March 2020

Google Cloud FedRAMP Implementation Guide

Establishing FedRAMP compliant policies and controls on GCP

Table of Contents

Disclaimer

This guide is for informational purposes only. Google does not intend the information or recommendations in this guide to constitute legal advice. Each customer is responsible for independently evaluating its own particular use of the services as appropriate to support its legal compliance obligations.

Intended Audience

For customers who are subject to the requirements of the Federal Risk and Authorization Management Program (FedRAMP), Google Cloud Platform supports FedRAMP compliance. This guide is intended for security officers, compliance officers, IT administrators, and other employees who are responsible for FedRAMP implementation and compliance on Google Cloud Platform. This guide should aid with understanding how Google is able to support FedRAMP compliance as well as understanding which Google Cloud tools, products, and services to configure to help meet your responsibilities under FedRAMP.

Overview

Google Cloud Platform supports FedRAMP compliance, and provides specific details on the approach to security and data protection in the Google Security Whitepaper and in the Google Infrastructure Security Design Overview. While Google provides a secure and compliant cloud infrastructure, customers are ultimately responsible for evaluating their own FedRAMP compliance, and for ensuring that the environment and applications that they build on top of Google Cloud Platform are properly configured and secured according to FedRAMP requirements.

This document will outline the FedRAMP Authority to Operate (ATO) phases at a high level, explain the Google Cloud shared responsibility model, highlight customer-specific responsibilities and suggest how to meet these requirements and guidelines on Google Cloud Platform.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that standardizes how the Federal Information System Act (FISMA) applies to cloud computing. It establishes a repeatable approach to security assessment, authorization, and continuous monitoring for cloud-based services.

Using FedRAMP's standards and guidelines, sensitive, mission essential, and mission critical data can be secured in the cloud, making it possible to detect cybersecurity vulnerabilities quickly.

At a high level, the goals of FedRAMP are to:

1. Ensure that cloud services and systems used by government agencies have adequate safeguards
2. De-duplicate efforts and reduce risk management costs
3. Enable government agencies to rapidly and cost effectively procure information systems and services

In adherence to FedRAMP, federal government agencies must:

1. Ensure that all cloud systems which process, transmit, and store government data use the FedRAMP security controls baseline(s)
2. Use the security assessment framework when granting security authorizations under FISMA
3. Enforce FedRAMP requirements through contracts with Cloud Service Providers (CSPs)

Authority to Operate (ATO)

Successful implementation and execution of the FedRAMP accreditation process culminates with an Authority to Operate (ATO) in the cloud. There are two paths for FedRAMP ATO: P-ATO and Agency ATO.

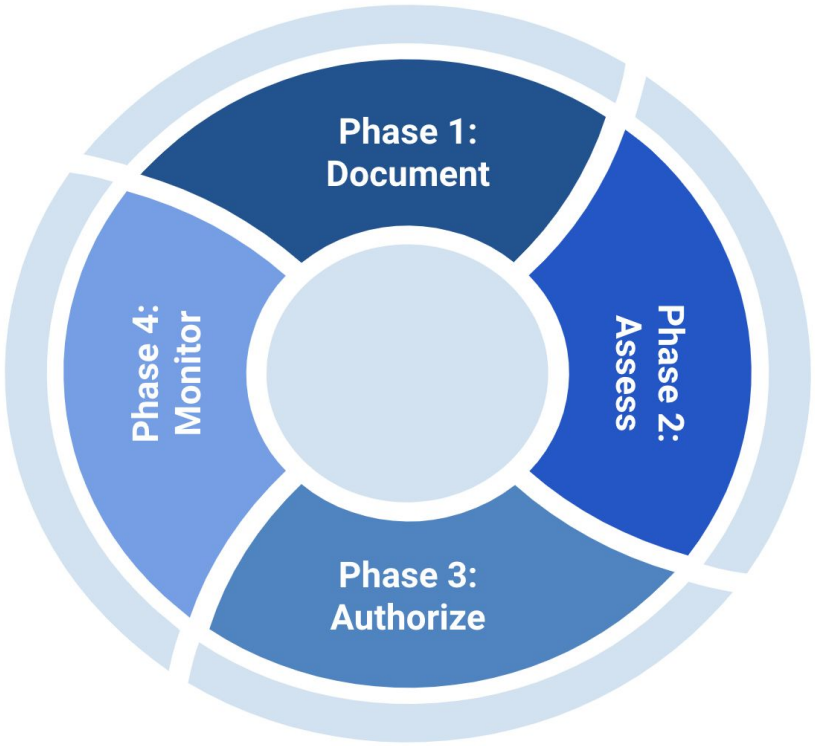
P-ATO, or Provisional Authority to Operate, is granted by the FedRAMP Joint Authorization Board (JAB). The JAB is composed of CIOs from DHS, GSA, and DoD; they define the baseline FedRAMP security controls and establish the FedRAMP accreditation criteria for 3rd party assessment organizations (3PAOs). Organizations and agencies request to have their information system security package processed by the JAB, and the JAB subsequently issues P-ATO to use cloud services.

With Agency ATO, the internal organization or agency designates authorizing officials (AOs) to conduct a risk review of the information system security package. The AO can engage 3PAOs or non-accredited, independent assessors (IAs) to review the information system security package. The AO, and subsequently the agency or organization, then authorizes the information system's use of cloud services. The security package is additionally sent to the FedRAMP

Program Management Office (PMO) for review; GSA is the PMO for FedRAMP. After review, the PMO published the security package for other agencies and organizations to use.

Security Assessment Framework

Authorizing Officials (AOs) at agencies and organizations must incorporate the FedRAMP security assessment framework (SAF) into their internal authorization processes to ensure that they meet FedRAMP requirements for cloud services use. The SAF is implemented in four phases:



Phase 1: Document	The organization or agency categorizes their information system as a Low, Moderate, or High impact system according to FIPS PUB 199 security objectives for confidentiality, integrity, and availability. Based on the system's FIPS categorization, the organization or agency should select the FedRAMP security controls baseline that correlates with the FIPS 199 categorization level of low, moderate, or high. Information systems owners must then implement the security controls captured in the respective controls baseline. Alternative implementations and justification for why a control can't be met or implemented is also acceptable. Details of the security controls implementation must be captured in a System

	Security Plan (SSP). System owners should select the SSP template according to the pursued FedRAMP compliance level - Low, Moderate, or High. The SSP describes the security authorization boundary, explains how the system implementation will address each FedRAMP security control, outlines system roles and responsibilities, defines expected system user behavior, exhibits how the system is architected and what the supporting infrastructure looks like. Use the FedRAMP authorization review template to track your ATO progress.

Phase 2: Assess	Once the Security Assessment Framework is complete, an independent assessor needs to test the information system to confirm that the security controls are implemented. The organization or agency can seek an accredited 3rd party assessment organization (3PAO) or a non-accredited independent assessor (IA) if the organization is pursuing an Agency ATO. The 3PAO or IA will create a security test plan based on the Security Assessment Plan (SAP) template. They'll use the FedRAMP baseline security test cases to assess the cloud system according to the proposed FedRAMP authorization level (Low, Moderate, High test cases). After completing the SAR, the 3PAO or IA will produce a Security Assessment Report (SAR). The SAR should include vulnerabilities, threats, and risks found during testing. System owners will have the opportunity to remediate risks identified in the SAR; the SAR should also provide guidance on how to mitigate the risks that were found. A Plan of Action and Milestones (POA&Ms) should be created to address vulnerabilities in the SAR: POA&M Template & Guide.

