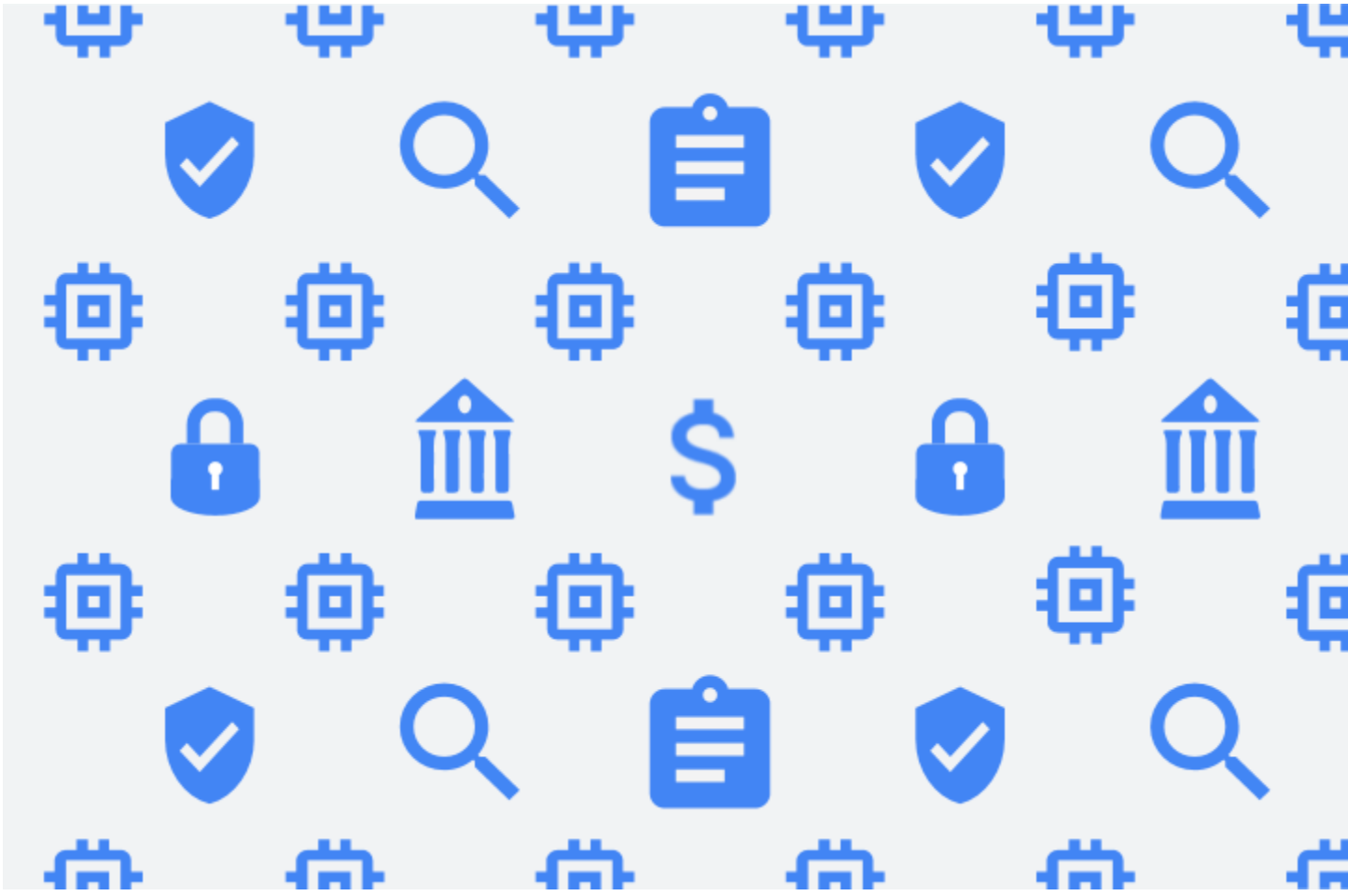
Google Cloud Whitepaper
October 2019

Response to the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook



Google Cloud

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of October 2019 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

