Commerical Cloud Service Providers and FedRAMP

(a white paper on the critical imperatives for commercial providers meeting the stringent security compliance requirements of Federal IT)

Author: Eric Nickel, Chief Systems Architect – March - 2019

How the Cloud Service Provider meets FedRAMP HIGH baseline security compliance

Not all Cloud Service Providers (CSPs) are created equal. And with that, not all CSP's will deliver a cloud service offering inside of a rigorous cybersecurity and compliance framework. Amazon Web Services (AWS) and Microsoft Azure are the leading providers of secure public cloud services. But what about other private cloud service offerings: how is the U.S. Government authorized to use the cloud service models? For those offering Software as a Service (SaaS), Infrastructure as a Service (IaaS), and/or Platform as a Service (PaaS), the CSP's must first meet the rigorous cybersecurity controls inside of the ***Federal Risk Authorization Management Program (FedRAMP)***.

Under FedRAMP, only approved cloud services are authorized to use by the U.S. Government

In 2011, a memo was released by the Executive Office of the President aimed at protecting US Citizen data in the cloud. The memo titled *"Memorandum for Chief Information Officers"* is issued from the Office of Management and Budget (OMB) and defines department and agency responsibility in establishing FedRAMP.

FedRAMP established the set of cloud computing standards used by all Federal Departments and Agencies as requirements in meeting the Federal Information System Management Act (FISMA), as it relates to cloud services. The goal of the program is to create efficiencies from the use of cloud services and to strengthen the cybersecurity posture of those cloud services to help protect U.S. Citizen data in the cloud.

Prior to the establishment of FedRAMP, the use of cloud services by Departments and Agencies led to a different set of security requirements for each cloud offering. To help reduce those inconsistencies, in 2015, FedRAMP launched a new security assessment framework using the National Institute of Standards and Technology-Risk Management Framework (NIST RMF). Now under the new FedRAMP- CSP's are readily available to benefit from the public partnership. Once authorized they are now found in the products listings on FedRAMP marketplace and system security documents are found on OMB Max.gov.

The Federal Risk Authorization Program

Is the standardized process for security assessment, authorization, and continuous monitoring for cloud products and services used by government agencies.

Security Assessment Framework consists of;

- Joint Authorization Board (JAB);
- Standard contract language, and;
- Repository of authorization packages.

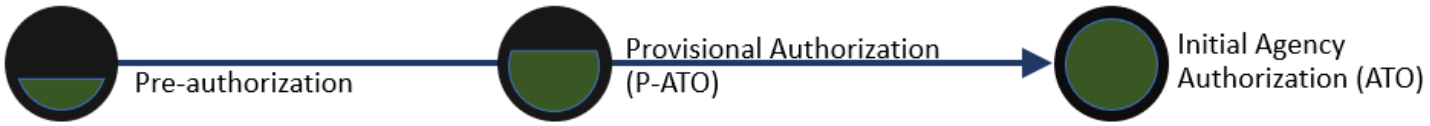
FedRAMP's four steps help align with the NIST Risk Management Framework (RMF) covered in NIST SP 800-37: **Document**; **Assess**; **Authorize** and **Monitor**.

Four key stakeholders in FedRAMP are the:

- Department of Homeland Security (DHS);
- JAB (Members from DoD, DHS and GSA);
- Program Management Office (PMO), and;
- Executive departments and agencies.

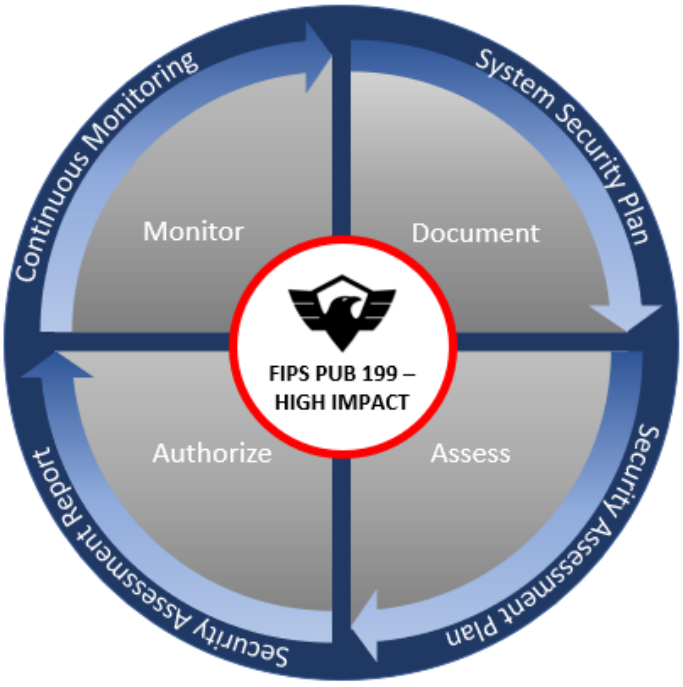
Four primary documents in the Security Authorization Package are the:

