Google Cloud Whitepaper
January 2023

Cloud best practices for Singapore financial institutions

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of January 2023 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

Singapore is a global tech epicenter, topping the 2017 Global Smart City Performance Index, which ranks urban environments on their integration of digital technology in mobility, public safety, health and productivity. Cloud computing is a critical contributor to Singapore's digital success. Due to government encouragement and regulatory support, the city-state is a regional leader in cloud computing. The Asia Cloud Computing Association ranked Singapore first in its 2018 Cloud Readiness Index. Similarly, the 2018 BSA Global Cloud Computing Scorecard ranked Singapore sixth out of 24 leading IT economies for its cloud computing preparedness based on its legal and regulatory environment, including its data protection regime. Following this trend, financial institutions ("FIs") in Singapore are also increasingly moving toward adopting cloud computing. Nonetheless, before migrating to the cloud, FIs in Singapore must consider their responsibilities associated with the city-state's specific regulatory requirements, as outlined by the Monetary Authority of Singapore ("MAS"), the city-state's central bank and financial regulatory authority.

While MAS permits FIs to use cloud computing services, it considers it to be a form of outsourcing. MAS advises FIs to perform due diligence and risk assessments on the cloud service providers ("CSPs") that they engage with. It also recommends that FIs establish governance frameworks and implement appropriate processes and controls to mitigate risks associated with such outsourcing in accordance with the MAS's Guidelines on Outsourcing ("MAS Guidelines"). In addition, the Association of Banks in Singapore ("ABS"), an industry association that represents the interests of the commercial and investment banking community within the city-state, provides practical steps for FIs wanting to leverage cloud computing technology. The ABS Cloud Computing Implementation Guide 2.0 ("the ABS Guide") contains best practice recommendations and considerations to support FIs' safe adoption of cloud.

With this whitepaper, Google aims to help its FI customers navigate the MAS Guidelines and the ABS Guide. In this paper we describe the standards recommended by MAS and ABS, provide an overview of Google's approach to information security and risk management, and the security responsibilities we share with our customers. We also discuss how Google Cloud supports its FI customers in the overall outsourcing process.

Overview of the MAS and the ABS Guidelines

It is important to note that these guidelines are not exhaustive of FIs' responsibilities and obligations. Customers should always perform due diligence to ensure that they meet all of the applicable legal requirements in Singapore. We also provide information about Singapore's laws and regulations concerning data protection and privacy in our Singapore Personal Data Protection Act whitepaper.

MAS Guidelines on Outsourcing

MAS Guidelines recognize cloud services as a form of outsourcing and direct FIs on how to adopt and govern such relationships. To learn more, refer to the MAS's guidelines on Operational Risk and Technology Risk.

Although the MAS Guidelines are not legally binding, the MAS expects FIs to follow the recommended practices when using outsourced services, particularly the arrangements that the MAS deems as "material."[1] FIs are ultimately responsible and accountable for managing their cloud services, and are subject to the MAS' oversight. In this section, we identify the most relevant risk management practices that MAS expects FIs to implement. Later in the paper, we present a table with more details on MAS best practices.

[1] Annex 2 of the MAS Guidelines. (2018, October). Retrieved from http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016%20revised%20on%205%20Oct%202018.pdf

ABS cloud implementation guide

One of ABS's primary roles is to work with its member banks and institutions to develop and deploy "industry guidelines that are in line with international best practices." Within this whitepaper, we discuss the ABS Guide, which provides FIs guidelines on due diligence reviews, vendor management, and key controls to implement when using CSPs. While the ABS Guide is not binding, FIs should follow its recommendations to ensure that they and their CSPs satisfy industry expectations, namely, having the appropriate baseline standard of controls and processes. To learn more about the ABS's other related guidelines, refer to its Guidelines for Outsourced Providers and Penetration Testing Guidelines.

The ABS Guide has four sections. The first section introduces cloud service and deployment models, and defines key terms. The second section describes "material" and "non-material" cloud outsourcing arrangements. The third section recommends due diligence and vendor management practices for such arrangements. The fourth section sets forth baseline controls CSPs should implement when engaging with FIs. We cover the latter three sections.

Overview of Google Cloud security, compliance, and the shared responsibility model

GCP and G Suite offer industry-leading infrastructure with comprehensive controls that can help our FI customers meet their objectives and satisfy the MAS Guidelines and ABS Guide requirements. Under the shared responsibility model, Google Cloud and our FI customers share the management of the IT environment, including responsibilities for security. We work with our customers to delineate these responsibilities in an effective and transparent way.