Phase 3: Authorize	The agency AO(s) will make a system authorization decision based on the SAP and SAR. The AO(s) will review the SAR to determine the overall risk posture of the information system. The final security authorization package, including the SSP, SAP, SAR, and any attachments, should be submitted to the AO. AOs make a risk assessment and formalize the decision in an ATO letter to the system owner and the FedRAMP PMO.

Phase 4: Monitor	Once P-ATO or Agency ATO is achieved, an ongoing authorization and assessment (A&A) process should follow; this is referred to as Continuous

	Monitoring. The system owners must continuously monitor the information system's security posture. For JAB P-ATO, a yearly security assessment and monthly continuous monitoring reports must be sent to the PMO. For Agency ATO, a yearly security assessment should occur and the organization or agency must update the FedRAMP authorization annually.

Review FedRAMP's agency authorization process for more details about the implementation phases.

Cloud Responsibility Model

Traditional infrastructure technology (IT) required organizations and agencies to purchase, physical data center or colocation space, physical servers, networking equipment, software, licenses, and other pieces of devices for building systems and services. With cloud computing, a cloud service provider invests in the physical hardware, datacenter, and global networking, while also providing virtual equipment, tools, and services for customers to use.

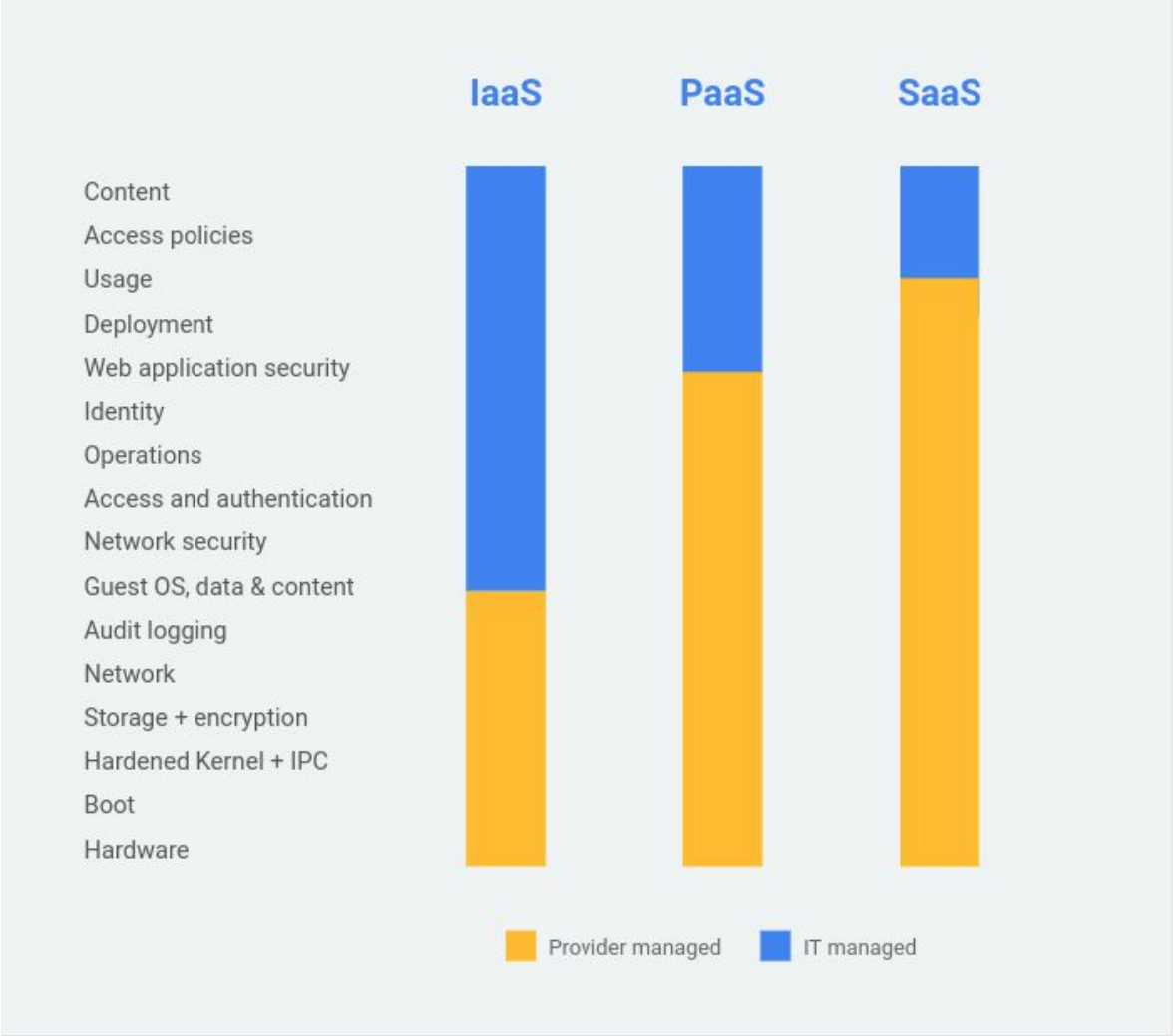
Three cloud computing models exist: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

In the IaaS model, CSPs essentially supply a virtual data center in the cloud; they deliver virtualized computing infrastructure such as servers, networks, and storage. While CSPs manage the physical equipment and data centers for these resources, customers are responsible for configuring and securing any of the platform or application resources they run on top of the virtualized infrastructure.

In the PaaS model, CSPs not only provide and manage the infrastructure and virtualization layer, they also provide customers with a pre-developed, pre-configured platform for creating software, applications, and web services. PaaS makes it easy for developers to create applications and middleware without worrying about security and configuration of the underlying hardware.

In the SaaS model, CSPs manage all of the physical and virtual infrastructure and the platform layer while delivering cloud-based applications and services for customers to consume. Internet applications that run directly from the web browser or by going to a website are SaaS applications. With this model, organizations and agencies don't have to worry about installing, updating, or supporting applications, they simply manage system and data access policies.

The figure below highlights CSP responsibility and customer responsibility on-prem and across the cloud computing models:



FedRAMP Responsibility

The cloud IT stack can be viewed relative to four layers - the physical infrastructure layer, the cloud infrastructure layer, the cloud platform layer, and the cloud software layer.

With respect to FedRAMP ATO, each layer of the cloud IT stack is considered an independent control boundary, and each control boundary requires a separate ATO. This means that despite Google Cloud Platform's FedRAMP compliance and having dozens of Google Cloud services that are covered by FedRAMP, customers are still required to implement FedRAMP security baseline controls and the SAF process to qualify their cloud systems and workloads as FedRAMP compliant.

There are two types of FedRAMP security controls across Low, Moderate, and High compliance baselines - controls implemented by **the information system**, and controls implemented by **the organization**. As organizations and agencies build out FedRAMP compliant systems on Google Cloud, they will inherit the physical infrastructure security controls that Google meets under its FedRAMP certification. They will additionally inherit any Physical Infrastructure, IaaS and PaaS security controls that are baked into Google's FedRAMP compliant products and services, and all SaaS controls when using G Suite. However, customers are required to implement all other security controls and configurations at the IaaS, PaaS, and SaaS levels, as defined by the FedRAMP security controls baseline.

