FedRAMP

FedRAMP Master Acronym and Glossary

Version 1.6

07/23/2020

GSA

info@fedramp.gov

fedramp.gov

DOCUMENT REVISION HISTORY

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

TABLE OF CONTENTS

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.

Acronym	Definition
3PAO	Third Party Assessment Organization
A2LA	American Association of Laboratory Accreditation
AA	Annual Assessment

AAL	Authenticator Assurance Level
AC	Access Control (security control family)
ACL	Access Control List
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
API	Application Programming Interface
APL	Approved Products List (DoD)
ASHRAE	American Society of Heating, Refrigerating and Air-conditioning Engineers
AT	Awareness and Training (security control family)
ATO	Authority to Operate
AU	Audit and Accountability (security control family)
BCP	Business Continuity Plan
BCR	Baltimore Cyber Range
BIA	Business Impact Analysis / Business Impact Assessment
BOD	Binding Operational Directive (DHS)
BPA	Blanket Purchase Agreement
C&A	Certification and Accreditation
CA	Security Assessment and Authorization (security control family)
CAC	Common Access Card
CAP	Corrective Action Plan
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CCB	Change Control Board / Configuration Control Board
CDM	Continuous Diagnostics and Mitigation
CD-ROM	Compact Disc Read-Only Memory

CERT	Computer Emergency Readiness Team
CI	Configuration Item
CI/CD	Continuous Integration/Continuous Deployment
CIA	Confidentiality, Integrity, Availability
CIDR	Classless Inter-Domain Routing
CIM	Common Information Model
CIO	Chief Information Officer
CIOC	Chief Information Officer Council
CIRT	Computer Incident Response Team
CIS	Control Implementation Summary
CISO	Chief Information Security Officer
CLI	Command Line Interface
CM	Configuration Management (security control family)
CMMI	Capability Maturity Model Integration
CMP	Configuration Management Plan
CMVP	Cryptographic Module Validation Program
CO	Contracting Officer
CoLo	Co Location
ConMon	Continuous Monitoring
CONOPS	Concept of Operations
CONUS	Continental/Contiguous United States
COOP	Continuity of Operations Plan
COR	Contracting Officer’s Representative
COTS	Commercial Off-The-Shelf

CP	Contingency Planning (security control family)
CPC	Contingency Planning Coordinator
CPD	Contingency Planning Director
CR	Change Request
CRM	Customer Responsibility Matrix or Customer Relationship Management
CSA	Cloud Security Alliance
CSIRC	Computer Security Incident Response Center
CSO	Cloud Service Offering
CSP	Cloud Service Provider
CSV	Comma Separated Values
CTO	Chief Technology Officer
CTW	Control Tailoring Workbook
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
D&A	Document and Assess (LI-SaaS)
DAA	Designated Approving Authority
DAS	Direct Attached Storage
DDoS	Distributed Denial of Service
DFR	Detailed Finding Review
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone

DNS	Domain Name System / Domain Name Server
DNSSEC	Domain Name System Security Extensions
DoD	Department of Defense
DoH	DNS over HTTPS
DoS	Denial of Service
DoT	DNS over TLS
DR	Deviation Request
DS	Database Scan
EA	Enterprise Architecture (OMB)
E-Authentication	Electronic Authentication
E-Discovery	Electronic Discovery
EC-Council	International Council of Electronic Commerce Consultants
ECSB	Enterprise Cloud Service Broker
ESI	Electronically Stored Information
FAL	Federation Assurance Level
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FDCCI	Federal Data Center Consolidation Initiative
FDIC	Federal Deposit Insurance Corporation
FED	Federal Government
FedRAMP	Federal Risk and Authorization Management Program
FFRDC	Federally Funded Research and Development Center
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards

FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act (2002)
FISMA	Federal Information Security Modernization Act (2014)
FOC	Final Operating Capability
FOIA	Freedom of Information Act
FP	False Positive
FPS	Federal Protective Service
FRA	Federal Records Act
FTP	File Transfer Protocol
GFI	Government Furnished Information
GIAC	Global Information Assurance Certification
GMT	Greenwich Mean Time
GSA	General Services Administration
GSS	General Support System
GUI	Graphical User Interface
HF	High Frequency
HIDS	Host Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System
HRT	Hardware Recovery Team
HSM	Hardware Security Module
HSPD	Homeland Security Presidential Directive
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol

