Google Cloud

# Strengthening Operational Resilience in Financial Services by Migrating to Google Cloud


**Authors**: Nick Godfrey, Dave Hannigan, David Knott, John Abel

*DISCLAIMER: This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein 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.*

Office of the CISO

# Table of Contents

# Executive Summary

Operational resilience is a key area of focus for financial services firms, and could be thought of as the next goal in addressing systemic risk in the financial services sector. Regulators are also increasingly focused on this risk: it is recognised that despite many years of bolstering financial stability by enhancing financial resilience following the financial crisis, the shocks that come from the operational side can be as significant as the shocks from the financial side[1].

Operational resilience can be defined as the "ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard"[2]. Given this definition, operational resilience needs to be thought of as a desired outcome, instead of a singular activity, and as such the approach to achieving that outcome needs to address a multitude of operational risks, including cybersecurity, third party, environmental and infrastructure, and technology risks.

The rapidly evolving nature of these operational risks, the complexity of financial services technology needs, and the commercial considerations involved are increasingly making their management unachievable using technology that is owned and operated by financial institutions or delivered through traditional technology outsourcing models. Furthermore, the extent of management focus on those activities has a diluting effect on the core mission of those firms, which is to provide high-quality services at a reasonable margin, and to be able to evolve those in an agile manner.

By migrating to Google Cloud, financial services firms can leverage capabilities and solutions that are inherently better suited to managing the underlying operational risks and thus ensure the operational resilience required by their customers, shareholders and regulators.

---

[1] "Resilience and continuity in an interconnected and changing world", Lyndon Nelson, Deputy CEO, Bank of England

[2] "Sound Practices to Strengthen Operational Resilience", FRB, OCC, FDIC

# Operational Resilience

## Defining Operational Resilience

Financial services firms and regulators are increasingly focused on operational resilience, reflecting the growing dependency that financial services has on complex systems, automation and technology, and third parties.

A number of alternative definitions of operational resilience are provided by regulators including:

> *"the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions."*[3]

> *"the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions."* [4]

> *"the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality"*[5]

What is common in these definitions is the approach of seeing operational resilience as an outcome that is achieved through the effective management of risks that may prevent the ongoing operation of important functions. To that end, it is important to consider all of the risks that may prevent their ongoing operation, rather than taking a narrow approach and/or assuming that operational resilience is effectively a different term for business continuity planning.

A second area of commonality is that significant emphasis is placed on identifying what are termed critical (sometimes referred to as "important") business services. Business services can be thought of as the way in which a retail or wholesale customer of the firm would perceive the services they use (an example from retail banking is mortgage origination).

As part of establishing the levels of operational resilience that a firm requires, it will often determine what its 'failure tolerance' is for a given business service, using a range of severe but plausible scenarios. In some locales this differs definitionally from 'risk appetite' and is designed to identify the point at which specific thresholds will be crossed, for example:

- Market impacting: the point at which there is an adverse effect on the wider financial services ecosystem
- Customer impacting: the point at which significant harm is done to customers of financial services firm

[3] "Operational resilience: Impact tolerances for important business Services" Bank of England CP19/29
[4] "Sound Practices to Strengthen Operational Resilience", FRB, OCC, FDIC
[5] "Draft Regulation on digital operational resilience for the financial sector", European Commission

Defining 'failure tolerance' using these external reference points reflects regulators' intent to strengthen the operational resilience of the sector as a whole. In other words, *the point at which a firm's failure damages the market or harms customers, may be different to the ambitions a firm may have regarding operational resilience as expressed by its risk appetite.*

Why is it important that the business service, with its defined failure tolerance (or risk appetite), is the starting point for managing operational resilience? Because it ensures that the outcome is what is right for the customer, firm and industry, rather than the outcome being an expression of levels of resilience that are available with today's technology, people, facilities and third parties.

As we will cover in the following sections, whilst operational resilience is conceptually simple, defining and achieving the required levels of operational resilience, and proving it on an ongoing basis, is hard. It is also of critical importance [6].