To leverage the security controls that Google Cloud provides, request a copy of Google's ATO package from the JAB and include the package with your organization or agency's security assessment paperwork. Additionally, include a copy of Google's attestation letter of FedRAMP compliance.

FedRAMP Implementation Recommendations

As mentioned, customers inherit some security controls from the cloud services provider, while others must be specifically configured by the customer. Many of the security controls that have to be configured by the customer, require agencies and organizations to create ***organization-defined*** policies, rules, and regulations to meet the control. This section suggests recommendations to aid customers in implementing NIST 800-53 security controls in the cloud using org-defined policies coupled with GCP tools, services, and best practices.

Note: Services listed in this section marked with * are not currently covered by FedRAMP, and services marked with + are not native Google Cloud services.

Access Control

To manage access control in Google Cloud, define organization administrators that will manage information system accounts in the cloud. Place those administrators in access control groups using Cloud Identity, Admin Console, or some other identity provider (e.g. Active Directory, LDAP, etc.), ensuring that 3rd party identity providers are federated with Google Cloud. Use Cloud Identity and Access Management (IAM) to assign roles and permissions to administrative groups, implementing least privilege and separation of duties.

Develop an org-wide access control policy for information system accounts in the cloud. Define the parameters and procedures by which your organization will create, enable, modify, disable, and remove information system accounts.

Account Management, Separation of Duties, Least Privilege

In the access control policy, define the parameters and procedures by which your organization will create, enable, modify, disable, and remove information system accounts. Define the conditions under which information system accounts should be used.

Also, identify the time period of inactivity in which users will be required to log out of a system (e.g. after x-minutes, hours, days). Use Cloud Identity, Admin Console, or application configurations to force users to log-out and/or re-authenticate after the defined time period.

Define what actions should be taken when privileged role assignments are no longer appropriate for a user in your organization. Google's *Policy Intelligence has an IAM Recommender feature that helps organizations remove unwanted access to GCP resources by using machine learning to make smart access control recommendations.

Define conditions under which groups accounts are appropriate. Use Cloud Identity or Admin Console to create groups or service accounts. Assign roles and permissions to shared groups and service accounts using Cloud Identity and Access Management (IAM). Use service accounts whenever possible.

Specify what atypical use of an information system account is for your organization, and use tools such as Cloud Operations Suite, *Cloud Security Command Center or *Forseti Security to alert information system admin on atypical use.

Following these guidelines will set the foundation for implementing the following security controls: AC-02, AC-02 (04), AC-02 (05), AC-02 (07), AC-02 (09), AC-02 (11), AC-02 (12), AC-05, AC-06 (01), AC-06 (03), AC-06 (05), AU-2, AU-3, AU-6, AU-12, SI-04, SI-04 (05), SI-04 (11), SI-04 (18), SI-04 (19), SI-04 (20), SI-04 (22), SI-04 (23).

Information Flow Enforcement, Remote Access

In the org-wide access control policy, define information flow control policies for your organization. Identify prohibited or restricted ports, protocols, and services. Define requirements and restrictions for interconnections to internal and external systems. Use tools such as Cloud VPC to create firewalls, logically isolated networks and subnetworks. Cloud Load Balancers, *Traffic Director, and VPC Service Controls can be implemented to help control the flow of information.

When setting information flow control policies, identify controlled network access points for your organization. Use tools such as Cloud Identity Aware Proxy to provide context-based access to cloud resources for remote and onsite users. Use Cloud VPN or Cloud Interconnect to provide secure, direct access to Cloud VPCs.

Set org-wide policies for executing privileged commands and accessing secure data over remote access. Use Cloud IAM and VPC Service Controls to restrict access to sensitive data and workloads.

Following these guidelines will set the foundation for implementing the following security controls: AC-04, AC-04 (08), AC-04 (21), AC-17 (03), AC-17 (04), CA-03 (03), CA-03 (05), CM-07, CM-07(01), CM-07(02).

Logon Attempts, System Use Notification, Session Termination

In the access control policy, specify how long a user should be delayed from accessing a log-on prompt when 3 unsuccessful login attempts has been exceeded in a 15 minute period. Define conditions and triggers under which user sessions will be terminated or disconnected.

Use Cloud Identity Premium Edition or Admin Console to manage mobile devices that connect to your network, including BYOD. Create org-wide security policies that apply to mobile devices. Outline requirements and procedures for purging and wiping mobile devices after consecutive unsuccessful login attempts.

Develop org-wide language and/or system-use notifications that provide privacy policies, terms of use, and security notices to users accessing the information system. Define the conditions under which org-wide notification(s) will be displayed before granting users access. Cloud Pub/Sub is a global messaging and event ingestion system that can be used to push notifications to applications and end users. *Chrome Enterprise Suite, including *Chrome Browser and *Chrome OS, can also be used with *Push API and *Notifications API to send notifications and updates to users.

Following these guidelines will set the foundation for implementing the following security controls: AC-07, AC-07 (02), AC-08, AC-12, AC-12 (01).

Permitted Actions, Mobile Devices, Information Sharing

In the access control policy, define user actions that can be performed on an information system without identification and authentication. Use Cloud IAM to regulate user access to view, create, delete, and modify specific resources.

Additionally, develop org-wide policies for information sharing. Determine circumstances under which information can be shared and when user discretion is required for sharing information. Employ processes to assist users with sharing information and collaborating across the organization. G Suite has a great feature set for controlled collaboration and engagement across teams.

Following these guidelines will set the foundation for implementing the following security controls: AC-14, AC-19 (05), AC-21.

Awareness and Training

Create security policies and associated training materials to disseminate to users and security groups across your organization at least annually. Google offers Professional Services options for educating users on cloud security, including but not limited to a Cloud Discover Security engagement and a G Suite Security Assessment.

Update security policies and training at least annually.

Following these guidelines to aid in implementing security control AT-01.

Auditing and Accountability

Create org-wide auditing policies and accountability controls that address procedures and implementation requirements for auditing personnel, events, and actions tied to cloud information systems.

In the org-wide auditing policy, outline events that should be audited in your organization's information systems, and the auditing frequency. Examples of logged events include: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications, examples include: administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Define additional events of interest for your organization.

The auditing policy should also specify indications of inappropriate or unusual activity for your organization. These activities should be monitored for, logged and flagged regularly (at least weekly).

Use Google's Cloud Operations Suite suite to manage logging, monitoring and alerting for your GCP, on-premise, or other cloud environments. Use Cloud Operations Suite to configure and track security events in your organization. Additionally, Cloud Monitoring allows users to set custom metrics to monitor for org-defined events in audit records.

Enable information systems to alert administrators in the event of audit processing failures. This can be implemented using tools like Cloud Pub/Sub and Cloud Alerting.

Set standards for alerting administrators within a set time period (e.g. within 15 minutes), in the event of a system or functional failure, to include when audit records reach a set threshold or volume capacity. Determine an org-wide granularity of time measurement, by which audit records should be time-stamped and logged. Define the level of tolerance for time-stamped records in the information system audit trail (e.g. nearly real-time, within 20 mins, etc).

