approved by the FedRAMP PMO.</td>
</tr>
<tr>
<td><strong>FedRAMP Tailored</strong></td>
<td>For Low Impact Software as a Service (LI-SaaS); see <a href="https://tailored.fedramp.gov/policy/">https://tailored.fedramp.gov/policy/</a></td>
</tr>
<tr>
<td>Federal Information Processing Standards (FIPS)</td>
<td>Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves the standards and guidelines that the National Institute of Standards and Technology (NIST) develops for federal computer systems. NIST issues these standards and guidelines as Federal Information Processing Standards (FIPS) for governmentwide use. NIST develops FIPS when there are compelling federal government requirements, such as for security and interoperability, and there are no acceptable industry standards or solutions. FIPS documents are available online on the FIPS home page: <a href="http://www.nist.gov/itl/fips.cfm">http://www.nist.gov/itl/fips.cfm</a>.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Fixed Endpoints</td>
<td>A physical device, fixed in its location, which provides 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.</td>
</tr>
<tr>
<td>Government Only Cloud</td>
<td>A cloud deployment model (see SSP Table 8-2). The cloud services and infrastructure are shared by several organizations/agencies with the same policy and compliance considerations.</td>
</tr>
<tr>
<td>Hybrid Cloud</td>
<td>A cloud deployment model (see SSP Table 8-2). The cloud services and infrastructure are 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).</td>
</tr>
<tr>
<td>Information Security Management System (ISMS)</td>
<td>A framework of policies and procedures that includes all legal, physical, and technical controls involved in an organization’s information risk management processes.</td>
</tr>
<tr>
<td>Infrastructure as a Service (IaaS)</td>
<td>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).</td>
</tr>
<tr>
<td>Inherited from Pre-existing Authorization</td>
<td>A control that is inherited from another CSP that has already received an Authorization</td>
</tr>
<tr>
<td>Interoperability</td>
<td>The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions.</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>A specification for an information security management system (ISMS)</td>
</tr>
<tr>
<td>Joint Authorization Board (JAB)</td>
<td>Consists of the DOD, GSA, and DHS CIOs</td>
</tr>
<tr>
<td>Joint Authorization</td>
<td>A FedRAMP Provisional Authority to Operate issued by the JAB</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>JAB</td>
<td>Board (JAB) Provisional Authority to Operate (P-ATO)</td>
</tr>
<tr>
<td>P-ATO</td>
<td>An open-standard file format that uses human-readable text to transmit data objects consisting of attribute-value pairs and array data types</td>
</tr>
<tr>
<td>MAC</td>
<td>A unique identifier assigned to a network interface controller that uniquely identifies each device on a network</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Provides a measuring capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts)</td>
</tr>
<tr>
<td>MAC</td>
<td>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.</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Discovering and monitoring the virtual resources, monitoring cloud operations and events, and generating performance reports</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Provides services related to the session layer of the OSI model, allowing applications on separate computers to communicate over a local area network. As strictly an API, NetBIOS is not a networking protocol.</td>
</tr>
<tr>
<td>NSO</td>
<td>One of six categories for FedRAMP Tailored LI-SaaS controls; NSO means FedRAMP has determined the control does not impact the security of the Cloud SaaS.</td>
</tr>
<tr>
<td>OTG-SESS-006</td>
<td>Testing for logout functionality (OWASP)</td>
</tr>
<tr>
<td>Performance Audit</td>
<td>Systematic evaluation of a cloud system by measuring how well it conforms to a set of established performance criteria</td>
</tr>
<tr>
<td>Physical Resource Layer</td>
<td>Includes all the physical resources used to provide cloud services, most notably the hardware and the facility</td>
</tr>
<tr>
<td>PaaS</td>
<td>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.</td>
</tr>
<tr>
<td>Portability</td>
<td>1. The ability to transfer data from one system to another without being required to recreate or re-enter data descriptions or to modify significantly the application being transported 2. The ability of a system or software to run on more than one type or size of computer under more than one operating system.</td>
</tr>
<tr>
<td>3. Of equipment, the quality of being able to function normally while being conveyed</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>Information privacy is the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) and personally identifiable information (PII) throughout its life cycle.</td>