## Operational Resilience is the Effective Management of Many Risks

Because Operational Risk is an outcome, it is important to identify the universe of operational risks that, if insufficiently managed, could compromise operational resilience. The key risks to consider are those that can disrupt the dependencies (i.e., people, technology, facilities, third parties) that underpin the firm's business services:

**Cybersecurity**
Continuously adjusting key controls, people, processes and technology to prevent, detect and react to external threats and malicious insiders

**Pandemics**
Sustaining business operations in scenarios where people cannot, or will not, work in close proximity to colleagues and customers

**Environmental and Infrastructure**
Designing and locating facilities to mitigate the effects of localised weather and infrastructure events, and to be resilient to physical attacks.

**Geopolitical**
Understanding and managing risks associated with geographic and political boundaries between intragroup and third-party dependencies

**Third-party Risk**
Managing supply chain risk, and in particular of critical outsourced functions by addressing vendor lock in, survivability and portability

**Technology Risk**
Designing Third-party and operating technology services to provide the required levels of availability, capacity, performance, quality and functionality

In subsequent sections we will examine how a migration to Google Cloud provides a path for customers to substantially improve the profile of these operational risks, and as such a mechanism for financial services firms and regulators to meet their operational resilience goals.

---

[6] "Resilience and continuity in an interconnected and changing world", Lyndon Nelson, Deputy CEO, Bank of England

# Summary of Regulator Perspectives

Global regulators increasingly recognise the importance of operational resilience, and that it can have as significant a bearing on financial stability as financial resilience (i.e., effective management of credit , market and liquidity risks). This section provides a summary of how regulators perceive this risk, and their approach to how firms should manage it. The appendix includes a **detailed overview** of some of the regulations that are in place, or emerging, around the world.

## Many Jurisdictions, but Common Themes

Google Cloud actively engages with policy makers regarding operational resilience, and related topics in numerous jurisdictions, and we welcome the approaches that are being taken. Financial services regulators in the United Kingdom[7], the European Union[8], the United States[9], and internationally[10] have all issued comprehensive guidance on operational resilience, and related topics (including outsourcing and third party risk, cybersecurity, information and communications technology, and pandemics), over the past 2 years.

As we have seen in the previous section there is significant commonality regarding the definition of operational resilience, and regarding the regulators' intentions behind it: that firms are expected to quantify their operational resilience requirements by reference to their position in the markets, and that they are expected to achieve that level of operational resilience even in the face of significant disruptions. And whilst the emphasis is on sustaining operations through any disruption, and that the responsibility for identifying risks to those operations lies squarely with the firms, most regulators provide guidance regarding the key operational risks that should be considered. For example:

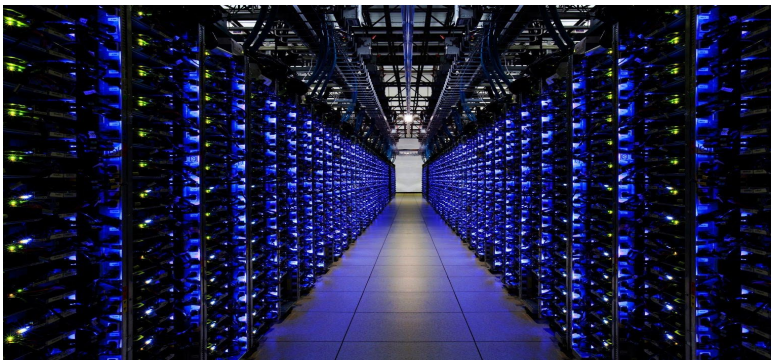
> *"In recent years, firms have experienced significant challenges from a wide range of disruptive events including **technology-based failures**, **cyber incidents**, **pandemic outbreaks**, and **natural disasters**. While advances in technology have improved firms' ability to identify and recover from various types of disruptions, increasingly sophisticated cyber threats and growing reliance on **third parties** continue to expose firms to a range of operational risks. These operational risks underscore the importance for firms of all sizes to strengthen their operational resilience."* [11]