Set VPC Resource Quotas to establish the capacity thresholds for audit record storage. Configure Cloud Budget Alerts to notify admins when a percentage of a resource limit has been reached or exceeded.

Define org-wide storage requirements for audit data and records, to include audit log availability and retention requirements. Google Cloud Storage can be used to store and archive audit logs, while BigQuery can be used to perform further log analysis.

Following these guidelines will set the foundation for implementing the following security controls: AU-01, AU-02, AU-04, AU-05, AU-05 (01), AU-06, AU-07 (01), AU-08, AU-08 (01), AU-09 (04), AU-09 (04), AU-12, AU-12 (01), AU-12 (03), CA-07.

Security Assessment and Authorization

Develop an org-wide security assessment and authorization policy that defines the procedures and implementation requirements of organization security assessments, security controls and authorization controls.

In the security assessment and authorization policy, define the level of independence required for security assessment teams to conduct impartial assessments of information systems in the cloud. The information systems that should be assessed by an independent assessor should be identified.

Security assessments should minimally cover: In-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing. The organization should define additional requirements and forms of security assessment.

The security assessment and authorization policy should specify security system classifications and requirements, including requirements for unclassified and non-national security systems.

Within the information flow control policies for your organization, outline requirements and restrictions for interconnections to internal and external systems. Set Cloud VPC firewall rules to allow and deny traffic to information systems, and use VPC service controls to protect sensitive data using security parameters.

Set org-wide auditing and accountability policies that enforce continuous monitoring requirements (CA-07).

Following these guidelines will set the foundation for implementing the following security controls: CA-01, CA-02, CA-02 (01), CA-02 (02), CA-02 (03), CA-03 (03), CA-03 (05), CA-07, CA-07 (01), CA-08, CA-09.

Configuration Management

Create an org-wide configuration management policy that defines the procedures and implementation requirements for org-wide configuration management controls, roles, responsibilities, scope, and compliance.

Standardize configuration setting requirements for org-owned information systems and system components. Provide operational requirements and procedures for configuring information systems. Explicitly call out how many previous versions of a baseline configuration the system administrators are required to retain for information system rollback support. Use Google's suite of Configuration Management tools to control IT system configurations as code, and monitor configuration changes using *Cloud Policy Intelligence, *Cloud Security Command Center, or *Forseti Security.

Specify configuration requirements for each type of information system in your organization (e.g. cloud, on-prem, hybrid, unclassified, CUI, classified, etc). Also, define security safeguard requirements for org-owned and BYOD devices, to include identifying safe and unsafe geographic locations. Use Cloud Identity Aware Proxy to enforce context-based access controls to org-owned data, including access controls by geographic location. Use Cloud Identity Premium edition or Admin Console to enforce security configurations on mobile devices that connect to the corporate network.

In the configuration management policy, define an org-wide configuration change control element, such as a change control committee or board. Document how frequently the change control element will meet and under which conditions. Establish a formal body for reviewing and approving configuration changes.

Identify the configuration management approval authorities for your organization; these administrators will review requests for changes to information systems. Define the time period that authorities have to approve or disapprove change requests. Provide guidance for change implementers to notify approval authorities once info system changes have been completed.

Set restrictions on the use of open source software across your organization, to include the specification of what software is approved and not approved for use. Cloud Identity or Admin Console can be used to enforce approved applications and software for your organization. With Cloud Identity Premium, single sign on and multi-factor authentication for 3rd party applications can be enabled.

Use tools such as Cloud Alerting to send notifications to security administrators when configuration changes are logged. Give admin access to tools like *Cloud Security Command Center, or *Forseti Security to monitor configuration changes in near real-time. Using *Cloud Policy Intelligence, machine learning is used to study configurations defined by your org, raising awareness when configurations change from the baseline.

Enforce least functionality across your organization using **information flow control policies**.

Following these guidelines will set the foundation for implementing the following security controls: CM-01, CM-02 (03), CM-02 (07), CM-03, CM-03 (01), CM-05 (02), CM-05 (03), CM-06, CM-06 (01), CM-06 (02), CM-07, CM-07 (01), CM-07 (02), CM-07 (05), CM-08, CM-08 (03), CM-10 (01), CM-11, CM-11 (01), SA-10.

Contingency Planning

Develop a contingency plan for your organization that defines the procedures and implementation requirements for contingency planning controls across your organization. Identify key contingency personnel, roles, and responsibilities across organizational elements.

Highlight the mission-essential and business-essential information system operations within your organization. Outline recovery time objectives (RTO) and recovery point objectives (RPO) for resuming essential operations once the contingency plan has been activated.

Document critical information systems and associated software. Identify any additional security-related information, and provide guidance and requirements for storing backup copies of critical system components and data. Deploy Google's global, regional, and zonal resources and world-wide locations for high availability. Use Google Cloud Storage classes for multi-regional, regional, backup and archive options. Implement global network auto-scaling and load-balancing with Cloud Load Balancer.

Following these guidelines will set the foundation for implementing the following security controls: CP-01, CP-02, CP-02 (03), CP-07, CP-08, CP-09 (03).

Identification and Authentication

Create an identification and authentication policy for your organization that specifies identification and authentication procedures, scopes, roles, responsibilities, management, entities, and compliance. Specify identification and authentication controls that are required by your organization. Use Cloud Identity Premium or Admin Console to identify corporate and personal devices that can connect to your organization's resources. Use Cloud Identity Aware Proxy (IAP) to enforce context aware access to resources.

Include guidance around authenticator content for your organization, authentication reuse conditions, standards for protecting authenticators, as well as standards for changing or refreshing authenticators. Additionally, capture requirements for using cached authenticators. Specify time limits for using cached authenticators and definitions around when cached authenticators should be expired. Define the minimum and maximum lifetime requirements and refresh time periods that should be enforced by information systems within your organization.

Use Cloud Identity or Admin Console to enforce password policies for sensitivity, character usage, new password creation or reuse, password lifetime, storage and transmission requirements.

Outline hardware and/or software token authentication requirements for authentication across your organization, including but not limited to PIV card and PKI requirements. *Google

Titan Security Keys can be used to enforce additional authentication requirements for administrators and privileged personnel.

In the identification and authentication policy, outline the Federal Identity, Credential, and Access Management (FICAM) information system components that are allowable for accepting 3rd parties in your organization. Google's Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to applications being accessed by external entities.

Following these guidelines will set the foundation for implementing the following security controls: IA-01, IA-03, IA-04, IA-05, IA-05 (01), IA-05 (03), IA-05 (04), IA-05 (11), IA-05 (13), IA-08 (03).

Incident Response

Establish an incident response policy for your organization, including procedures to facilitate and implement incident response controls. Create security groups for your organization's incident response teams and authorities. Use tools such as Cloud Operations Suite or *Cloud Security Command Center to share incident events, logs, and details. *Incident Response Management (IRM) enables admin to investigate and resolve information system security incidents end-to-end.

Develop an incident response test plan, procedures and checklists, requirements and benchmarks for success. Specify classes of incidents that should be recognized by your organization, and outline the associated actions to take in response to such incidents. Define the specific actions that should be taken by authorized personnel in the event of an incident, such as steps for managing information spills, cybersecurity vulnerabilities and attacks.Take advantage of capabilities in G Suite to scan and quarantine email content, block phishing attempts, and set restrictions on attachments. Use Cloud Data Loss Prevention to inspect, classify, and de-identify sensitive data to help restrict exposure.

