accenture | Google Cloud

Security Framework for Financial Services

Executive Summary

Table of Contents

Table of Figures

Background:

This is a technical whitepaper, joint-published between Accenture and Google, that describes best practices, general recommendations, and security considerations that Financial Institutions should reflect on when using (or looking to migrate to) Google Cloud. This paper is not an implementation guide and should not be used as a prescriptive architecture for financial institutions.

Disclaimer:

This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors. This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement, or approval of this content by the owners of such marks is intended, expressed, or implied.

The content contained in this document is correct as of January 2023. This technical paper represents the status quo as of the time it was written. Google Cloud's products, security policies, and systems might change going forward as Google continually improves protection mechanisms.

This reference framework is for informational purposes only. Accenture does not intend the information or recommendations in this guide to constitute as definitive configuration advice. Each organization is responsible for independently evaluating their own particular use of the services as appropriate to support its legal, compliance, security, and functional obligations.

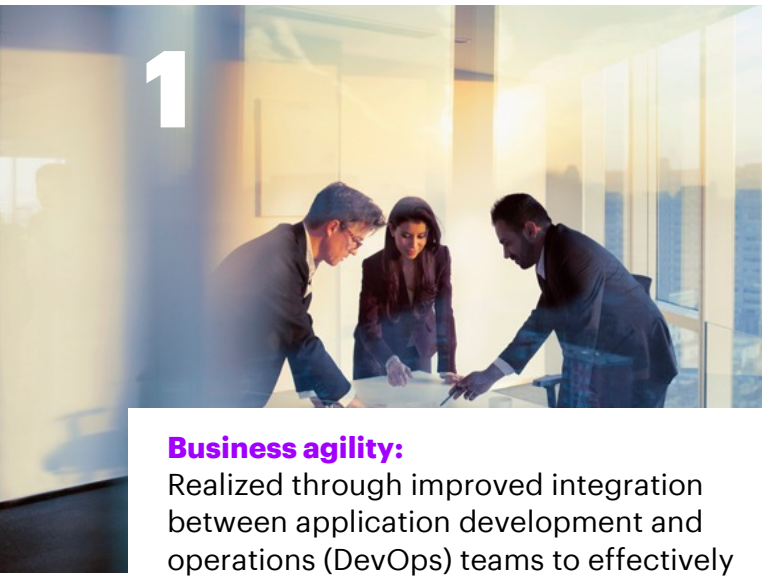
Section 1

Introduction

Introduction

The journey to cloud for financial institutions (FIs) starts with the same goal as other industries transitioning to the cloud: increase developer velocity and scalability while accelerating time to value for the end customers.

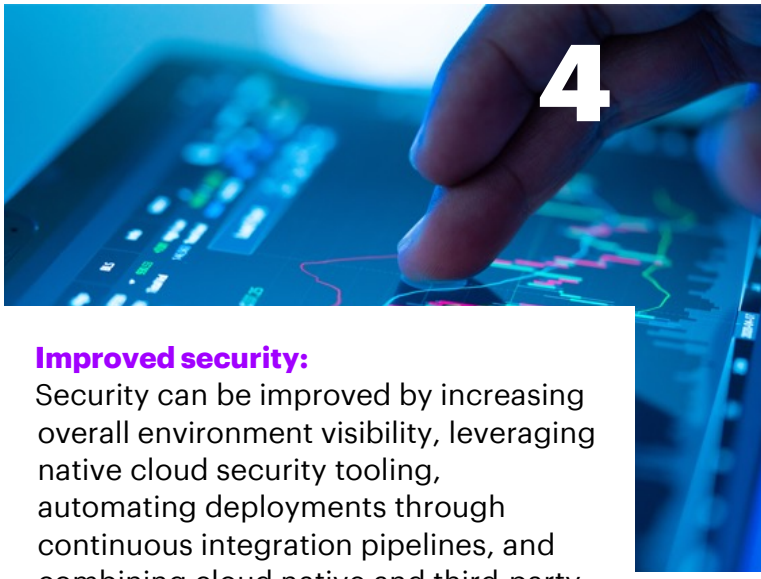
Cloud and virtualization technologies introduce several benefits to banking and financial services organizations. The adoption of these technologies allows for (but is not limited to):



Business agility:
Realized through improved integration between application development and operations (DevOps) teams to effectively identify and correct/iterate on issues.