> *"strengthen banks' ability to absorb operational risk-related events, such as **pandemic**, **cyber incidents**, **technology failures** or **natural disasters**, which could cause significant operational failures or wide-scale disruptions in financial markets"* [12]

---

[7] Bank of England, Prudential Regulation Authority, Financial Conduct Authority
[8] European Banking Authority, European Insurance & Occupational Pensions Authority, European Securities & Markets Association
[9] Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation
[10] Basel Committee on Banking Supervision, International Organisation of Securities Commissions
[11] "Sound Practices to Strengthen Operational Resilience", FRB, OCC, FDIC
[12] "Principles for operational resilience", Basel Committee on Banking Supervision

## Cloud Technologies Can Enhance Operational Resilience



There is also a growing recognition that, far from creating unnecessary new risk, a well executed migration to cloud technology over the coming years will provide capabilities to financial services that will enable them to strengthen their operational resilience in ways that are not otherwise achievable. For example:

*"Cloud service providers offer ready-made solutions that can accelerate time to market. With the benefit of their scale, they also offer leading-edge analytics, enabling businesses to learn and adjust their business models almost in real time. And they can offer greater resilience"* [13]

*"It is not necessarily a bad thing that firms are moving more stuff to the cloud. [ ... ] It may be that the cyber resilience of some cloud providers is higher than that of some individual firms"* [14]

*"One example of the potential benefits of outsourcing is evident in the use of cloud-based services or infrastructure. Based upon (....) "interactions with cloud computing experts, proponents of cloud-based infrastructures highlight several advantages:*

**Improved accessibility**
Services are accessible from a wide variety of devices and from any location with network access to the cloud.

**Cost efficiency**
Cloud provider resources are pooled to serve multiple clients, which creates economies of scale. This reduces the cost of data storage.

**Demand scalability**
The cloud provides a flexible platform that can grow and shrink to match the client's needs.

**Always-on availability**
Applications running on a cloud infrastructure are rarely offline and are accessible whenever there is an internet connection.

**Improved Security**
A key concern of a cloud provider is to carefully monitor the cloud's security, which is more efficient than security monitoring a conventional in-house system."[15]

---

[13] "New economy, new finance, new Bank" Bank of England
[14] IT failures in the Financial Services Sector, UK House of Commons Treasury Select Committee
[15] "Principles on Outsourcing", International Organisation of Securities Commissions

*"CS" (Cloud Services) "can potentially offer a number of advantages, which include economies of scale, cost-savings, access to quality system administration well as operations that adhere to uniform security standards and best practices. CS may also be used to provide the flexibility and agility for institutions to scale up or pare down on computing resources quickly as usage requirements change, without major hardware and software outlay as well as lead-time. In addition, the distributed nature of CS may enhance system resilience during location-specific disasters or disruptions"*[16]

*"From a technological perspective, large public cloud providers can often offer an IT environment that is at least as robust as the one individual FIs could create on their own premises. Economies of scale can allow cloud providers to less expensively achieve a high degree of redundancy, geographic diversity and advanced security and engineering."*[17]

Google Cloud understands the importance of this risk in maintaining the stability of the global financial system, the need for the right regulatory frameworks to manage it, and is committed to helping our customers achieve their operational resilience goals and to working with policymakers to develop associated standards. Our global platform, and the services and solutions accessible to customers provide a uniquely differentiated set of capabilities to help them manage the critical operational risks necessary to achieve operational resilience.

[16] "Guidelines on Outsourcing", Monetary Authority of Singapore
[17] "Third-party dependencies in cloud services", Financial Stability Board

# Strengthening Operational Resilience by Migrating to Google Cloud

We have established that achieving operational resilience is hard, with a multidimensional set of risks to manage, and that those risks are some of the most dynamic in the universe of risks that affect financial services. By adopting Google Cloud, financial services firms have the opportunity to strengthen their operational resilience and address these risks in new ways, for two key reasons:

- Google Cloud's infrastructure, and operating model, is of a scale and robustness that is commercially and technically largely unachievable by financial services firms.[18] Therefore, the foundations on which you build your applications and business are already significantly more resilient.
- The differentiated solutions and capabilities we provide to customers with which they can build their applications and businesses are positioned to help firms do that to a higher level of operational resilience than has been achievable previously.