- System Security Plan (SSP) details the CSP's system security environment.
- System Assessment Plan (SAP) details the vulnerability testing.
- System Assessment Report (SAR) details the independent assessor's findings and recommendations
- Plan of Actions and Milestones (POA&M) provides details on the approach to addressing security vulnerabilities.



Security Assessment Framework

FedRAMP is now THE only Government-wide organizational risk management program for public cloud service offerings. The framework now used for risk authorization consists of four steps in a continuous lifecycle security assessment similar to the NIST (SP) 800-37, "Risk Management Framework (RMF) for Information Systems and Organizations". The four steps now used to authorize a cloud service provider's offering are **Document, Assess, Authorize and Monitor.**



Proper selection of the impact level for the cloud service offering is critical to identify the appropriate security controls. To do so, the CSP will first measure the overall impact potential by determining the highest potential impact value in **LOW, MODERATE, or HIGH.** The three security objective values for- Confidentiality, Integrity and Availability can be found in Table 1 of FIPS 199 *"Standards for Security Categorization of Federal Information and Information Systems" which defines potential impact for each.*

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

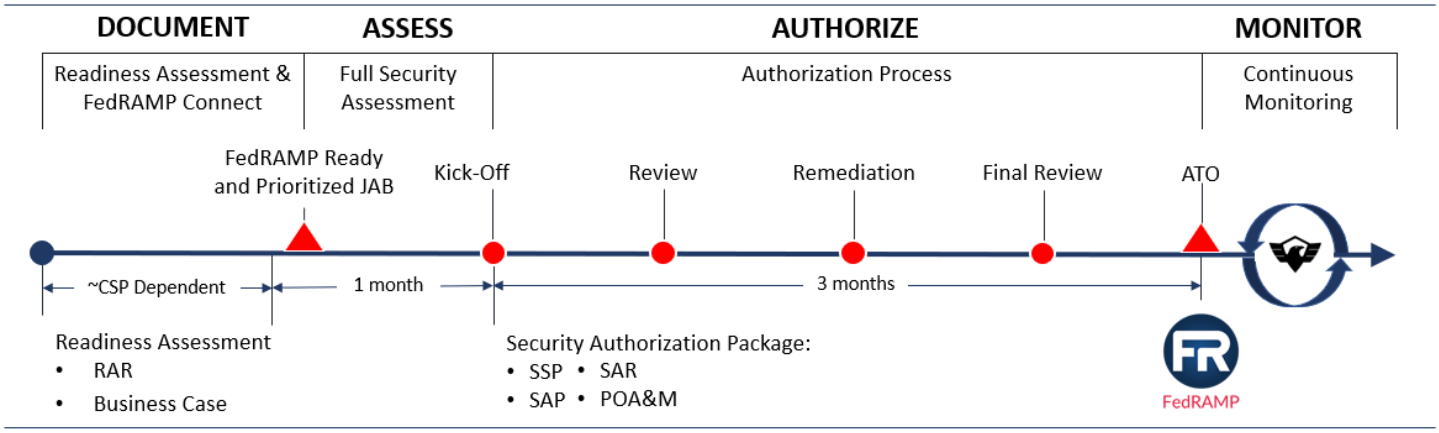
TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

CyberSecure IPS is THE preferred security provider to monitor service offerings with FedRAMP HIGH security objectives- the Infrastructure Monitoring System (IMS) is proven effective in meeting those objectives to the U.S. Government. In fact the IMS is the only security provider used with alarmed carrier protected distribution system (PDS) technology to deliver Committee on National Security Systems CNSS Instruction 7003 standard operating procedures compliance to the U.S. Government and now proven to monitor compliance in the new Security Assessment Framework (SAF) for cloud services created by FedRAMP.