Increased efficiency and resiliency:
Accomplished through near-instant deployments of virtualized or containerized systems (as dictated by business growth or client engagement).

Reduced operating costs:
Exemplified by the ability to scale cloud workloads (elasticity) in response to business demands. This is contrasted by the traditional datacenter environment, where companies deploy mostly under-utilized systems at significantly higher capital expenditure cost.



Improved security:
Security can be improved by increasing overall environment visibility, leveraging native cloud security tooling, automating deployments through continuous integration pipelines, and combining cloud native and third-party technologies.

While the rewards of transitioning to the cloud are appealing, there can be inherent risk – and due to the sensitive and high-value nature of the data FIs commonly process and exchange, it is critical that any significant change to the IT infrastructure is secure by design. Aside from the transaction data itself, individual client data in the form of personally identifiable information (PII) as well as sensitive and proprietary records must be protected. Moreover, to ensure that strong security controls are properly configured and privacy by design frameworks are applied – regulatory bodies mandate numerous requirements, recurring audits, and certifications of compliancy.

There are constant threats in the form of cyber-attacks that target cloud infrastructure and navigating the shared responsibility model can add an extra level of complexity. In addition, there are a collection of elements (for example, security control configuration, regulatory compliancy, protection against cyber-attacks, and navigating the shared responsibility model) that often makes transitioning to the cloud a daunting and tumultuous process for FIs.

One of the most perennial threats to FIs is the exfiltration (or inadvertent exposure) of data to malicious or unapproved actors or systems. Data exfiltration is a security breach that involves sensitive, proprietary, or secure information that carries a significant material loss to a person, system, or organization. Although organizations are generally improving in the area of detecting unauthorized access attempts, data breaches are ever evolving; the average total cost of a data breach in 2020 was $3.86 million[1] – accentuating the importance of strong data exfiltration controls in a cloud environment.

An additional concern for FIs is successfully integrating and deploying security monitoring controls. A 2020 Data Breach Report from IBM indicated that the average time to detect a network breach is roughly 280 days.[2] Without insights into the activity in a cloud environment – the overall attack surface is vastly expanded.

This technical paper attempts to address the collection of security concerns by providing a comprehensive preventative and detective reference framework that indicates how FIs can secure their Google Cloud environment.

The paper begins by providing an overview of the Banking and Financial Services sector and outlines current trends in the industry. Then, before discussing the reference framework itself, the paper describes the methodology for producing the reference framework. The reference framework builds off the December 2022 Google Security Foundations Guide sample architecture and includes specific considerations that need to be taken for Google Cloud services that either store or use sensitive data.

Important: The full version of this paper contains a comprehensive preventative and detective reference framework and control mappings to compliance requirements that are not included in this (Executive Summary) version of the paper. If you are interested in receiving the full technical paper, please refer to the **Contact Us** section located in Section 4.

accenture | Google Cloud

Section 2

Financial Services Sector Overview

Financial Services Sector Overview

In the outmoded model, FIs relied on traditional IT infrastructure and legacy systems to meet their technological demands. However, an increasing number of banks have been transitioning to the cloud to meet regulatory demands for increased transparency, to achieve higher capital requirements, and garner faster growth and higher margins. By shifting to the cloud, companies are reshaping their operating models, advancing their products and services, and improving the overall customer experience. To position themselves to remain competitive (and to transition effectively to the cloud) FIs should perform the following activities:

Transform operating, delivery, and governance models to include their cloud landscape.

Address regulatory compliance requirements.

Embed proper security controls.

Develop a functioning, comprehensive reference architecture that leverages a secure cloud foundation.

Establish processes for security management, including governance & risk management, security monitoring, and incident response.

By performing these activities and adopting an enterprise-wide strategy, FIs can reduce concerns surrounding cloud adoption while successfully leveraging the cloud. Aside from adoption strategies, it is equally important that security is taken into consideration as early as possible during the migration process.

To support adoption, Google Cloud offers a range of native security solutions (and supports compatibility with third-party solutions) to help FIs enable better business outcomes. Cloud native security solutioning helps companies be:

Fast:
With cloud service provider (CSP) native accelerators that enable security capabilities and controls to be deployed in minutes or hours, rather than months.

Frictionless:
With security embedded in existing solutions, business processes, and operational teams.