In this section, we discuss Google Cloud's comprehensive information security, data protection, and risk management processes, as well as the shared responsibility model.

Google Cloud's approach to security and data protection

Google's focus on security and protection of information is among our primary design criteria. Security is at the core of everything we do; it is embedded in our culture and our architecture and we focus on improving it every day. In this section, we provide an overview of the organizational and technical controls we use to protect your data. To learn more about our approach to security and compliance, refer to the Google security whitepaper for GCP and the Google Cloud security and compliance whitepaper for G Suite.

Data Usage Philosophy & Customer Control

Google Cloud customers own their data, not Google. We fully respect that the data organizations and users put into Google Cloud's systems belongs to them, and we process our customers' data solely in accordance with our customer contracts. To learn more, refer to the Cloud Data Processing Addendum. Also refer to our Data deletion whitepaper for more details.

Data Trust Principles

We want our customers to feel confident that taking advantage of Google Cloud products does not require them to compromise on security or control of their data, and believe that trust is created through transparency. To learn more about our commitment to safeguarding customer data, refer to Google Cloud Privacy and our employee Code of Conduct.

Strong Security Culture

Security is central to Google culture. It is integral to our employee background checks, employee security training, and company-wide events to raise awareness and drive innovation in security and privacy. To learn more, refer to the security culture section of the Google security whitepaper.

Security Team

Google employs several hundreds of security and privacy professionals, including some of the world's foremost experts in the domain. This team maintains the company's defence systems, develops security review processes, builds security infrastructure, implements Google's security policies, and actively scans for security threats. For more information, refer to the security team, vulnerability management and monitoring sections of the Google security whitepaper.

Trusted Infrastructure

We conceived, designed, and built Google Cloud to operate securely. It runs on the same Google infrastructure that supports multiple of Google's own billion user applications. To learn more, refer to the Google Infrastructure Security Design Overview, as well as the Cloud Data Processing Addendum.

Data Encryption

Google supports various encryption protocols and ciphers to protect data in transit between the customer and Google and within Google's infrastructure. For more information, check out the Encryption in transit Google Cloud whitepaper.

In addition, Google Cloud encrypts customer content stored at rest by default, using one or more encryption mechanisms. For more information, refer to the G Suite encryption whitepaper and Google Cloud Platform encryption at rest whitepaper.

Restricted Access to Customer Data

To keep data private and secure, only a limited group of Google employees have access to customer data, and access rights and levels are based on job function and role. To learn about how customers can view Google's access to their data, refer to Access Transparency product page.

State-of-the-Art Data Centre Security

Google data centre physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data centre floor features laser beam intrusion detection. Our data centres are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. To learn more, refer to Google Data Centers.

Vulnerability Management & Threat Monitoring

We administer a vulnerability management process that actively scans for security threats. In addition, our security monitoring program gathers information from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities.

Data Segregation and Protection for Multi-Tenancy Environments

To prevent unauthorized access by other tenants sharing the same physical server, we logically isolate our customers' data. To learn more about our logical isolation, refer to the Administrative Access section of the Google security whitepaper.

Incident Response Plans and Breach Notification

We have a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. The Google security team operates 24/7, and 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.

Business Continuity Plans

At Google Cloud, we plan on our services being always available, even when we are upgrading or maintaining our systems. We achieve better than 99% reliability through operating world class infrastructure that is designed with system redundancy and security at the core to keep services running 24/7/365. For more information, refer to our GCP SLAs and G Suite SLA.

Business Continuity Plans can be invoked in any of the following incidents / event types. The following list is not comprehensive but representative of the sorts of incidents / events Google is planning for:

- Natural Disaster - Such as an earthquake, flood, tornado, hurricane, wildfire, etc.
- Data Centre Emergency - Outages affecting the availability of DC availability or access to common infrastructure.
- Executive Threat - An event that threatens the safety of an executive at Google
- Active Shooter - Individual(s) who are attempting to harm people with a firearm, typically in a confined and populated area
- Pandemic - An outbreak of a regional or global disease that impacts Google

Technology

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. To learn more about our security technologies, refer to our security products & capabilities page.

Our Data Protection Terms and Conditions

The Cloud Data Processing Addendum supplement the Cloud Terms of Service and describe our commitment to protecting customer data.