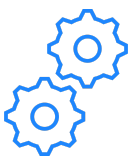
To expand on the first point, Google Cloud has made substantial investments in technical resilience over the past 20 years. It is the same technology that powers Google Search and other Google services, 6 of which serve over 1 billion users each. Cornerstones of this model include:

### Distributed Data Center

Google has 24 Regions around the world, and 73 Zones, allowing us to service customers in over 200 countries, and we continue to grow.

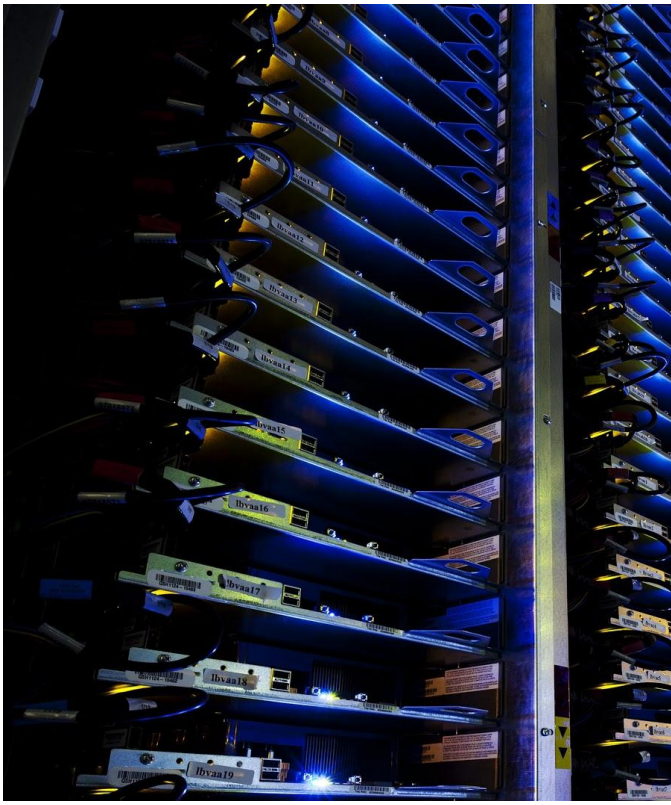
### Global Networks

Google operates one of the largest backbone networks in the world with over 130 points of presence, providing low latency and increased security.