Scalable:
With automation and self-healing processes applied to reduce manual steps and break the resourcing model to enable organizations to scale.

Proactive:
With pre-emptive controls established to block accidental or malicious security incidents from happening in the first place.

Cost effective:
Security can be baked-in from the onset to avoid additional costs incurred from adding security in the aftermath.

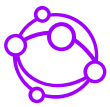
Compliant with regulatory frameworks:
Security blueprints and templates can centralize policy definitions while driving automated execution of deployments in alignment with compliance requirements.

2.1 Cloud Adoption

With many attractive incentives for cloud, the mass adoption trends are apparent. Recent trends indicate that cloud adoption rates are steadily increasing. A 2020 study of the financial services sector found that 91% of respondents are either actively using the cloud or intend to use it in the next 6 to 9 months,[3] which is double the number from the same study from 2015. This large uptick is a clear indicator of the importance of cloud for FIs. In addition, external factors, such as the COVID-19 pandemic, accelerated the demand for digital customer-bank interactions and a work-from-home employee workforce.

When looking at main reasons on why FIs are adopting the cloud, there are a few primary, influencing factors:

Compute and Container storage offering burst capacity as needed.



Data analytics and data at scale for storing and processing large amounts of data.

Usage of cloud native technologies which allows FIs to adopt shift left pipelines and utilize infrastructure as code.

2.2 Concerns and Challenges

Although many FIs are already using the cloud in some capacity (or intend to in the future), many may still be apprehensive when it comes to cloud adoption. The most common concerns include:[4]

- Technical cyber/security control gaps.
- Loss of reputation from data loss or exfiltration.
- Contractual concerns with the cloud provider.
- Meeting regulatory compliance.
- Data privacy concerns.
- Unmet requirements from internal compliance functions.

These concerns draw the question: If business demand and adoption rates for cloud are rapidly increasing, but there are looming security and compliance concerns – how can FIs securely and confidently migrate to the cloud? Section 3 describes how Google Cloud's infrastructure is an effective enabler for cloud migration, and the full version of the paper describes how to effectively configure a Google Cloud environment in a secure default state using a preventative and detective architecture.

If you are interested in receiving the full technical paper, please refer to the **Contact Us** section located in Section 4.

Section 3

Google Cloud as an Enabler for Transformation

Google Cloud as an Enabler for Transformation

Public cloud providers offer companies the ability to scale their capabilities compared to the traditional on-premise model. Moreover, public clouds offer increased security, centralized management, and a large variety of on-demand services and resources.

With Google Cloud, the catalog of offerings continues to rapidly grow, and each Google Cloud service exposes a wide range of customizable configurations and controls that enables business and security needs. Google embeds best practices in its cloud platform that provides FIs with a presence of mind when adopting the cloud; FIs can be assured that they are building on top of a reliable, secured foundation and either optimize the controls or take advantage of additional service-specific security guidance.

3.1 Shared Responsibility Model

Conventionally, security in public clouds differs intrinsically from customer-owned on-premises infrastructure. Public clouds provide a delineation of shared responsibility between the customer and the cloud provider, where customer-owned infrastructure is all self-managed.

Google Cloud's product and service offerings range from classic platform as a service (PaaS), to infrastructure as a service (IaaS), to software as a service (SaaS). At large, the boundaries of responsibility between the company and the cloud provider change based on the services that have been selected by the customer.

At a minimum, as a part of their shared responsibility for security, public cloud providers should enable companies to start with a solid, secured foundation. Providers should empower customers and make it easy for them to understand and execute their part of the shared responsibility model. With Google Cloud, there are opportunities for organizations to have a closer collaboration with Google to address security and risk. Google promotes shared fate for risk management in the cloud by providing unique tools, detailed guidance, and best practices to reduce customer risk from day one. Google also has a risk protection program that can be read about further in the Announcing the Risk Protection Program: Moving from shared responsibility to shared fate document.

As a cloud provider, the security responsibilities of Google and the security responsibilities of the FI must be clearly defined. The three types of as-a-service platforms are shown in Figure 1 below. This model identifies the areas of responsibility of FIs leveraging Google Cloud in IaaS, PaaS, and SaaS deployments.