IMS tailors to protecting compliant cloud service provider offerings with HIGH security objectives. IMS is used by the CISO to enhance security controls to high impact levels in four control families found inside of the security assessment framework:

- System and Communication Protection (SC)
- System and Information Integrity (SI)
- Physical and Environmental Protection (PE)
- Maintenance (MA)

Note: *See the FedRAMP High security controls baseline to find details for each security control enhancement provided by IMS.*



Authorization Process

The authorization process is a collective effort between the Agency, Independent Third-Party Assessment Organization (3PAO) and the CSP. The CSP's role during the authorize process is to ensure their cloud service offering meets the required FedRAMP security controls in the minimum security control baseline. Security Authorization Packages require CSP's to submit four primary key artifacts to document, assess, authorize and monitor a service offering:

- System Security Plan (SSP)
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Plan of Action & Milestones (POA&M)

The **System Security Plan** is both the security overview and a detailed description of the security requirements for the cloud service that must be in place for implementation.

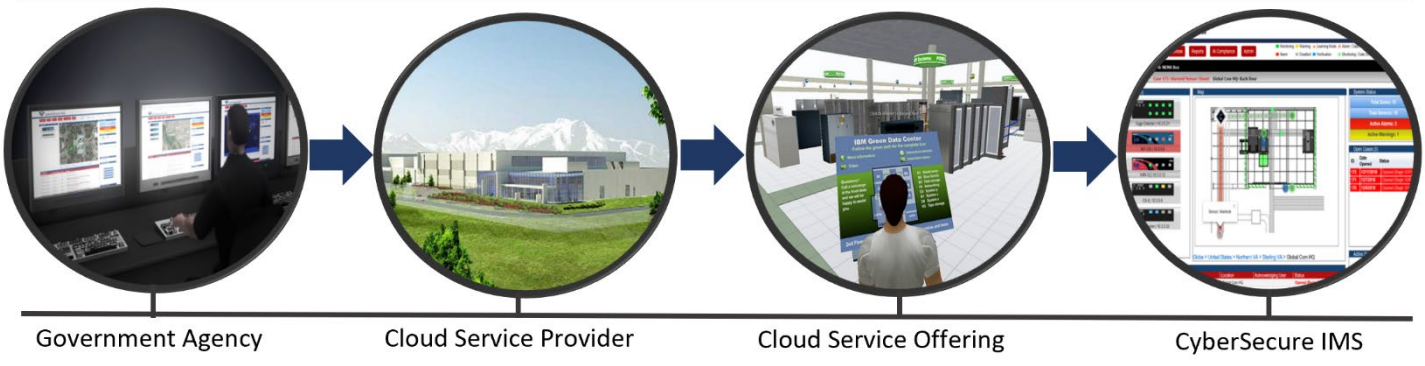
The **Security Assessment Plan** is both the documented test and remediation procedures that the CSP and 3PAO must follow to satisfy the requirements in the SSP.

The **Security Assessment Report** documents the 3PAO's findings during the actual security assessment and communicates any inherent risk to the Authorizing Agency.

The **Plan of Action & Milestones** provides the structured framework for aggregating system vulnerabilities and deficiencies through the security assessment lifecycle of the cloud service offering.

After completion and final review of the primary documents and when all security objectives are satisfied in the POA&M, the security authorization package is submitted to the Authorizing Official (AO) for review. If the risk is acceptable to the Agency, the AO will issue an Authority to Operate (ATO) and the cloud service provider will be monitored inside of the security assessment framework for cloud services.

An Authorization letter from the AO is then issued to the FedRAMP Program Management Office (PMO) and the CSP is now available on the FedRAMP Marketplace with the approved cloud service offering. The security authorization package is also readily available for further collaboration and partnerships on the knowledge management platform found on Max.gov.



Continuous Monitoring

The ability to continuously monitor to assure confidentiality, integrity and availability of the information transport systems is a critical component to a successful public cloud service offering. To maintain the security authorization package and FedRAMP compliance CSPs will need to continuously monitor the cloud services and update the four primary artifacts developed during the security assessment over the lifecycle of the cloud service offering. The updated security authorization package is provided to the Agencies Authorizing Official for further review and approval on a monthly basis and annual security control testing will be performed by the 3PAO after the initial authorization is granted.