</tr>
<tr>
<td><strong>Privacy-Impact Audit</strong></td>
<td>Systematic evaluation of a cloud system by measuring how well it conforms to a set of established privacy-impacts criteria</td>
</tr>
<tr>
<td><strong>Private Cloud</strong></td>
<td>A cloud deployment model (see SSP Table 8-2). The cloud services and infrastructure are dedicated to a specific organization/agency and to no other clients.</td>
</tr>
<tr>
<td><strong>Provided by Customer</strong></td>
<td>A control where the customer needs to provide additional hardware or software in order to meet the control requirement</td>
</tr>
<tr>
<td><strong>Provisioning/Configuration</strong></td>
<td>The process of preparing and equipping a cloud to allow it to provide services to its users</td>
</tr>
<tr>
<td><strong>Public Cloud</strong></td>
<td>A cloud deployment model (see SSP Table 8-2). The cloud services and infrastructure support multiple organizations and agency clients.</td>
</tr>
<tr>
<td><strong>Rapid Provisioning</strong></td>
<td>Automatically deploying cloud system based on the requested service/resources/capabilities</td>
</tr>
<tr>
<td><strong>Resource Abstraction and Control Layer</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Resource Change</strong></td>
<td>Adjusting configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud</td>
</tr>
<tr>
<td><strong>Software as a Service (SaaS)</strong></td>
<td>One of the three main categories of cloud computing, SaaS is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Refers to information security. &quot;Information security&quot; means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.</td>
</tr>
<tr>
<td><strong>Security Audit</strong></td>
<td>Systematic evaluation of a cloud system by measuring how well it conforms to a set of established security criteria</td>
</tr>
<tr>
<td><strong>Service Aggregation</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
| **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
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>arbitrage</td>
<td>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.</td>
</tr>
<tr>
<td>Service Consumption</td>
<td>A Cloud Broker in the act of using a Cloud Service</td>
</tr>
<tr>
<td>Service Deployment</td>
<td>All of the activities and organization needed to make a cloud service available</td>
</tr>
<tr>
<td>Service Intermediation</td>
<td>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.</td>
</tr>
<tr>
<td>Service Provider Corporate</td>
<td>A control that originates from the CSP’s corporate network</td>
</tr>
<tr>
<td>Service Provider Hybrid</td>
<td>A control that makes use of both corporate controls and additional controls to a particular system at the CSP</td>
</tr>
<tr>
<td>Service Provider System Specific</td>
<td>A control specific to a particular system when the control is not part of the service provider corporate controls</td>
</tr>
<tr>
<td>Shared</td>
<td>A control that is partially implemented by the CSP and partially by the customer</td>
</tr>
<tr>
<td>SOC 2</td>
<td>Developed by the American Institute of CPAs (AICPA), the SOC 2 framework includes five key sections, forming a set of criteria called the Trust Services Principles. These include:</td>
</tr>
<tr>
<td></td>
<td>1. The security of the service provider’s system</td>
</tr>
<tr>
<td></td>
<td>2. The processing integrity of this system</td>
</tr>
<tr>
<td></td>
<td>3. The availability of this system</td>
</tr>
<tr>
<td></td>
<td>4. The privacy of personal information that the service provider collects, retains, uses, discloses and disposes of for user entities</td>
</tr>
<tr>
<td></td>
<td>5. The confidentiality of the information that the service provider’s system processes or maintains for user entities</td>
</tr>
<tr>
<td>Stratum-1 Time Server</td>
<td>A Stratum-1 Network Time Protocol (NTP) server has a direct connection to a hardware (Stratum-0) clock and is a primary network time server. Lower stratum servers reference a server in the stratum above. Stratum indicates the distance of a time server from the source reference clock.</td>
</tr>
<tr>
<td>Support Team</td>
<td>The FedRAMP Support Team is the group of individuals that responds to <a href="mailto:info@fedramp.gov">info@fedramp.gov</a></td>
</tr>
<tr>
<td>Threat</td>
<td>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</td>
</tr>
<tr>
<td>Threat Actor</td>
<td>An entity that initiates the launch of a threat agent</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Threat Agent</td>
<td>An element that provides the delivery mechanism for a threat</td>
</tr>
<tr>
<td>Validation and</td>
<td>The PMBOK Guide, a standard adopted by IEEE, defines validation and verification as follows in its 4th edition:</td>
</tr>
</tbody>
</table>
| Verification          | "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 on the protection of the confidentiality, integrity, or availability of the system (application and associated data) |