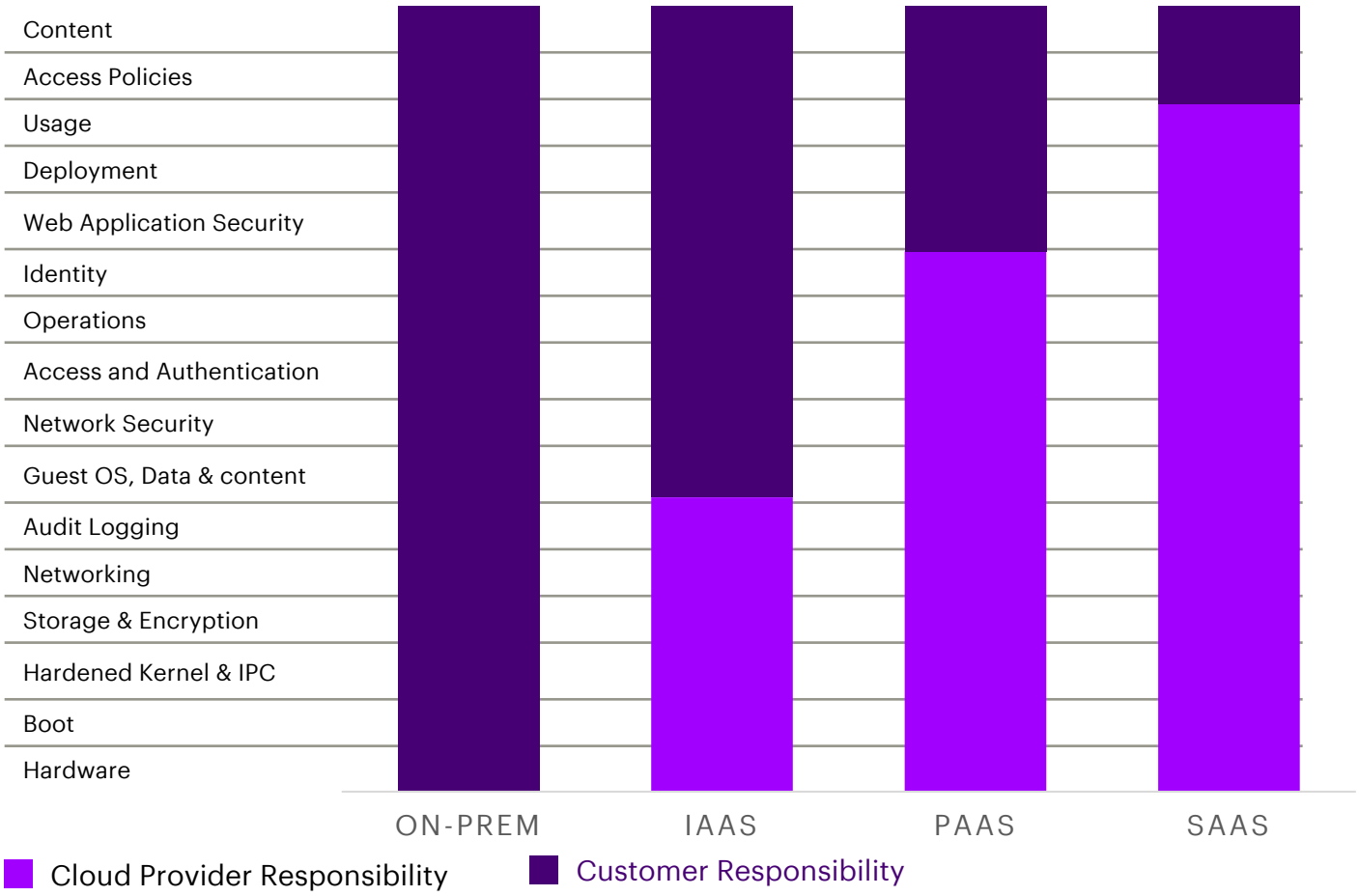


Figure 1: Shared Responsibility Model[5]

As depicted, there are clear incentives to use the offerings on the cloud as opposed to on-premises. For IaaS, PaaS, and SaaS deployments – as the responsibility decreases so too does the overhead cost. The clear delineation also helps companies understand what they are responsible for and enables a more seamless transition to the cloud.

3.2 Operational Resiliency of Google's Infrastructure

Cloud Service Providers (CSPs) work hard to secure their infrastructure and upgrade their native security features. They innovate to create and release new services at an increasingly rapid pace.