Specify org-wide requirements for incident response training, including training requirements for general users and privileged roles & responsibilities. Enforce time period requirements for taking training (e.g. within 30 days of joining, quarterly, annually, etc).

Following these guidelines will set the foundation for implementing the following security controls: IR-01, IR-02, IR-03, IR-04 (03), IR-04 (08), IR-06, IR-08, IR-09, IR-09 (01), IR-09 (03), IR-09 (04).

System Maintenance

Create a system maintenance policy for your organization, documenting system maintenance controls, roles, responsibilities, management, coordination requirements and compliance. Define parameters for controlled maintenance, including approval processes for conducting off-site maintenance and repairs, and org-wide turn around times for replacing failed devices and parts. Your organization will benefit from Data deletion on Google Cloud Platform data and equipment sanitization, and Google's Data Center security & innovation for off-site maintenance and repairs.

Following these guidelines will set the foundation for implementing the following security controls: MA-01, MA-02, MA-06.

Media Protection

As part of Google Cloud's FedRAMP ATO, we meet media protection requirements for physical infrastructure. Review Google's Infrastructure Security Design and Security Overview. Customers are subsequently responsible for meeting virtual infrastructure security requirements.

Develop a media protection policy for your organization, documenting media controls, protection policies and procedures, compliance requirements, management roles & responsibilities. Document procedures for facilitating and implementing media protections across your organization. Create security groups defining personnel and roles for managing media and their protections.

Specify approved media types and accesses for your organization, including digital and non-digital media restrictions. Additionally, set media markings and media handling caveats that must be implemented across your organization, including security marking requirements inside and outside of controlled access areas. Use *Google Data Catalog to manage cloud resource metadata, simplifying data discovery. Control cloud resource compliance across your organization, regulating the distribution and discovery of cloud resources with *Google Private Catalog.

Identify how media that is managed by your organization should be sanitized and disposed of or reused. Also, outline use cases and/or circumstances where sanitization, disposal, or reuse of media/devices are required or acceptable. Define the media safeguard methods and mechanisms that are deemed acceptable for your organization.

With Google, you'll benefit from Data deletion on Google Cloud Platform data and equipment sanitization, and Google's Data Center security & innovation. In addition, Cloud KMS and Cloud HSM provide FIPS-compliant cryptographic protection, while *Google Titan Security Keys can be used to enforce additional physical authentication requirements for administrators and privileged personnel.

Following these guidelines will set the foundation for implementing the following security controls: MP-01, MP-02, MP-03, MP-04, MP-06, MP-06 (03), MP-07.

Physical and Environmental Protection

As part of Google Cloud's FedRAMP ATO, we meet physical and environmental protection requirements for physical infrastructure. Review Google's Infrastructure Security Design and Security Overview. Customers are subsequently responsible for meeting virtual infrastructure security requirements.

Establish a physical and environmental protection policy for your organization, outlining protection controls, protection entities, compliance standards, roles, responsibilities, and

management requirements. Outline how physical and environmental protection should be implemented across your organization.

Create security groups defining personnel and roles for managing physical and environmental protections. Require admin accessing sensitive computational resources to use *Titan Security Keys or some other form of MFA to verify access integrity.

In the physical and environmental protection policy, define physical access control requirements for your organization. Identify facility entry & exit points for information system sites, access control safeguards for such facilities, and inventory requirements. Take advantage of tools such as *Google Maps Platform to visually display and track facilities, entry and exit points for locational mappings. Use Cloud Resource Manager and *Private Catalog to control access to cloud resources, making them organized and easily discoverable.

Use Cloud Monitoring to configure loggable events, accesses and incidents. Define org-wide physical access events that should be logged in Cloud Logging. Use *Incident Response Management to address physical security incidents that have been triggered, and consolidate findings in *Cloud Security Command Center.

Use the physical and environmental protection policy to account for emergency situations, such as emergency shutoff of information systems, emergency power, fire suppression, and emergency response. Identify points of contact for emergency response, including local emergency responders and physical security personnel for your organization. Outline requirements and locations for alternate work sites. Specify security controls and personnel for primary and alternate work sites. Deploy Google's global, regional, and zonal resources and world-wide locations for high availability. Use Google Cloud Storage classes for multi-regional, regional, backup and archive options. Implement global network auto-scaling and load-balancing with Cloud Load Balancer. Create declarative Deployment Templates to establish a repeatable, template-driven deployment process.

Following these guidelines will set the foundation for implementing the following security controls: PE-01, PE-03, PE-03 (01), PE-04, PE-06, PE-06 (04), PE-10, PE-13 (02), PE-17.

System Security Planning

Develop a security planning policy for your organization, outlining security planning controls, roles, responsibilities, managements, security planning entities for your organization, and compliance requirements. Outline how security planning should be implemented across your organization.

Create groups to define security planning personnel accordingly. Specify security groups for security assessments, audits, hardware and software maintenance, patch management, and contingency planning for your organization. Use tools such as Cloud Operations Suite, *Cloud Security Command Center or *Forseti Security to monitor security, compliance, and access control across your organization.

Following these guidelines will set the foundation for implementing the following security controls: PL-01, PL-02, PL-02 (03).

Personnel Security

Create a personnel security policy that outlines who security personnel are, roles and responsibilities of security personnel, how personnel security should be implemented, and what personnel security control should be enforced across your organization. Capture conditions that would require individuals to go through organizational security screening, re-screening, and investigation. Outline requirements for security clearances in your organization.

Include guidance for addressing personnel termination and transfer. Define needs and parameters for exit interviews and the security topics that should be discussed during such interviews. Specify when security/admin entities in your organization should be notified of personnel termination, transfer, or reassignment (e.g. within 24 hours). Specify actions that must be completed by personnel and the organization in the event of a transfer, reassignment or termination. Also, cover requirements for enforcing formal employee sanctions. Explain when security personnel/admin should be notified of employee sanctions, and sanction processes.

Use Cloud IAM to assign roles and permissions to personnel. Add, remove, disable and enable personnel profiles and accesses in Cloud Identity or Admin Console. Enforce additional physical authentication requirements for administrators and privileged personnel using *Titan Security Keys.

Following these guidelines will set the foundation for implementing the following security controls: PS-01, PS-03, PS-04, PS-05, PS-07, PS-08.

Risk Assessment

Implement a risk assessment policy that outlines who risk assessment personnel are, what risk assessment controls should be enforced across your organization, and procedures for carrying out risk assessments within your organization. Define how risk assessments should be documented and reported. Use tools such as *Forseti Security and *Cloud Security Command Center to automatically notify security personnel of security risks and the overall security posture of your organization.

Leverage Google's suite of risk assessment tools such as Cloud Security Scanner, Container Analysis, Cloud Armor, and G Suite phishing and malware protection to scan for and report on vulnerabilities across your organization's information systems. Make these tools available to risk assessment personnel and admin to help identify and eliminate vulnerabilities.

Following these guidelines will set the foundation for implementing the following security controls: RA-01, RA-03, RA-05.