Trusted & Robust Infrastructure

Google is an innovator in hardware, software, network, and system management technologies. We custom design our servers, proprietary operating system, and geographically distributed data centers to operate all our services securely including both consumer services as well as our enterprise services for Google Cloud — G Suite and Google Cloud Platform. Using the “defense in depth” principles, we have created an IT infrastructure at Google where security is tightly woven and built into progressive layers — starting from the physical security of our data centers, to building underlying security-designed hardware and software, to continuing with secure service deployment, secure data storage with end user privacy safeguards, secure communication between services, secure Internet communication, and finally, to operating the infrastructure in a secure fashion.

Our infrastructure components are designed to be highly redundant. This redundancy applies to server design and deployment, data storage, network and Internet connectivity, and the software services themselves. This “redundancy of everything” creates a robust solution that is not dependent on a single server, data center, or network connection. In the event of hardware, software, or network failure, platform services and control planes are capable of automatically changing the configuration so that customers can continue to work without interruption. Our highly redundant infrastructure also helps customers protect themselves from data loss. Customers can create and deploy our cloud-based resources across multiple regions and zones, allowing them to build resilient and highly available systems.

For more information about our infrastructure, refer to the Google Cloud Infrastructure Security Design Overview, GCP Data Processing and Security Terms, Appendix 2: Security Measures and G Suite Data Processing Amendment, Appendix 2: Security Measures.

State-of-the-Art Data Center Security

Google Cloud has a dedicated security team that supports state-of-the-art data centers. Our data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that detect and track intruders. Access logs, activity records, and camera footage are reviewed as a part of our incident response process. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Access to data centers are heavily monitored and controlled-- fewer than one percent of Googlers will ever set foot in one. For more information, refer to our data centers page.

Data Encryption

Google Cloud Platform (GCP) encrypts customer data at rest, without any action required from customers, using one or more encryption mechanisms. There are some exceptions noted in this document. In addition to encryption at rest, GCP uses various methods of encryption, both default and user configurable, for data in transit. The type of encryption used depends on the OSI layer, the type of service, and the physical infrastructure component.

Hypervisor Controls

At Google Cloud, we initially started from the open-source KVM (Kernel-based Virtual Machine) hypervisor — validated by scores of researchers, to build the foundation of Google Compute Engine and Google Container Engine. Since then, we have significantly invested in building additional hardening and protection to improve the safety and security of customer applications, based on our research and testing experience. This includes reducing the attack surface area by removing unnecessary components of the open-source KVM code, reducing the number of the kernel binaries and moving their functionality to the user mode, and creating our own user-space virtual machine monitor. We also perform on-going penetration testing and security reviews of the open-source KVM as well as Google Cloud KVM to ensure that we don't have vulnerabilities that could be exploited. Furthermore, we report our security findings back to linux.org to improve the open-source KVM, for the benefit of the overall open-source community. For more information on our KVM hypervisor security, check out our GCP blog.

Cloud-Native Technology

At Google Cloud, we continue to invest heavily in security, both in the design of new features and the development of cutting-edge tools for customers to more securely manage their environments on GCP as well as G Suite. Examples include the GCP Cloud Security Command Center and the G Suite Security Center, which bring actionable insights to security teams. VPC Service Controls also help to establish virtual security perimeters for sensitive data. For more information about our security technologies, refer to our security products & capabilities page.