Google Cloud boasts operational resiliency in its hardware and infrastructure. Operational resiliency can be defined as the "ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard."[6]

By adopting Google Cloud, financial services firms can strengthen their operational resilience and address risks in new ways, for two key reasons:[7]

1. Google Cloud's infrastructure and operating model is of a scale and robustness that is largely commercially and technically unachievable by financial service firms.[8]

2. Google Cloud offers a wide array of differentiated solutions and capabilities.

The areas of operational resiliency span across several components. These are depicted in Figure 2, along with a few bullets that explain how Google Cloud ensures operational resiliency within these components.

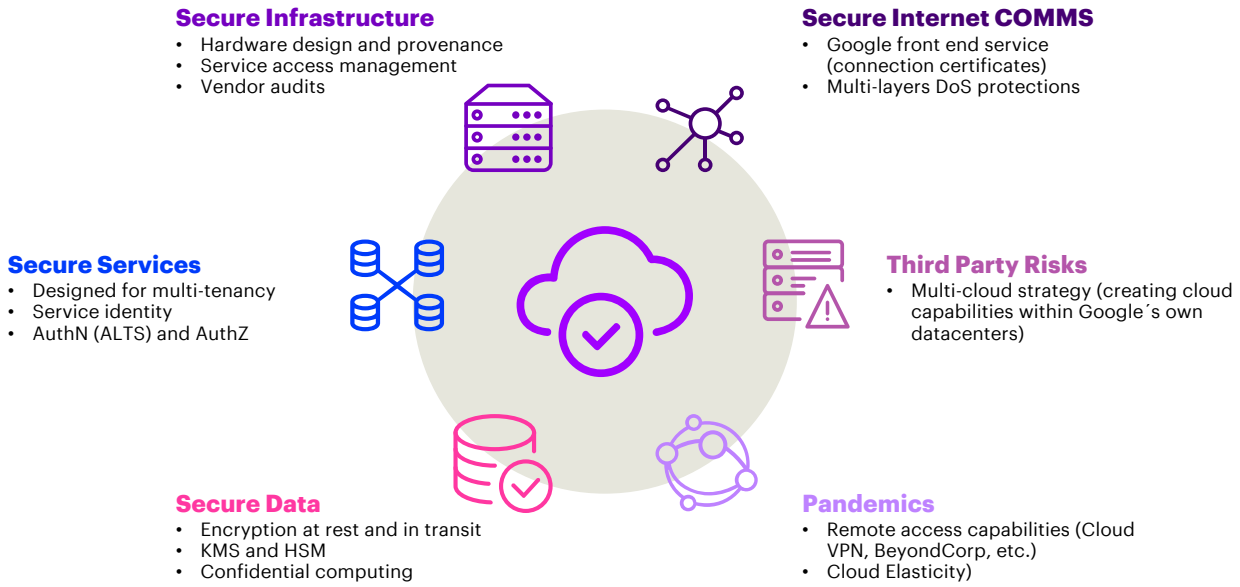


Figure 2: Components that Comprise Operational Resiliency in Google Cloud

For more information on the security of Google Cloud's infrastructure, refer to the Infrastructure design for availability and resilience whitepaper.

accenture | Google Cloud

Section 4
Contact Us

Contact Us

The full version of this paper contains a comprehensive preventative and detective reference framework and control mappings to compliance requirements that are not included in this (Executive Summary) version of the paper.

To receive the full version of the paper, or for any questions regarding the content of the paper, please reach out to the key points of contact below.