System and Services Acquisition

Develop a system and services acquisition policy that outlines key personnel's roles and responsibilities, acquisition and services management, compliance, and entities. Outline system and services acquisition procedures and implementation guidelines for your organization.

Define your organization's system development lifecycle for information systems and information security. Outline information security roles and responsibilities, personnel, and how your organization's risk assessment policy should drive and influence system development life-cycle activities.

Highlight procedures that should be carried out within your organization when information system documentation is not available and/or undefined. Engage your organization's information system administrators and/or system services personnel as required. Define any required training for administrators and users that are implementing or accessing information systems within your organization.

Use tools such as *Cloud Security Command Center and *Forseti Security to track security compliance, findings, and security control policies for your organization. Google outlines all of its security standards, regulations, and certifications to help educate customers on how to meet compliance requirements and laws on Google Cloud. In addition, Google offers a suite of security products to help customers continuously monitor their information systems, communications, and data both in the cloud and on-premise.

Specify any locational restrictions for your organization's data, services, and information processing, and under which conditions data can be stored elsewhere. Google offers global, regional, and zonal options for data storage, processing, and services utilization in GCP.

Leverage the configuration management policy to regulate developer configuration management for system and services acquisition controls, and **use the security assessment and authorization policy** to enforce developer security testing and evaluation requirements.

Following these guidelines will set the foundation for implementing the following security controls: SA-01, SA-03, SA-05, SA-09, SA-09 (01), SA-09 (04), SA-09 (05), SA-10, SA-11, SA-16.

System and Communications Protection

Create a system and communications protection policy that outlines key personnel's roles and responsibilities, implementation requirements for systems communication protection policies, and required protection controls for your organization. Identify the types of denial of service attacks your organization recognizes and monitors for, and outline DoS protection requirements for your organization.

Use Cloud Operations Suite to log, monitor, and alert on predefined security attacks against your organization. Implement tools such as Cloud Load Balancing and Cloud Armor to safeguard your cloud perimeter, and leverage Cloud VPC services such as firewalls and network security controls to protect your internal cloud network.

Identify your organization's resource availability requirements; define how cloud resources will be allocated across your organization and what constraints will be implemented to restrict over-utilization. Use tools such as Cloud Resource Manager to control access to resources at the organization, folder, project, and individual resource level. Set Cloud Resource Quotas to manage API requests and resource utilization in GCP.

Establish boundary protection requirements for your information systems and system communications. Define requirements for internal communications traffic and how internal

traffic should engage with external networks. Specify requirements for proxy servers and other network routing and authentication components.

Take advantage of *Cloud Traffic Director to manage network traffic and communications flow for your organization. Use Cloud Identity Aware Proxy to control access to cloud resources based on authentication, authorization, and context - including geographic location or device fingerprint. Implement *Google Private Access, *Cloud VPN, or *Cloud Interconnect to secure network traffic and communications between internal and external resources. Cloud VPC can be used to define and secure your organization's cloud networks; establish subnetworks to further isolate cloud resources and network perimeters.

Additionally, Google offers global software-defined networks with multi-regional, regional, and zonal options for high-availability and failover. Define failure requirements for your organization to ensure that your information systems fail to a known state. Capture requirements for preserving information system state information. Use Managed Instance Groups and Deployment Manager templates to re-instantiate failed or unhealthy resources. Give administrators access to *Cloud Security Command Center or *Forseti Security to actively monitor your organization's confidentiality, integrity, and availability posture.

In the policy, outline your organization's requirements for managing cryptographic keys, including requirements for key generation, distribution, storage, access, and destruction. Cloud KMS and Cloud HSM can be used to manage, generate, use, rotate, store and destroy FIPS-compliant security keys in the cloud.

Google encrypts data at rest by default, however you can use Cloud KMS with Compute Engine and Google Cloud Storage to additionally encrypt data using cryptographic keys. You can also deploy Shielded VMs to enforce kernel-level integrity controls on GCE VMs

Following these guidelines will set the foundation for implementing the following security controls: SC-01, SC-05, SC-06, SC-07 (08), SC-07 (12), SC-07 (13), SC-07 (20), SC-07 (21), SC-12, SC-24, SC-28, SC-28 (01).

System and Information Integrity

Implement a system and information integrity policy that outlines key personnel's roles and responsibilities, integrity implementation procedures and requirements, compliance standards, and security controls for your organization. Create security groups for the personnel in your organization that are responsible for system and information integrity. Outline flaw-remediation requirements for your organization, to include guidelines for monitoring, assessing, authorizing, implementing, planning, benchmarking, and remediating security flaws across your organization and its information systems.

Leverage Google's suite of security tools, including by not limited to Chrome Browser, Cloud Security Scanner, Container Analysis, G Suite Phishing & Malware Protections, G Suite Security Center, and Cloud Armor to protect against malicious code, cyber attacks and common vulnerabilities, quarantine spam, set spam and malware policies, alert administrators on vulnerabilities, and to gain insights across your organization for central management. Use tools such as Cloud Operations Suite, *Cloud Security Command Center or *Forseti Security to centrally manage, alert on and monitor your organization's security controls and findings. More

specifically, Cloud Operations Suite should be used to log administrative actions, data accesses, and system events initiated by privileged users and personnel across your organization. notify administrative personnel on error messages and information system error handling.

Define security-relevant events relative to your organization's software, firmware, and information (e.g. zero-day vulnerabilities, unauthorized data deletion, installation of new hardware, software, or firmware, etc). Explain the steps that should be taken when these types of security-relevant changes occur. Specify monitoring objectives and/or indicators of attack for administrators to pay special attention to, to include essential information that should be monitored within information systems across your organization. Define system and information monitoring roles and responsibilities, as well as monitoring & reporting frequency (e.g. real-time, every 15 mins, every hour, quarterly reporting, etc).

Capture requirements for analyzing communications traffic for information systems across your organization. Specify requirements for discovering anomalies, including system points for monitoring. *Google's Network Telemetry services make it possible to conduct in-depth network performance and security monitoring. Google also has strong 3rd party partnerships that integrate with GCP for scanning and protecting cloud endpoints and hosts, such as +Aqua Security and +Crowdstrike. Shielded VMs make it possible to harden devices, verify authentication and ensure secure boot processes.

Define how your organization should check and safeguard against security anomalies and integrity violations. Use tools such as *Cloud Security Command Center, *Forseti Security, or *Cloud Policy Intelligence to monitor and detect configuration changes. Use +Configuration Management Tools or Deployment Manager templates to re-instantiate or to halt changes to cloud resources.

Additionally in the system information and integrity policy, specify requirements for authorizing and approving network services within your organization. Outline approval and authorization processes for network services. Cloud VPC is essential for defining cloud networks and subnetwork using firewalls to protect network perimeters. VPC Service Controls make it possible to enforce additional network security perimeters for sensitive data in the cloud.

On top of all of this, you'll automatically inherit Google's secure boot stack and trusted, defense in depth infrastructure.

Following these guidelines will set the foundation for implementing the following security controls: SI-01, SI-02 (01), SI-02 (03), SI-03 (01), SI-04, SI-04 (05), SI-04 (11), SI-04 (18), SI-04 (19), SI-04 (20), SI-04 (22), SI-04 (23), SI-05, SI-06, SI-07, SI-07 (01), SI-07 (05), SI-07 (07), SI-08 (01), SI-10, SI-11, SI-16.