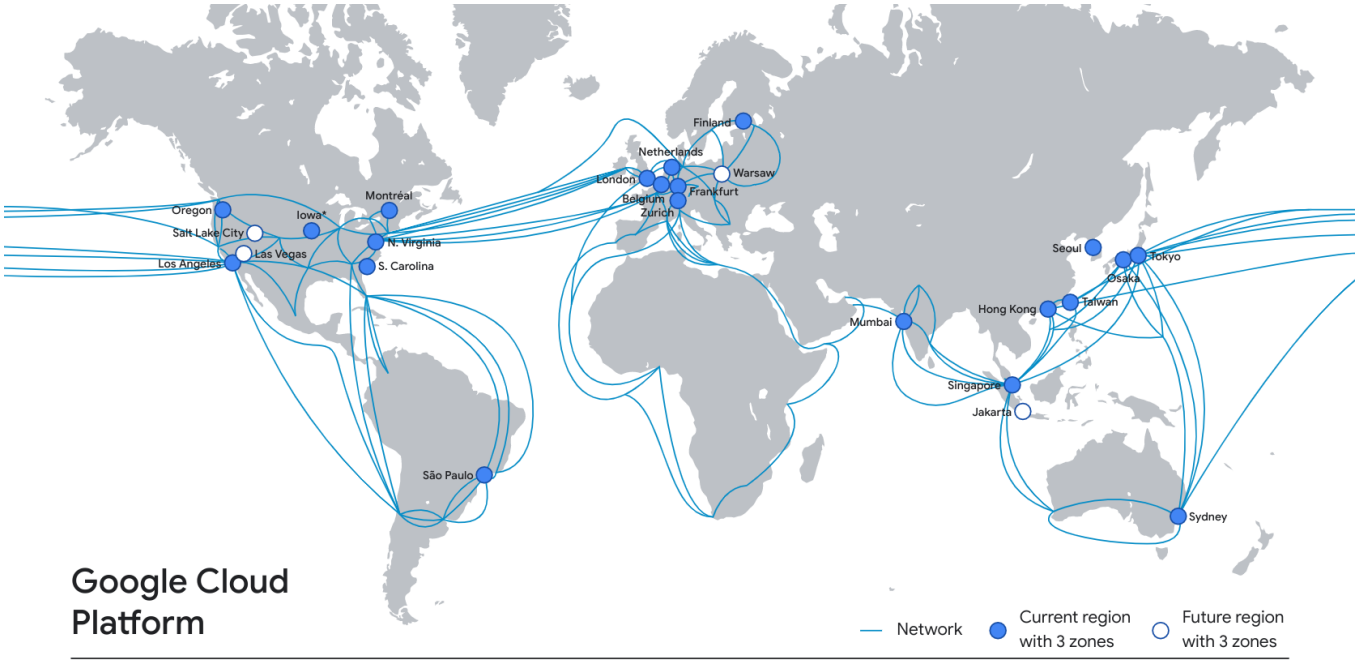
### Highly Available Services

We provide compute, database, network, storage and other services to very high levels of availability, backed by published SLAs.[19]



[18] "Third-party dependencies in cloud services", Financial Stability Board

[19] https://cloud.google.com/terms/sla




Our global infrastructure

Regarding the second point: Google Cloud products are able to provide customers with a level of operational resilience when building applications and businesses in Google Cloud that is inherently, and significantly, higher than what an individual firm is likely to be able to achieve. To expand on that, the following sections discuss the key risks associated with operational resilience, as previously outlined, and highlight some of the differentiating aspects of Google Cloud that customers can use to achieve that higher level of operational resilience.

## Cybersecurity

Google has a global scale technical infrastructure designed to provide security through the entire information processing lifecycle. This infrastructure provides secure deployment of services, secure storage of data with end user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators.

The security of the infrastructure is designed in progressive layers starting from the physical security of data centers, continuing on to the security of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes in place to support operational security. As we will see, Google's scale means it is able to invest in approaches to security that are beyond the technical and commercial means of most financial services firms[20], and as such, by migrating to Google Cloud, they can immediately benefit from a reduction in cybersecurity risk.