HW	Hardware
IA	Identification and Authentication (security control family)
IA	Independent Auditor / Assessor
IAA	Inter-Agency Agreement
IaaS	Infrastructure as a Service
IAL	Identity Assurance Level
IAO	Independent Assessment Organizations
IAP	Internet Access Points
IAW	In Accordance With
ID	Identification
IG	Inspector General
IOC	Initial Operating Capability
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPSec	Internet Protocol Security
IPT	Integrated Product Team
IR	Incident Response (security control family)
IRP	Incident Response Plan
IS	Information System
ISA	Interconnection Security Agreement
ISCP	Information System Contingency Plan
iSCSI	Internet Small Computer System Interface
ISConMon	Information Security Continuous Monitoring

ISIMC	Information Security and Identity Management Committee
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISP	Internet Service Provider
ISPP	Information Security Policies and Procedures
ISSO	Information System Security Officer
IT	Information Technology
ITCP	IT Contingency Plan
IV&V	Independent Verification and Validation
IXP	Internet Exchange Point
JAB	Joint Authorization Board (FedRAMP)
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LI-SaaS	Low Impact Software as a Service
LMS	Learning Management System
MA	Maintenance (security control family)
MAC	Media Access Control
MAX	MAX.gov (Secure Repository)
MFA	Multi-Factor Authentication
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection (security control family)
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
NDA	Non-Disclosure Agreement
NetBIOS	Network Basic Input/Output System
NFPA	National Fire Protection Association
NGO	Non-Governmental Organization
NIAP	National Information Assurance Partnership
NIS	Network Information System
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
NNTP	Network News Transfer Protocol
NOC	Network Operations Center
NPPD	National Protection and Programs Directorate (DHS)
NSA	National Security Agency
NTP	Network Time Protocol
NTTAA	National Technology Transfer and Advancement Act
NVD	National Vulnerability Database
NVI	NAT Virtual Interface
ODAL	Outage and Damage Assessment Lead
OEP	Occupant Emergency Plan

OGC	Office of the General Counsel
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OR	Operational Requirement
OS	Operating System
OSINT	Open Source Intelligence
OSCAL	Open Security Controls Assessment Language
OSCP	Online Certificate Status Protocol
OWASP	Open Web Application Security Project
P&P	Policies and Procedures
PA	Provisional Authorization
PaaS	Platform as a Service
P-ATO	Provisional Authority to Operate
PCI	Payment Card Industry (Data Security Standard)
PDF	Portable Document Format
PDS	Protective Distribution System
PE	Physical and Environmental Protection (security control family)
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning (security control family)
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
POSIX	Portable Operating System Interface
PS	Personnel Security (security control family)
PTA	Privacy Threshold Analysis
PTR	Penetration Test Report
PUB	Publication
QA	Quality Assurance
QC	Quality Control
QM	Quality Management
RA	Risk Assessment (security control family)
RA	Risk Adjustment
RAR	Readiness Assessment Report
RBAC	Role-Based Access Control
RFC	Request for Change
RFI	Request for Information
RFP	Request for Proposal
RFQ	Request for Quotation
RIP	Routing Information Protocol
RMF	Risk Management Framework
ROB	Rules of Behavior

ROE	Rules of Engagement
ROI	Return On Investment
RP	Relying Party
RTO	Recovery Time Objective
SA	System and Services Acquisition (security control family)
SaaS	Software as a Service
SAF	Security Assessment Framework
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SAP	Security Assessment Plan
SAR	Security Assessment Report
SAS	Security Assessment Support
SC	System and Communications Protection (security control family)
SC	Security Coordinator
SCAP	Security Content Automation Protocol
SCR	Significant Change Request
SCSI	Small Computer System Interface
SD	Secure Digital
SDLC	System Development Life Cycle
SI	System and Information Integrity (security control family)
SIA	Security Impact Analysis
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SME	Subject Matter Expert

SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SO	System Owner
SOC	Security Operations Center
SOC	System and Organization Controls (AICPA)
SOP	Standard Operating Procedure
SORN	System of Records Notice
SP	Service Processor
SQL	Structured Query Language
SRT	Software Recovery Team
SSL	Secure Sockets Layer
SSO	Single Sign-On
SSP	System Security Plan
SDO	Standards Developing Organization
SW	Software
TAA	Trade Agreements Act
TCP	Transmission Control Protocol
TFTP	Trivial FTP
TIC	Trusted Internet Connection
TICAP	Trusted Internet Connection Access Providers
TLD	Top Level Domain
TLS	Transport Layer Security
TOS	Terms of Service
TP	Test Plan

TR	Technical Representative / Reviewer
TT	Telecommunications Team
TTS	Technology Transformation Services
UHF	Ultra-High Frequency
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
US	United States
USGCB	United States Government Configuration Baseline
URL	Uniform Resource Locator
USB	Universal Serial Bus
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
UTC	Universal Time Coordinated
UUCP	Unix-to-Unix Copy Protocol
VD	Vendor Dependency
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
XML	Extensible Markup Language

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.

Term	Meaning
Agency Authority to Operate	An authorization that is issued by a federal department, office, or agency
Cloud Access	To make contact with or gain access to a cloud service
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, and/or 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 Service 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 Service Providers and Cloud Consumers
Cloud Provider	A person, organization or entity responsible for making a service available to service consumers
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 where the customer needs to apply a configuration in order to meet the control requirement

Container	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.
CSA STAR Certification	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.
Data Portability	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.
Digital Authentication	The process of establishing confidence in user identities presented digitally to a system, which was previously referred to as Electronic Authentication (E-Authentication)
FedRAMP Accelerated	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* .
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 System Security Plan (SSP) and its attachments, a Security Assessment Report (SAR), a Plan of Action and Milestones (POA&M) and a Continuous Monitoring Plan.
FedRAMP Connect	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
FedRAMP In-Process	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
FedRAMP P-ATO	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.
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 (RAR) which must be reviewed and approved by the FedRAMP PMO.
FedRAMP Tailored	For Low Impact Software as a Service (LI-SaaS); see https://tailored.fedramp.gov/policy/

Federal Information Processing Standards (FIPS)	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: http://www.nist.gov/itl/fips.cfm.
Fixed Endpoints	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.
Government Only Cloud	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.
Hybrid Cloud	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).
Information Security Management System (ISMS)	A framework of policies and procedures that includes all legal, physical, and technical controls involved in an organization's information risk management processes
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 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
ISO 27001	A specification for an information security management system (ISMS)
Joint Authorization Board (JAB)	Consists of the DOD, GSA, and DHS CIOs
Joint Authorization	A FedRAMP Provisional Authority to Operate issued by the JAB

Board (JAB) Provisional Authority to Operate (P-ATO)	
JavaScript Object Notation	An open-standard file format that uses human-readable text to transmit data objects consisting of attribute-value pairs and array data types
Media Access Control (MAC) Address	A unique identifier assigned to a network interface controller that uniquely identifies each device on a network
Metering	Provides 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	Discovering and monitoring the virtual resources, monitoring cloud operations and events, and generating performance reports
Network Basic Input/Output System (NetBIOS)	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.
NSO	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.
OTG-SESS-006	Testing for logout functionality (OWASP)
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 (PaaS)	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 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.

	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	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.
Provided by Customer	A control where the customer needs to provide additional hardware or software in order to meet the control requirement
Provisioning/ Configuration	The process of preparing and equipping a cloud to allow it to provide services to its users
Public Cloud	A cloud deployment model (see SSP Table 8-2). The cloud services and infrastructure support multiple organizations and agency clients.
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	Adjusting configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud
Software as a Service (SaaS)	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.
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's corporate network
Service Provider Hybrid	A control that makes use of both corporate controls and additional controls to a particular system at the CSP
Service Provider System Specific	A control specific to a particular system when the control is not part of the service provider corporate controls
Shared	A control that is partially implemented by the CSP and partially by the customer
SOC 2	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: 1. The security of the service provider's system 2. The processing integrity of this system 3. The availability of this system 4. The privacy of personal information that the service provider collects, retains, uses, discloses and disposes of for user entities 5. The confidentiality of the information that the service provider's system processes or maintains for user entities
Stratum-1 Time Server	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.
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

Threat Agent	An element that provides the delivery mechanism for a threat
Validation and Verification	The PMBOK Guide, a standard adopted by IEEE, defines validation and verification as follows in its 4th edition: "*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)