Conclusion

Security and compliance in the cloud is a joint effort on behalf of the customer and the cloud services provider. While Google ensures that the physical infrastructure and corresponding services support compliance against dozens of 3rd party standards, regulations and certifications, customers are required to ensure that anything they build in the cloud is compliant.

Google Cloud supports customers in their compliance efforts by making the same set of security products and capabilities that Google uses to protect its infrastructure, available for customers.

Additional Resources

- Google Security Products & Capabilities

External Resources

- GSA FedRAMP Security Controls Quick Guide
- FedRAMP Security Controls Baseline(s)
- FedRAMP Moderate SSP Template
- FedRAMP High SSP Template
- FedRAMP for Cloud Service Providers
- FedRAMP Security Assessment Framework
- FedRAMP Template Documentation

Appendix

FedRAMP Moderate Security Controls

There are 325 security controls for FedRAMP moderate compliance in the cloud. 83 security controls are information system requirements, while 242 controls are requirements for the organization. The security controls breakdown for the organization and the information system is as follows:

Information System Controls

Access Control: AC-2 (2), AC-2 (3), AC-2 (4), AC-2 (10), AC-3, AC-4, AC-4 (21), AC-6 (9), AC-6 (10), AC-7, AC-8, AC-10, AC-11, AC-11 (1), AC-12, AC-17 (1), AC-17 (2), AC-17 (3), AC-18 (1)

Audit and Accountability: AU-3, AU-3 (1), AU-5, AU-7, AU-7 (1), AU-8, AU-8 (1), AU-9, AU-9 (2), AU-12

Configuration Management: CM-5 (1), CM-5 (3), CM-7 (2)

Contingency Planning: CP-10 (2)

Identification and Authentication: IA-2, IA-2 (1), IA-2 (12), IA-2 (2), IA-2 (3), IA-2 (8), IA-2 (11), IA-3, IA-5 (1), IA-5 (2), IA-5 (11) , IA-6, IA-7, IA-8, IA-8 (1), IA-8 (2), IA-8 (4)

Media Protection: MP-5 (4)

Risk Assessment: RA-5 (5)

Systems and Communications Protection: SC-2, SC-4, SC-5, SC-6, SC-7, SC-7 (5), SC-7 (7), SC-7 (8), SC-7 (18), SC-8, SC-8 (1), SC-10, SC-13, SC-15, SC-20, SC-21, SC-22, SC-23, SC-28, SC-28 (1), SC-39

System and Information Integrity: SI-3 (2), SI-3 (7), SI-4 (4), SI-4 (5), SI-6, SI-7 (1), SI-8 (2), SI-10, SI-11, SI-16

Organization Controls

Access Control: AC-1, AC-2, AC-2 (1), AC-2 (5), AC-2 (7), AC-2 (9), AC-2 (12), AC-5, AC-6, AC-6 (1), AC-6 (2), AC-6 (5), AC-14, AC-17, AC-17 (4), AC-17 (9), AC-18, AC-19, AC-19 (5), AC-20, AC-20 (1), AC-20 (2), AC-21, AC-22

Awareness and Training: AT-1, AT-2, AT-2 (2), AT-3, AT-4

Audit and Accountability: AU-1, AU-2, AU-2 (3), AU-4, AU-6, AU-6 (1), AU-6 (3) ,AU-9 (4), AU-11

Security Assessment and Authorization: CA-1 ,CA-2, CA-2 (1), CA-2 (2), CA-2 (3), CA-3, CA-3 (3), CA-3 (5), CA-5, CA-6, CA-7, CA-7 (1), CA-8, CA-8 (1), CA-9

Configuration Management: CM-1, CM-2, CM-2 (1), CM-2 (2), CM-2 (3), CM-2 (7), CM-3, CM-4, CM-5, CM-5 (5), CM-6, CM-6 (1), CM-7, CM-7 (1), CM-7 (5), CM-8, CM-8 (1), CM-8 (3), CM-8 (5), CM-9, CM-10, CM-10 (1), CM-11

Contingency Planning: CP-1, CP-2, CP-2 (1), CP-2 (2), CP-2 (3), CP-2 (8), CP-3, CP-4, CP-4 (1), CP-6, CP-6 (1), CP-6 (3), CP-7, CP-7 (1), CP-7 (2), CP-7 (3), CP-8, CP-8 (1), CP-8 (2), CP-9, CP-9 (1), CP-9 (3), CP-10

Identification and Authentication: IA-1, IA-2 (5), IA-4, IA-4 (4), IA-5, IA-5 (3), IA-5 (4), IA-5 (6), IA-5 (7), IA-8 (3)

Incident Response: IR-1, IR-2, IR-3, IR-3 (2), IR-4, IR-4 (1), IR-5, IR-6, IR-6 (1), IR-7, IR-7 (1), IR-7 (2), IR-8, IR-9, IR-9 (1), IR-9 (2), IR-9 (3), IR-9 (4)

Maintenance: MA-1, MA-2, MA-3, MA-3 (1), MA-3 (2), MA-3 (3), MA-4, MA-4 (2), MA-5, MA-5 (1), MA-6

Media Protection: MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-6 (2), MP-7, MP-7 (1)

Physical and Environmental Protection: PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-6 (1), PE-8, PE-9, PE-10, PE-11, PE-12, PE-13, PE-13 (2), PE-13 (3), PE-14, PE-14 (2), PE-15, PE-16, PE-17

Planning: PL-1, PL-2, PL-2 (3), PL-4, PL-4 (1), PL-8

Personnel Security: PS-1, PS-2, PS-3, PS-3 (3), PS-4, PS-5, PS-6, PS-7, PS-8

Risk Assessment: RA-1, RA-2, RA-3, RA-5, RA-5 (1), RA-5 (2), RA-5 (3), RA-5 (6), RA-5 (8)

System and Services Acquisition: SA-1, SA-2, SA-3, SA-4, SA-4 (1), SA-4 (2), SA-4 (8), SA-4 (9), SA-4 (10), SA-5, SA-8, SA-9, SA-9 (1), SA-9 (2), SA-9 (4), SA-9 (5), SA-10, SA-10 (1), SA-11, SA-11 (1), SA-11 (2), SA-11 (8)

System and Communications Protection: SC-1, SC-7 (3), SC-7 (4), SC-7 (12), SC-7 (13), SC-12, SC-12 (2), SC-12 (3), SC-17, SC-18, SC-19

System and Information Integrity: SI-1, SI-2, SI-2 (2), SI-2 (3), SI-3, SI-3 (1), SI-4, SI-4 (1), SI-4 (2), SI-4 (14), SI-4 (16), SI-4 (23), SI-5, SI-7, SI-7 (7), SI-8, SI-8 (1), SI-12

FedRAMP High Security Controls

There are 420 security controls for FedRAMP high compliance in the cloud. 106 security controls are information system requirements, while 314 controls are requirements for the organization. The security controls breakdown for the organization and the information system is as follows:

Information System Controls

Access Control: AC-2 (2), AC-2 (3), AC-2 (4), AC-2 (10), AC-2 (11), AC-3, AC-4, AC-4 (8), AC-4 (21), AC-6 (8), AC-6 (9), AC-6 (10), AC-7, AC-7 (2), AC-8, AC-10, AC-11, AC-11 (1), AC-12, AC-12 (1), AC-17 (1), AC-17 (2), AC-17 (3), AC-18 (1)