[20] "Third-party dependencies in cloud services", Financial Stability Board

## Secure Infrastructure

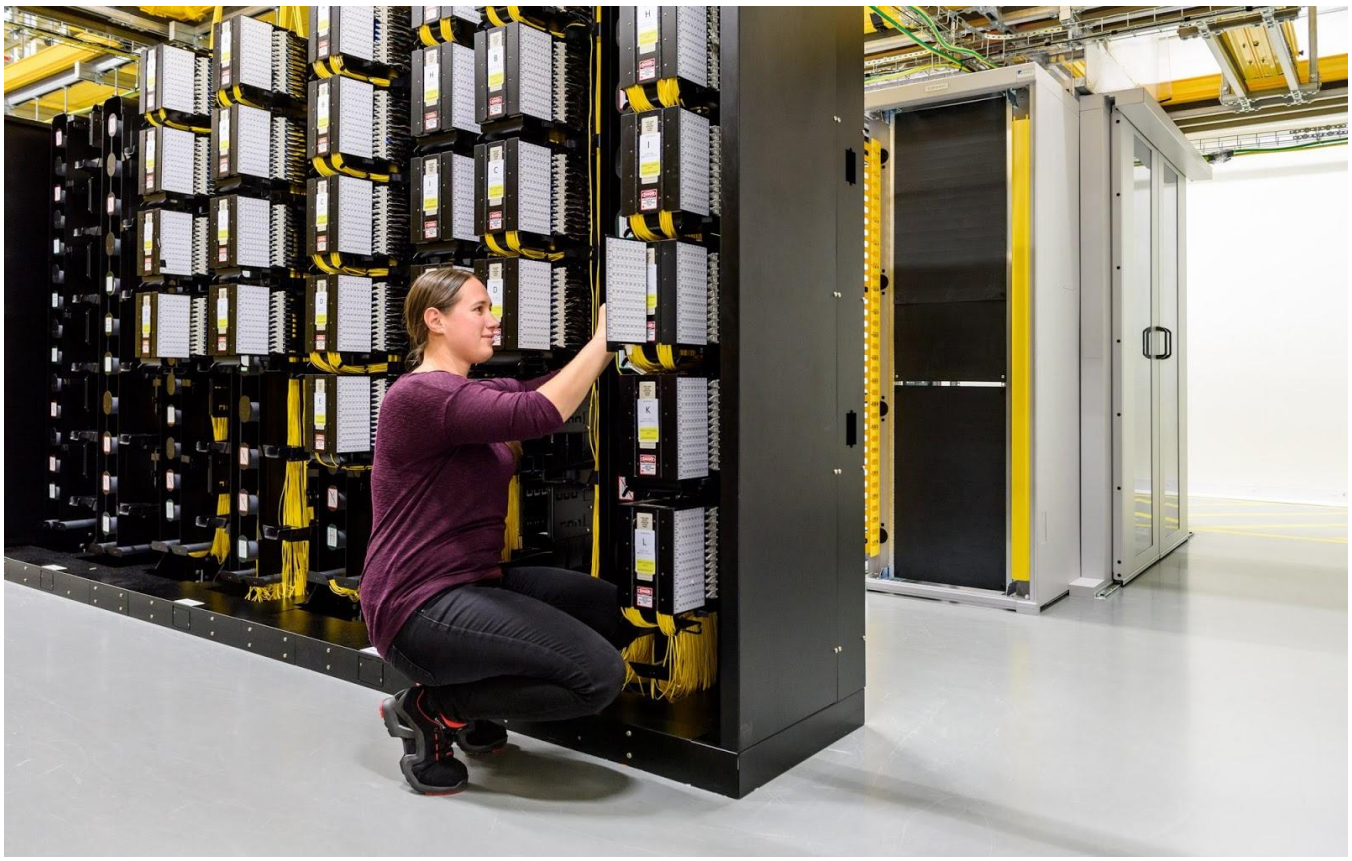
Google's servers and their operating system are designed and custom built for Google. Further, we design and include hardware specifically for security - like Titan - our custom security chip that we use to establish a hardware root of trust in our servers and peripherals.

### Hardware Design and Provenance

Both the server boards and the networking equipment are custom-designed by Google, and don't include unnecessary components like video cards or peripheral interconnects that can introduce vulnerabilities. We vet component vendors we work with and choose components with care, while working with vendors to audit and validate the security properties provided by the components.

### Service Access Management

The owner of a service can use access management features provided by the infrastructure to specify exactly which other services can communicate with it. For example, a service may want to offer some APIs solely to a specific 'allowed list' of other services. That service can be configured with those service account identities and access restriction is then automatically enforced.



## Secure Services

Google Cloud infrastructure is fundamentally designed to be multi-tenant, and does not assume any trust between services running on the infrastructure. This 'zero-trust' model contrasts significantly with the approach traditionally used in data centers, where reliance is placed on the external network perimeter to protect internal resources. Services are further secured as follows

**Service Identity**
Each service that runs on the infrastructure has an associated service account identity. A service is provided with cryptographic credentials that it can use to prove its identity. These identities are used by clients to ensure that they are talking to the correct intended server, and by servers to limit access to methods and data to particular clients.

**Service Access Management**
The owner of a service can use access management features provided by the infrastructure to specify exactly which other services can communicate with it. For example, a service may want to offer some APIs solely to a specific 'allowed list' of other services. That service can be configured with those service account identities and access restriction is then automatically enforced.