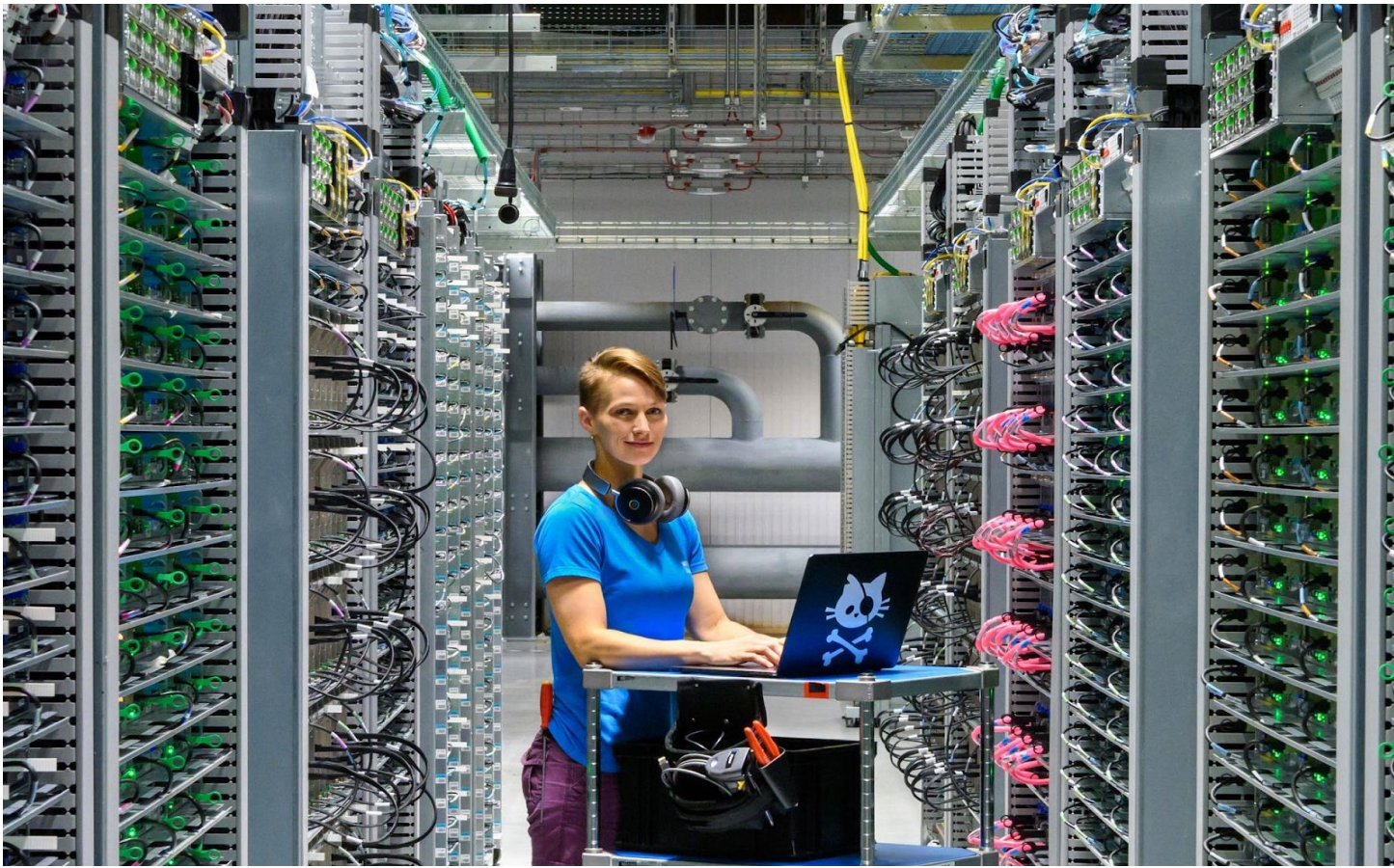
Vulnerability Management & Threat Monitoring

Our vulnerability management process actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities.

In addition, our security monitoring program gathers information from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities. Google security engineers look for security incidents that might affect the integrity of the infrastructure. Moreover, automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs.

Data Access & Customer Control

Google Cloud customers own their data, not Google. Google will only process customer data in accordance with its customer contract terms. We also provide customers with solutions that allow granular control of resource permissions. For example, by using Cloud Identity and Access Management (IAM), customers can map job functions to groups and roles so users only access the data they need to get the job done. Customers can also use our cross-function product, Cloud Identity, to manage users, devices and apps from a single console. Customers may delete data from our systems or take it with them if they choose to stop using our services.