Google Cloud's approach to compliance

Industry Certifications & Independent Third-party Audits and Attestations

Google Cloud offerings 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. For more information, refer to our compliance resource center.

With respect to the financial services sector and the Asia-Pacific region, we adhere to the following relevant standards and have the following certifications:

MTCS Standard 584 Tier 3 (Cloud Security)

The Multi-Tier Cloud Security (MTCS) Singapore Standard 584 is a cloud security certification managed by the Singapore Info-communications Media Development Authority. The standard has three tiers designed to certify cloud service providers at different levels of operational security, with Tier 3 having the most stringent requirements. In obtaining the MTCS certification, a cloud service provider must complete a self-disclosure form that details its level of security and covers, among other things, data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery, as well as incident and problem management. Google Cloud has obtained Tier 3 certification, the highest level. For a full list of our products and services that are MTCS Tier 3 certified, refer to our MTCS webpage. To understand our security and privacy infrastructure assurances, refer to Google's MTCS self-disclosure form.

ISO 27001 (Information Security Management)

The International Organization for Standardization 27001 (ISO 27001) is one of the most widely recognized, internationally accepted security standards; it outlines and provides the requirements for an information security management system (ISMS). The ISO 27001 lays out a framework and checklist of controls that allows Google to ensure a comprehensive and continually improving model for security management. GCP and G Suite are certified as ISO 27001 compliant.

ISO 27017 (Cloud Security)

The International Organization for Standardization 27017 (ISO/IEC 27017:2015) gives guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidelines for relevant controls specified in ISO/IEC 27002 and more controls with implementation guidelines that specifically relate to cloud services. This standard provides controls and implementation guidelines for both cloud service providers (like Google) and our cloud service customers. GCP and G Suite are certified as ISO 27017 compliant.

ISO 27018 (Cloud Privacy)

The International Organization for Standardization 27018 (ISO 27018) is an international standard of practice for protection of personally identifiable information (PII) in Public Clouds Services. 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.

SSAE 18 / ISAE 3402 (SOC 1, SOC 2, and SOC 3)

The Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) created the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) to keep pace with globally recognized international accounting standards. Notably, SSAE 18 aligns closely with the International Standard on Assurance Engagements 3402 (ISAE 3402). In addition, SSAE 18 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. The Service Organization Controls (SOC) framework is the method by which the control of financial information is measured. A SOC 1 report documents a service organization's controls that may be relevant to financial reporting. A SOC 2 report is based on the AICPA's existing Trust Services principles and criteria, and provides an evaluation of an organization's information systems relevant to security, availability, processing integrity, and confidentiality. A SOC 3 report is based on existing SysTrust and WebTrust principles. Google has SOC 1, SOC 2, and SOC 3 reports for Google Cloud Platform and G Suite.

PCI DSS

Established by the major credit card associations, the PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. To better protect cardholder data, the PCI Security Standards Council created the Payment Card Industry (PCI) Data Security Standards (DSS) as a set of network security and business best practice guidelines that establish a "minimum security standard" to protect customers' payment card information. Google Cloud undergoes an annual third-party audit to certify individual products against the PCI DSS. This means that these services provide an infrastructure upon which customers may build their own services or applications that store, process, or transmit cardholder data. For a list of GCP services that are PCI DSS 3.2 compliant, refer to our PCI DSS compliance page.

FedRAMP

Established by the U.S. Federal Government, Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Google maintains a FedRAMP Moderate authorization to operate (ATO) for Google Cloud Platform and G Suite. Our FedRAMP status is also posted on the government's website: FedRAMP Marketplace. FedRAMP is used by many institutions globally to evaluate the robustness of their IT and application security posture. The controls prescribed by FedRAMP are used in this document to show how Google Cloud helps our customers meet the guidelines of the MAS and ABS.