FedRAMP Summary

For the U.S. Government the FedRAMP program is the established set of cloud computing standards used by all Federal Departments and Agencies to meet the requirements of the Federal Information Systems Management Act (FISMA). The FedRAMP Security Assessment Framework (SAF) is the Government-wide organizational risk management framework (RMF) used to monitor continuous compliance of public cloud service offerings. Cloud Service Providers (CSPs) must meet all of the security controls in the FedRAMP minimum security control baseline as the catalog of minimum required security controls that are required for a public cloud service offering along with the additional guidance provided for security control enhancements that must be used with the application of Moderate and High Impact security objectives in the cloud processing environment.

The Infrastructure Monitoring System is used by the leading cloud service providers to meet the demand for high security control baselines on their public cloud service offerings. IMS has already proven to be effective in providing the physical safeguards that prevent unauthorized information disclosure in High threat level environments for the U.S. Government. Today the IMS is deployed globally as the only security solution used to monitor the protected distribution systems by the U.S. Government and it now provides CSPs with FedRAMP compliant security control enhancements used to automate detection, route alarms and provide case management on any unauthorized attempt to exfiltrate data from a protected cloud service offering. The IMS even ensures that the cloud service offering is properly secured during installs and maintenance periods and operates using the same standard operating procedures used by the security personnel in U.S. Government Department and Agencies protecting the confidentiality and the integrity over the transmission mediums used to actively transport National Security Information (NSI) without encryption. IMS also meets security guidance mandated by the Committee on National Security Systems CNSS Instruction 7003 (CNSSI 7003) used to protect controlled unclassified and classified information system network boundaries through controlled access areas (CAAs) and Uncontrolled Access Areas (UAAs).

For the cloud service provider offering that must meet the FedRAMP High impact security control baseline- the Infrastructure Monitoring System will enhance your ability to continuously monitor FedRAMP compliance within the new security assessment framework without the additional complexity or burden on your security personnel. The IMS monitors and protects your cloud service offerings with the granular level of visibility, protection and control needed to enhance those security objectives within a single dashboard. The table below is a summary of the FedRAMP High Baseline security control enhancements provided by the IMS to use as guidance in tailoring your cloud service offerings security objectives to FedRAMP High impact.

Security Control Baseilne

The FedRAMP Security Controls Baseline provides a catalog of FedRAMP High, Moderate, Low baseline security controls, along with additional guidance and security enhancements for Low, Moderate and High Impact. The IMS FedRAMP High Baseline Template below provides a summary of controls inherited by the IMS. This template can be used as supplemental guidance to begin your tailoring process for the IMS when it is applied to your cloud service offering.

IMS FedRAMP High Baseline Summary

SYSTEM AND COMMUNICATIONS PROTECTION (SC) CONTROL FAMILY		LOW	MOD	HIGH
SC-7 (10)	Boundary Protection | Prevent Unauthorized Exfiltration	☐	☐	☒
SC-8 (1)	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	☐	☒	☒
SYSTEM AND INFORMATION INTEGRITY (SI) CONTROL FAMILY		**LOW**	**MOD**	**HIGH**
SI-4 (1)	Information System Monitoring | System Wide Intrusion Detection System	☐	☒	☒
SI-4 (2)	Information System Monitoring | Automated Tools for real-time analysis	☐	☐	☒
SI-4 (5)	Information System Monitoring | System Generated Alerts	☐	☒	☒
SI-4 (16)	Information System Monitoring | Correlate Monitoring Information	☐	☐	☒
SI-4 (18)	Information System Monitoring | Analyze Traffic / Covert Exfiltration	☐	☐	☒
SI-4 (24)	Information System Monitoring | Indicators of Compromise	☐	☐	☒
SI-7 (5)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations	☐	☐	☒
MAINTENANCE (MA) CONTROL FAMILY		**LOW**	**MOD**	**HIGH**
MA-2	Controlled Maintenance	☒	☒	☒
MA-2 (2)	Controlled Maintenance | Automated Maintenance Activities	☐	☐	☒
MA-3	Maintenance Tools	☐	☒	☒
PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) CONTROL FAMILY		**LOW**	**MOD**	**HIGH**
PE-3 (1)	Physical Access Control | Information System Access	☐	☐	☒
PE-4	Access Control for Transmission Medium **(CNSSI 7003)**	☐	☒	☒
PE-6 (1)	Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment	☐	☒	☒
PE-6 (4)	Monitoring Physical Access | Monitoring Physical Access to Information Systems	☐	☐	☒
PE-8 (1)	Visitor Access Records | Automated Records Maintenance Review	☐	☐	☒
PE-14 (2)	Temperature and Humidity Controls | Monitoring with Alarms / Notifications	☐	☒	☒

IMS FedRAMP High Baseline Details

System and Communications Protection (SC) Control Family

SC-7 Boundary protection

The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are physically separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

SC-8 (1) Transmission confidentiality and integrity | cryptographic or alternate physical protection

The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information; detect changes to information during transmission unless otherwise protected by alternative physical safeguards.