Unauthorized Access Prevention

Protection from Google insider threats

Only a small group of Google employees has access to customer data based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources. Request for additional access is granted according to a stringent formal process, as dictated by our security policies and is also tracked through audit records. Access Transparency gives you near real-time logs when Google Cloud Platform administrators access your content. Moreover, we have extended Access Transparency to G Suite. Access Transparency for G Suite enables you to get more visibility into actions taken by Google staff related to your data. You can view the reason for each access, including references to specific support tickets where relevant, which may help you support your audit requirements.

Protection from multi-tenancy threats

To prevent unauthorized access by other tenants sharing the same physical server, we logically isolate our customers' data. We also have a variety of isolation and sandboxing techniques for protecting a service from other services running on the same machine. These techniques include normal Linux user separation, language and kernel-based sandboxes, and hardware virtualization. Furthermore, we perform encryption at the application layer which allows our infrastructure to isolate itself from potential threats at the lower levels of storage such as malicious disk firmware. For more information about our logical isolation, refer to the Administrative access section in the Google Security Whitepaper.

Protection from external threats

To prevent unauthorized access to our customers' data from external threat actors, we employ a defense in depth approach starting with state-of-the-art physical security at our data centers. We have also designed our entire infrastructure stack for security, using cryptographic signatures to ensure no unauthorized changes can be made without detection. This starts from low level components such as the BIOS, and includes all key components of the boot process such as the bootloader, kernel and the base

operating system. All of the components are controlled, built and hardened by us. In addition, our operations teams detect and respond to threats to the infrastructure from both insiders and external actors, 24/7/365.

Incident Response Plans & Breach Notification

Google has a rigorous incident management process that specifies actions, escalations, mitigation, resolution, and notification of potential incidents impacting the confidentiality, integrity, or availability of systems or data. We assign the highest priority to events that directly impact our customers. Key staff are trained in forensics and handling evidence in preparation for an event. We test incident response plans for key areas, such as systems that store sensitive customer information. The Google security team operates 24/7.

Additionally, we will promptly notify customers if we detect a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to their data on systems we manage. Moreover, we will assist with investigative efforts via our support team. For more information, refer to our Data Incident Response Process Whitepaper.

Google has a rigorous data incident management process that specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of systems or data.

Third-Party Suppliers, Vendors & Subcontractors

Google reviews the information governance practices and security posture of the vendors, third-party suppliers, and their products with which Google shares confidential or sensitive information. We ensure that they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Google includes an Information Protection Addendum (IPA) to contracts with its sub-processors who have access to customer data. The IPA defines the security and privacy obligations sub-processors must meet to satisfy Google's requirements regarding customer data. A list of GCP's sub-processors and the services they provide is available here. A list of G Suite's sub-processors and the services they provide is available here.

Google Cloud's Approach to Compliance

Industry Certifications & Independent Third-Party Attestations

Google Cloud products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn the trust of our customers. We are constantly working to expand our coverage.

Below are certifications and assessments most relevant to the financial industry in the United States. For more information, refer to our compliance page.

ISO 27001
The International Organization for Standardization (ISO) 27001 is a security standard that outlines and provides the requirements for an information security management system. The 27001 standard lays out a framework and checklist of controls that allows Google to ensure a comprehensive and continually improving model for security management. Google Cloud is certified as ISO 27001 compliant.

ISO 27017
The ISO/IEC 27017:2015 gives guidelines for information security controls applicable to cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002 and more controls with implementation guidance that specifically relate to cloud services. Google Cloud is certified as ISO 27017 compliant.

ISO 27018
The ISO 27018 is a "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors." This standard primarily focuses on security controls for public-cloud service providers acting as PII processors. GCP and G Suite are certified as ISO 27018 compliant.