Security & Regulatory Compliance Specialists

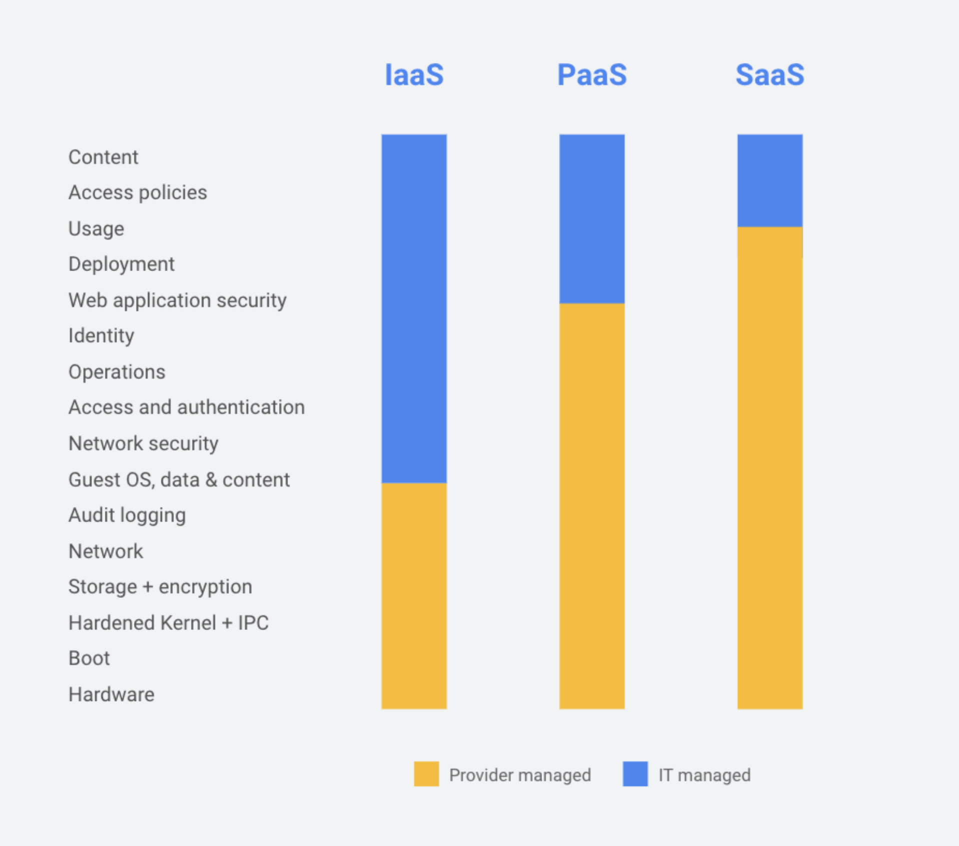
Google Cloud has a dedicated compliance team that reviews compliance with security laws and regulations around the world. As new frameworks are created, the Compliance team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties. In addition, Google contractually commits to the following:

- We will maintain adherence to ISO 27001, ISO 27017, ISO 27018 and SOC 2 and SOC 3 audits during the term of the agreement.
- We will define how data is protected through specific defined security standards.
- Customers may contact Google's Cloud Data Protection Team for questions or comments.

The Google Cloud shared responsibility model

Under our shared Responsibility Model, the cloud customer and its 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. The shared responsibility model does not remove the accountability and risk from customers using Google Cloud services, but it does help relieve the burden as we manage and control system components and physical control of facilities. It also shifts a portion of the cost of security and compliance onto Google Cloud and away from our customers. The figure below visually demonstrates an example of the shared responsibility model across on-prem, 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 helps FIs meet the MAS and ABS guidelines

In this section, we break down the MAS Guidelines' recommended standards and the ABS Guide's suggested baseline controls into separate tables to identify the party responsible for meeting the criteria, whether the FI or Google Cloud, pursuant to the Shared Responsibility model.

How we support FIs in meeting the MAS Guidelines' recommendations

A mapping on how Google can support customers in meeting the MAS Guidelines can be found here. In the table, we provide a description of each MAS control objective followed by Google's supporting controls. Although FIs bear the responsibility for implementing the MAS Guidelines with respect to managing outsourcing risks, the information in the table can be leveraged by the institutions as part of their ongoing due diligence.

How our controls align to the ABS guide's recommended controls

This table lists the key controls recommended by the ABS when entering into a cloud outsourcing arrangement. The table provides a brief description of each control's objectives, and identifies Google Cloud's corresponding supporting controls. Like with the MAS Guidelines, customers remain responsible for ensuring compliance with the recommendations as they consider moving workloads to the cloud. Customers may use the information contained in the table to assist in their assessment of Google Cloud as a cloud service provider.

Conclusion

FIs operating in Singapore should follow the MAS Guidelines on Outsourcing and the ABS Cloud Computing Implementation Guide 1.1 to ensure that their outsourced cloud computing arrangements meet the regulatory and financial industry expectations. Doing so will help FIs better safeguard their customer information. As a trusted partner and global leader in cloud computing services, Google Cloud is committed to working with our FI customers to fulfill their strategic objectives while satisfying regulatory guidelines.