Audit and Accountability: AU-3, AU-3 (1), AU-3 (2), AU-5, AU-5 (1), AU-5 (2), AU-6 (4), AU-7, AU-7 (1), AU-8, AU-8 (1), AU-9, AU-9 (2), AU-10, AU-12, AU-12 (1), AU-12 (3)

Configuration Management: CM-5 (1), CM-5 (3), CM-7 (2), CM-11 (1)

Contingency Planning: CP-10 (2)

Identification and Authentication: IA-2, IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (4), IA-2 (8), IA-2 (9), IA-2 (11), IA-2 (12), IA-3, IA-5 (1), IA-5 (2), IA-5 (11), IA-5 (13), IA-6, IA-7, IA-8, IA-8 (1), IA-8 (2), IA-8 (4)

Maintenance: MA-4 (6)

Media Protection: MP-5 (4)

Risk Assessment: RA-5 (5)

Systems and Communications Protection: SC-2, SC-3, SC-4, SC-5, SC-6, SC-7, SC-7 (5), SC-7 (7), SC-7 (8), SC-7 (18), SC-7 (20), SC-8, SC-8 (1), SC-10, SC-13, SC-15, SC-20, SC-21, SC-22, SC-23, SC-23 (1), SC-24, SC-28, SC-28 (1),SC-39

System and Information Integrity: SI-3 (2), SI-3 (7), SI-4 (4), SI-4 (5), SI-4 (22), SI-4 (24), SI-6, SI-7 (1), SI-7 (5), SI-8 (2), SI-10, SI-11, SI-16

Organization Controls

Access Control: AC-1, AC-2, AC-2 (1), AC-2 (5), AC-2 (7), AC-2 (9), AC-2 (12), AC-2 (13), AC-5, AC-6, AC-6 (1), AC-6 (2), AC-6 (3), AC-6 (5), AC-6 (7), AC-14, AC-17, AC-17 (4), AC-17 (9), AC-18, AC-18 (3), AC-18 (4), AC-18 (5), AC-19, AC-19 (5), AC-20, AC-20 (1), AC-20 (2), AC-21, AC-22

Awareness and Training: AT-1, AT-2, AT-2 (2), AT-3, AT-3 (3), AT-3 (4), AT-4

Auditing and Accountability: AU-1, AU-2, AU-2 (3), AU-4, AU-6, AU-6 (1), AU-6 (3), AU-6 (5), AU-6 (6), AU-6 (7), AU-6 (10), AU-9 (4), AU-9 (4), AU-11

Security Assessment and Authorization: CA-1, CA-2, CA-2 (1), CA-2 (2), CA-2 (3), CA-3, CA-3 (3), CA-3 (5), CA-5, CA-6, CA-7, CA-7 (1), CA-7 (3), CA-8, CA-8 (1), CA-9

Configuration Management: CM-1, CM-2, CM-2 (1), CM-2 (2), CM-2 (3), CM-2 (7), CM-3, CM-3 (1), CM-3 (2), CM-3 (4), CM-3 (6), CM-4, CM-4 (1), CM-5, CM-5 (2), CM-5 (5), CM-6, CM-6 (1), CM-6 (2), CM-7, CM-7 (1), CM-7 (5), CM-8, CM-8 (1), CM-8 (2), CM-8 (3), CM-8 (4), CM-8 (5), CM-9, CM-10, CM-10 (1), CM-11

Contingency Planning: CP-1, CP-2, CP-2 (1), CP-2 (2), CP-2 (3), CP-2 (4), CP-2 (5), CP-2 (8), CP-3, CP-3 (1), CP-4, CP-4 (1), CP-4 (2), CP-6, CP-6 (1), CP-6 (2), CP-6 (3), CP-7, CP-7 (1), CP-7 (2), CP-7 (3), CP-7 (4), CP-8, CP-8 (1), CP-8 (2), CP-8 (3), CP-8 (4), CP-9, CP-9 (1), CP-9 (2), CP-9 (3), CP-9 (5), CP-10, CP-10 (4)

Identification and Authentication: IA-1, IA-2 (5), IA-4, IA-4 (4), IA-5, IA-5 (3), IA-5 (4), IA-5 (6), IA-5 (7), IA-5 (8), IA-8 (3)

Incident Response: IR-1, IR-2 IR-2 (1), IR-2 (2), IR-3, IR-3 (2), IR-4, IR-4 (1), IR-4 (2), IR-4 (3), IR-4 (4), IR-4 (6), IR-4 (8), IR-5, IR-5 (1), IR-6, IR-6 (1), IR-7, IR-7 (1), IR-7 (2), IR-8, IR-9, IR-9 (1), IR-9 (2), IR-9 (3), IR-9 (4)

Maintenance: MA-1, MA-2, MA-2 (2), MA-3, MA-3 (1), MA-3 (2), MA-3 (3), MA-4, MA-4 (2), MA-4 (3), MA-5, MA-5 (1), MA-6

Media Protection: MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-6 (1), MP-6 (2), MP-6 (3), MP-7, MP-7 (1)

Physical and Environmental Protection: PE-1, PE-2, PE-3, PE-3 (1), PE-4, PE-5, PE-6, PE-6 (1), PE-6 (4), PE-8, PE-8 (1), PE-9, PE-10, PE-11, PE-11 (1), PE-12, PE-13, PE-13 (1), PE-13 (2), PE-13 (3), PE-14, PE-14 (2), PE-15, PE-15 (1), PE-16, PE-17, PE-18

Planning: PL-1, PL-2, PL-2 (3), PL-4, PL-4 (1), PL-8

Personnel Security: PS-1, PS-2, PS-3, PS-3 (3), PS-4, PS-4 (2), PS-5, PS-6, PS-7, PS-8

Risk Assessment: RA-1, RA-2, RA-3, RA-5, RA-5 (1), RA-5 (2), RA-5 (3), RA-5 (4), RA-5 (6), RA-5 (8), RA-5 (10)

System and Services Acquisition: SA-1, SA-2, SA-3, SA-4, SA-4 (1), SA-4 (2), SA-4 (8), SA-4 (9), SA-4 (10), SA-5, SA-8, SA-9, SA-9 (1), SA-9 (2), SA-9 (4), SA-9 (5), SA-10, SA-10 (1), SA-11, SA-11 (1), SA-11 (2), SA-11 (8), SA-12, SA-15, SA-16, SA-17

System and Communications Protection: SC-1, SC-7 (3), SC-7 (4), SC-7 (10), SC-7 (12), SC-7 (13), SC-7 (21), SC-12, SC-12 (1), SC-12 (2), SC-12 (3), SC-17, SC-18, SC-19

System Information and Integrity: SI-1, SI-2, SI-2 (1), SI-2 (2), SI-2 (3), SI-3, SI-3 (1), SI-4, SI-4 (1), SI-4 (2), SI-4 (11), SI-4 (14), SI-4 (16), SI-4 (18), SI-4 (19), SI-4 (20), SI-4 (23), SI-5, SI-5 (1), SI-7, SI-7 (2), SI-7 (7), SI-7 (14), SI-8, SI-8 (1), SI-12