SOC 2 & 3 (SSAE16 / ISAE 3402 Type II)

Service Organization Controls ("SOC") reports—SOC 2 and SOC 3—evaluate an organization's information systems and controls with respect to security, availability, processing integrity, and confidentiality or privacy based on the existing SysTrust and WebTrust principles. The Auditing Standards Board of the American Institute of Certified Public Accountants ("AICPA") created the Statement on Standards for Attestation Engagements No. 16 ("SSAE 16"), which aligns closely with the International Standard on Assurance Engagements 3402 ("ISAE 3402"). SSAE 16 and ISAE 3402 are used to generate a report by an objective third-party attesting to a set of statements which an organization asserts about its controls. Google Cloud undergoes a regular third-party audit to certify individual products against the SOC 2 and SOC 3 standards.

Internal Audit & Compliance Team

Google has a dedicated internal audit team that reviews compliance with security laws and regulations around the world. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties. For more information, refer to the Internal audit and compliance specialist section in the Google Security Whitepaper.

Google contractually commits to the following:

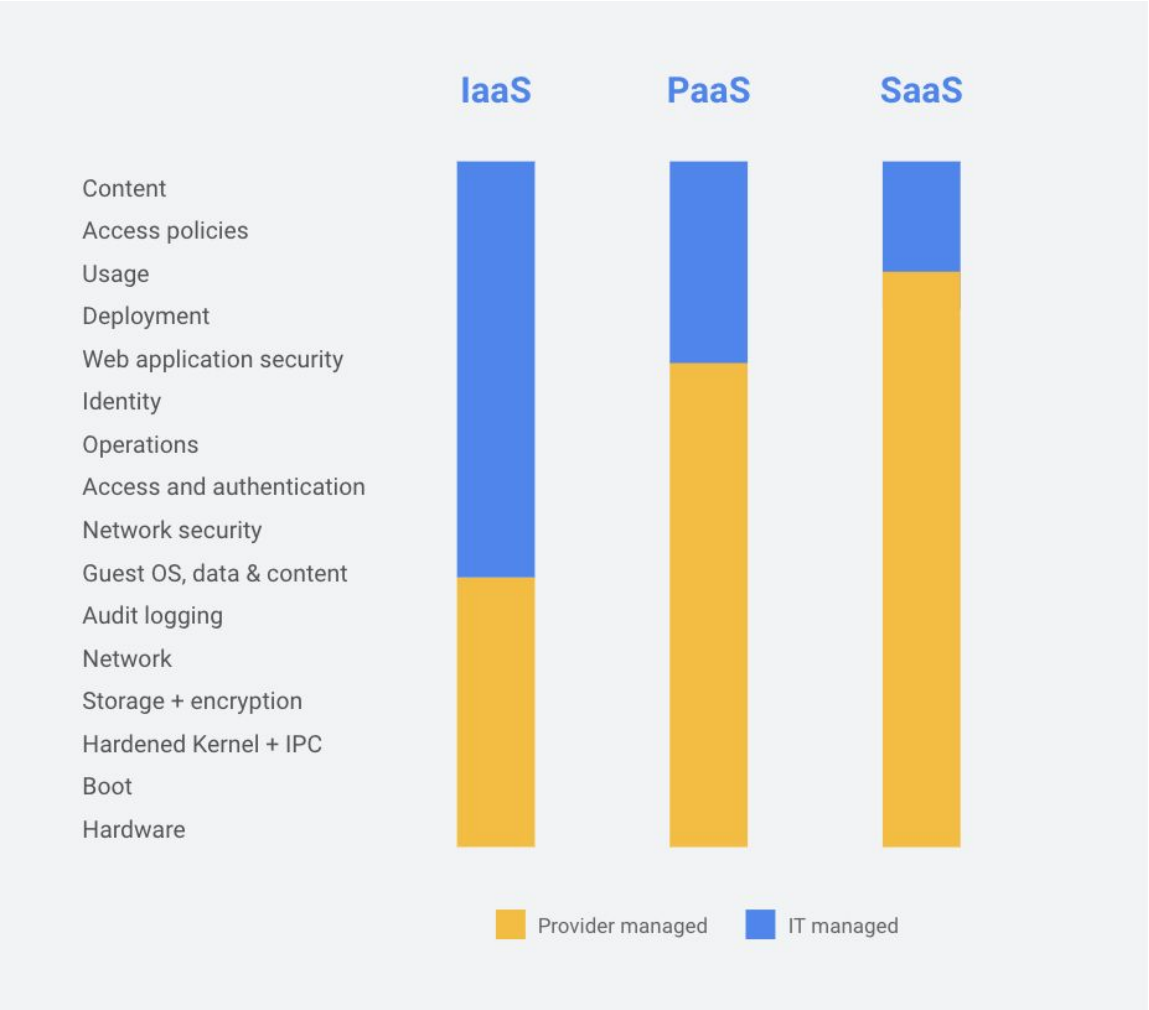
- Google will maintain adherence to ISO 27001, ISO 27017, ISO 27018, and SOC 2/3 audits during the term of the agreement;
- Google will define how data is processed, stored, and protected through specific defined security standards;
- Customers may contact Google's Data Privacy Officer for questions or comments;
- Administrators can export customer data in standard formats at any time during the term of the agreement and do so free of charge.