System and Information Integrity Control Family

SI-4 (1) information system monitoring | system-wide intrusion detection system

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

SI-4 (2) Information system monitoring | automated tools for real-time analysis

The organization employs automated tools to support near real-time analysis of events.

SI-4 (16) Information system monitoring | correlate monitoring information

The organization correlates information from monitoring tools employed throughout the information system.

SI-4 (18) Information system monitoring | analyze traffic/covert exfiltration

The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at interior points within the system (e.g., subsystems, subnetworks) to detect covert exfiltration of information.

SI-4 (24) Information system monitoring | indicators of compromise

The information system discovers, collects, distributes, and uses indicators of compromise.

SI-4 (5) Information system monitoring | system-generated alerts

The information system alerts when indications of compromise or potential compromise occur.

SI-7 (5) Software, firmware, and information integrity | automated response to integrity violations

The information system automatically shuts the information system down; restarts the information system; implements security safeguards when integrity violations are discovered.

Physical and Environmental Protection (PE) Control Family

PE-3 (1) physical access control | information system access

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at physical spaces containing one or more components of the information system.

PE-4 Access control for transmission medium

The organization controls physical access to information system distribution and transmission lines within organizational facilities using security safeguards. Supplemental Guidance: Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

References: NSTISSI No. 7003.

PE-6 (1) Monitoring physical access | intrusion alarms / surveillance equipment

The organization monitors physical intrusion alarms and surveillance equipment

PE 6(4) Monitoring physical access | monitoring physical access to information systems

The organization monitors physical access to the information system in addition to the physical access monitoring of the facility. Supplemental Guidance: This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers).

PE-14 (2) temperature and humidity controls | monitoring with alarms / notifications

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Maintenance (MA) Control Family

MA-2 (2) Controlled maintenance | automated maintenance activities

The organization: (a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and (b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

MA-3 (3) Maintenance tools | prevent unauthorized removal

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from explicitly authorizing removal of the equipment from the facility.

Glossary of Acronyms

3PAO	Third Party Assessment Organization
AO	Authorizing Official
ATO	Authority to Operate
CNSS	Committee on National Security Systems
CSP	Cloud Service Provider
DHS	Department of Homeland Security
DoD	Department of Defense
EoP	Executive Office of the President
FedRAMP	Federal Risk Authorization Management Program
FISMA	Federal Information Systems Management Act
FIPS	Federal Information Processing Standards
GSA	General Services Administration
IaaS	Infrastructure as a Service
IMS	Infrastructure Monitoring System
JAB	Joint Authorization Board
MA	Maintenance
MP	Media Protection
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PaaS	Platform as a Service
PE	Physical and Environmental Protection
POA&M	Plan of Action and Milestones
PMO	Program Management Office
RMF	Risk Management Framework
SaaS	Software as a Service
SAF	Security Assessment Framework
SAR	Security Assessment Report
SAP	Security Assessment Plan
SC	System and Communications Protection
SI	System and Information Integrity
SSP	System Security Plan

Standards and Guidance Reference

CNSSI 7003	Protected Distribution Systems
FIPS PUB 199	Standards for Security Categorization of Federal Information and Information Systems
NIST SP 800-145	The NIST Definition of Cloud Computing
NIST SP 800-61, Rev 2	Computer Security Incident Handling Guide
NIST SP 800-34, Rev 1	Contingency Planning Guide for Federal Information Systems
NIST SP 800-27, Rev A	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
NIST SP 800-53A, Rev 4	Guide for Assessing the Security Controls in Federal Information Systems
NIST SP 800-18	Guide for Developing Security Plans for Federal Information Systems
NIST SP 800-37, Rev 1	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
NIST SP 800-60, Rev 1	Guide for Mapping Types of Information and Information Systems to Security Categories