Nneka Emegwa

Managing Director; Accenture LLP
Global GCP Security Lead

Juan Elizondo

Senior Manager; Accenture LLP
US GCP Security Lead

Josh Monteiro

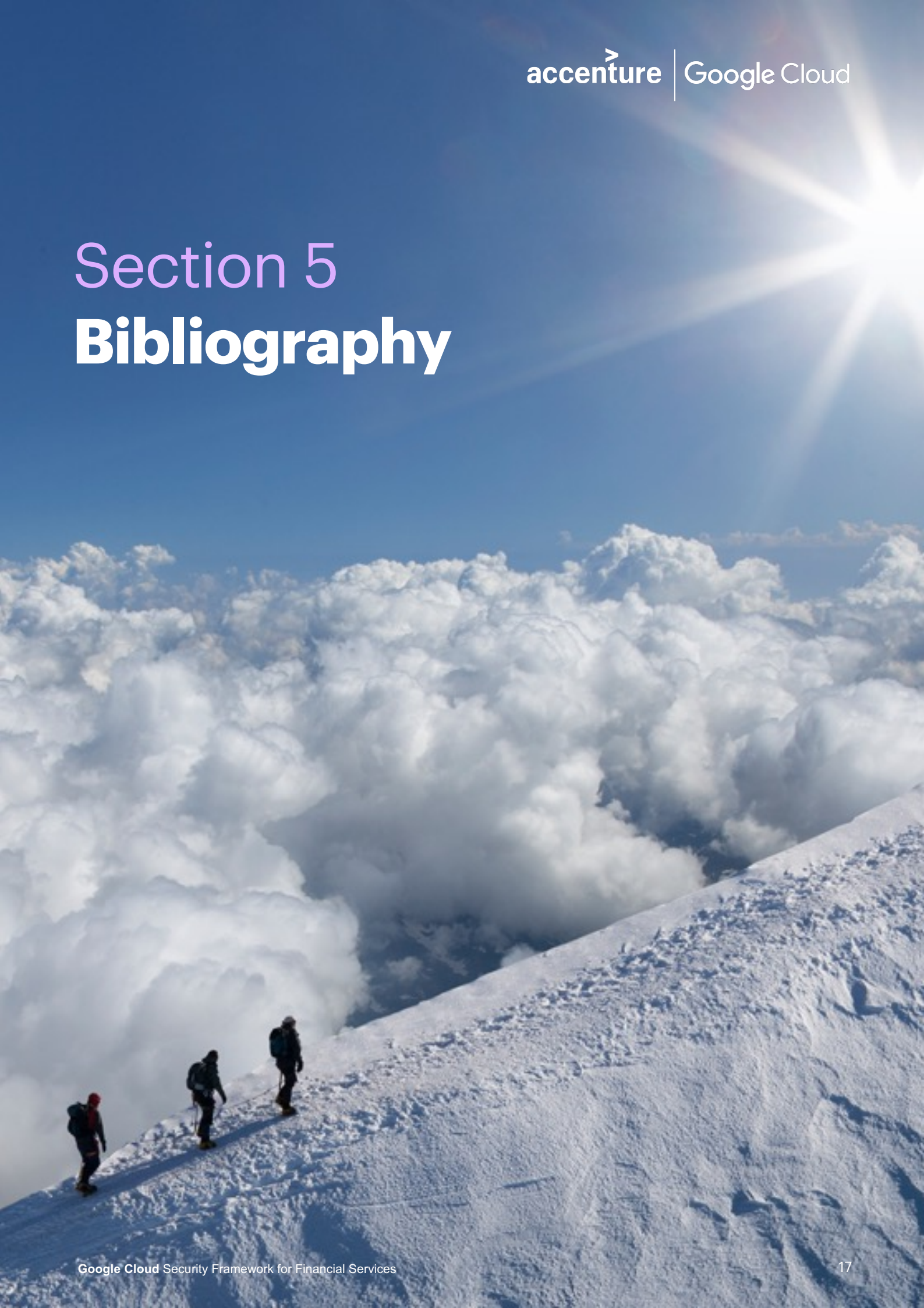
Senior Manager; Accenture LLP
Canada GCP Security Lead

Connor Herriford

Consultant; Accenture LLP
GCP Security Architecture Lead

Andy Chang

Product Manager; Google



Section 5
Bibliography

Bibliography

1 IBM Security. (2020). Cost of a Data Breach Report 2020. https://www.ibm.com/security/digital-assets/cost-data- breach-report/#/

2 Ibid.

3 Cloud Security Alliance. (2020). Cloud Usage in the Financial Services Sector.

4 Ibid.

5 Google Cloud. (2021, December). Google Cloud security foundations guide. https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

6 Sound Practices to Strengthen Operational Resilience", FRB, OCC, FDIC

7 Godfrey, N., Hannigan, D., Knott, D., & Abel, J. (2021). Strengthening Operational Resilience in Financial Services by Migrating to Google Cloud. Google Cloud. https://services.google.com/fh/files/misc/google_cloud_operational_resilience_fin_serv.pdf

8 "Third-party dependencies in cloud services", Financial Stability Board

accenture | Google Cloud

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 710,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.