The Shared Responsibility Model

Under the Shared Responsibility Model, the cloud customer and its cloud service provider (CSP) share the responsibilities of managing the IT environment, including those related to security and compliance. As a trusted partner, Google Cloud's role in this model includes providing services on a highly secure and controlled platform and offering a wide array of security features from which customers can benefit. Shared responsibility enables our customers to allocate resources more effectively to their core competencies and concentrate on what they do best. Although the Shared Responsibility Model does not remove the accountability and risk from customers using Google Cloud services, we help by operating and controlling system components and physical control of facilities. The figure below visually demonstrates an example of the Shared Responsibility Model across

Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) offerings. Keep in mind that responsibilities will vary depending on the specific services being used.

For more information on Google Cloud product and security configurations, customers should reference the applicable product documentation.



How Google Cloud Supports Financial Institutions in Satisfying the FFIEC's IT Examination Procedures

In this section, we provide access to a resource in which we map Google Cloud's comprehensive information security and risk management capabilities to the most relevant FFIEC Examination Procedures in the OTS and IS Booklets. In addition, we help our customers by providing services on a secure and controlled platform and by offering a wide array of security products that can assist them with fulfilling the FFIEC IT Examination Handbook guidance.

Mapping Our Capabilities to the FFIEC IT Handbook Exam Procedures

The FFIEC advises FIs to have internal mechanisms and controls in place to properly manage outsourcing arrangements and to establish appropriate information security processes. Implementing the recommendations of the guidelines is primarily the responsibility of each individual FI. The table below lists some of the key requirements of the OTS and IS Booklets' Examination Procedures, which serve as models for federal examiners in their evaluations of FIs. In the table, we identify Google's and our FI customers' respective responsibilities. We also highlight where Google Cloud can support our customers in meeting the exam objectives, even if we are not the responsible party. FIs should not consider the exam procedures listed below as exhaustive. FIs should, as always, perform due diligence to ensure they cover all of the FFIEC standards and principles, as well as any other applicable financial-related laws.

For more information about how Google Cloud's information security features help our FI customers satisfy the OTS and IT Booklets' guidelines, refer to the FFIEC IT Examination Procedures & Shared Responsibility Workbook.

Disclaimer

The Workbook is for informational purposes only and does not constitute legal advice. It is intended to assist customers understand our shared responsibilities under the FFIEC's regulatory guidance. The Workbook does not cover the entire IT Handbook; nor does it address applicable laws and regulations. FIs ultimately bear responsibility for satisfying any legal requirements and the regulator's examination criteria.

Google Cloud Products to Help Fulfill the FFIEC IT Handbook Standards

Google Cloud delivers a range of product offerings to help our financial services customers meet the regulatory standards as prescribed in the FFIEC IT Examination handbook. We list some of the relevant Google Cloud products and services in the tables below. Please refer here for more information on our controls mapping for FFIEC regulatory requirements.

GCP

Category	Offering	Description
Governance	Cloud Console	GCP's integrated management console
	Cloud Console Mobile App	Manage GCP services from your Android or iOS device
	Cloud Deployment Manager	Manage cloud resources with simple templates
	Cloud Endpoints	Develop, deploy, and manage APIs on any Google Cloud backend
	Cloud Shell	Manage infrastructure and applications from the command-line in any browser
	Stackdriver	Monitoring and management for services, containers, applications, and infrastructure
	Stackdriver Monitoring	Provides visibility into the performance, uptime, and overall health of applications running on GCP and AWS
Identity & Access Management	Cloud IAM	Fine-grained identity and access management
	Cloud Identity	Easily manage user identities, devices, and applications from one console
	Cloud Identity-Aware Proxy	Use identity to guard access
	Cloud Resource Manager	Hierarchically manage resources on GCP
	Firebase Authentication	Simple multi-platform sign-in
	Security Keys	Prevent phishing with security keys
Data Security	Cloud Data Loss Prevention API	Discover and redact sensitive data
	Cloud Hardware Security Module (HSM)	Protect your cryptographic keys in a fully managed cloud-hosted HSM service
	Cloud Key Management Service (KMS)	Manage encryption keys on GCP
	Encryption at Rest	Encryption at rest by default

Category	Offering	Description
Data Security (continued)	Encryption in Transit	Default TLS encryption provided to protect data in transit between customers and Google infrastructure
Network Security	Application Layer Transport Security	Mutual authentication and transport encryption system
	Cloud Load Balancing	High performance, scalable load balancing
	Virtual Private Cloud (VPC)	Manage networking functionality for your Cloud Platform resources
	VPC Service Controls	Define secure access zones for sensitive data in GCP services
Infrastructure Security	Binary Authorization	Deploy only trusted containers on Kubernetes Engine
	Container Security	Secure your container environment on GCP
	Shielded VMs	Hardened virtual machines on GCP
Application Security	Apigee	Design, secure, analyze, and scale APIs anywhere.
	Cloud Security Scanner	Automatically scan your App Engine apps
Security Monitoring & Operations	Access Transparency	Expand visibility over your cloud provider through near real-time logs
	Cloud Security Command Center	A comprehensive security and data risk platform for GCP
	Stackdriver Logging	Store, search, analyse, monitor, and alert on log data

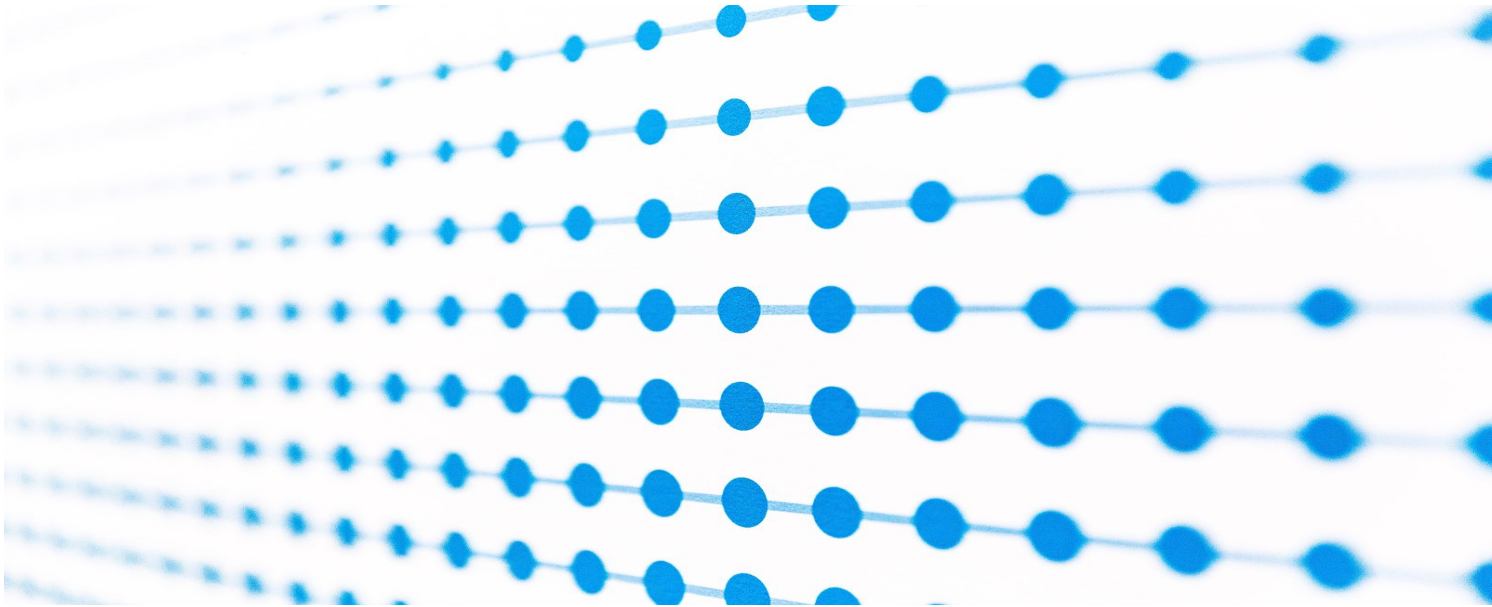
G Suite

Category	Offering	Description
Governance	Admin Console	Manage G Suite for your organization
	Mobile Management	Mobile management for Android, iOS, Windows, and more
	Vault	Archiving and eDiscovery for email, files, and chat
Identity & Access Management	Centralized Cloud Access Management	G Suite enables unified access to other enterprise cloud applications; our identity and access management (IAM) service lets administrators manage all user credentials and cloud applications access in one place

	G Suite Doc Controls	Control file-sharing permissions for your organization's Google Drive files and folders
Data Security	2048-Bit Encryption Keys	G Suite uses an RSA encryption key length of 2048 bits and changes them every few weeks
	G Suite DLP Drive	Use Data Loss Prevention (DLP) rules to scan files for sensitive content in Google Drive
	G Suite DLP Mail	Use DLP rules to scan inbound and outbound email for sensitive information
	Email Encryption	Every single email message sent and received is encrypted while moving between Google's data centers
Security Monitoring & Operations	Suspicious Login Monitoring	We use robust machine learning to help detect suspicious logins; when suspicious logins are detected, administrators are notified so they can work to ensure the accounts are secured

Conclusion

Google Cloud customers looking to use GCP and G Suite in a compliant manner with the FFIEC's "Outsourced Cloud Computing" guidelines may leverage this document as well as the FFIEC IT Examination Procedures & Shared Responsibility Workbook. We encourage our customers to review the other IT Handbook Booklets and to utilize the FFIEC's Cybersecurity Assessment Tool to help determine their risks and cybersecurity readiness.



Additional Resources

As you continue on your journey to build FFIEC IT Examination Handbook compliant applications or environments, we invite you to take advantage of the resources listed below.

Learn More

	GCP	G Suite
Learn Why Other Organizations are Choosing Google Cloud	Why Google Cloud?	Why G Suite
Learn More About Our Services	Google Cloud Solutions	G Suite Learning Center
Learn More About Our Pricing	Google Cloud Pricing	G Suite Solution

Engage

	GCP	G Suite
Try Google Cloud For Free	GCP Free Tier	G Suite Free Trial
Call Our Knowledge Center	844-613-7589	855-312-7191
Have Questions Regarding Security, Privacy or Compliance?	Contact Google Cloud Support Center or your specified Account Manager	

Act

	GCP	G Suite
Get Google On Your Team	Fill out this form or call 844-613-7589	Fill out this form or call 855-312-7191
Train Your Team	Google Cloud Training	G Suite Training
Quickstarts - *Deploy your first solution in 10 minutes or less*	Getting Started With GCP	G Suite Quick Start Guide

Get Support

	GCP	G Suite
Frequently Asked Questions	GCP FAQs	G Suite FAQs
Customer Technical Support	Contact our Google Cloud Support Center	