**Application Layer Transport Security (ALTS)**
At Google, we use ALTS, a mutual authentication and transport encryption system that runs at the application layer, to protect RPC communications. Using application-level security allows applications to have authenticated remote peer identity, which can be used to implement fine-grained authorization policies.

**Binary Authorization for Borg**
is an internal deploy-time enforcement check that minimizes insider risk by ensuring that production software and configuration deployed at Google is properly reviewed and authorized, particularly if that code has the ability to access user data. This allows Google to ensure that code and configuration deployments meet certain standards and allows for enforcement of software provenance in the production environment.

## Secure Data

Data is encrypted at rest, and in transit, by default in Google Cloud using 3rd party validated cryptography. Customers do not need to do anything to enable that. We recognise that customers and regulators may wish for a higher level of control or autonomy in certain situations and when processing certain types of data. To that end, Google Cloud offers a range of key management solutions, and the ability to encrypt data whilst it is being processed.


### Customer Managed Keys

Google Cloud allows customers to manage their own keys within the Google Key Management System (KMS), or within a dedicated HSM owned and operated by Google.

### Customer Owned Keys

For a higher level of control, customers may supply their own keys to operate with the Google KMS, or in certain situations within an HSM in a co-lo adjacent to the Google data center.

### External Key Manager

Where the highest level of control is needed, Google provides External Key Manager (EKM), where keys are held in customer facilities and accessed only as needed. By also adding Key Access Justification (see below), customers become the ultimate arbiters of access to their keys.

### Confidential Computing

Google Cloud customers can encrypt data in use, taking advantage of security technology offered by modern CPUs (e.g., Secure Encrypted Virtualization extension supported by 2nd Gen AMD EPYC™ CPUs) together with confidential computing cloud services. Customers can be confident that their data will stay private and encrypted even while being processed.

## Secure Internet Communications

As discussed earlier, Google's infrastructure consists of a large set of machines that are interconnected over the network, and that the security of inter-service communication is not dependent on the security of the network. However, we do isolate our infrastructure from the internet into a private IP space so that we can more easily implement additional protections such as defenses against denial of service (DoS) attacks by only exposing a subset of the machines directly to external internet traffic.

### Google Front End Service

When a service wants to make itself available on the Internet, it can register itself with an infrastructure service called the Google Front End (GFE). The GFE ensures that all TLS connections are terminated using correct certificates and following best practices such as supporting perfect forward secrecy.

### Denial of Service (DoS) Mitigation

The sheer scale of our infrastructure enables Google to simply absorb many DoS attacks. That said, we have multi-tier, multi-layer DoS protections that further reduce the risk of any DoS impact on a service running behind a GFE. After our backbone delivers an external connection to one of our data centers, it passes through several layers of hardware and software load-balancing. These load balancers report information about incoming traffic to a central DoS service running on the infrastructure. When the central DoS service detects that a DoS attack is taking place, it can configure the load balancers to drop or throttle traffic associated with the attack.

## Secure Operations

We provide tools and solutions that provide you with the control and autonomy you need to manage your security in Google Cloud.

### Manage Google Insider Threat

Google Cloud offers unparalleled transparency of Google employee access to your environments with Access Transparency, and unique offerings that allow you to control access to your encryption keys by deploying External Key Manager and Key Access Justifications.

### Manage External Threats

Leverage the scale of Google Cloud's infrastructure, and data analysis capabilities, to store and analyse petabytes of security data using Chronicle and Backstory.

### Security in the Cloud

We believe that your security in Google Cloud is a shared fate, and we provide Blueprints, Landing Zones and Security Command Centre to help you manage your critical controls.

## Pandemics

A pandemic, as we have seen during 2020, forces the decoupling of people (be they employees, or customers) from specific physical locations and facilities. This introduces a number of operational challenges, such as the need to work and collaborate remotely, which in turn can increase operational risk and reduce operational resilience if not appropriately managed using the right solutions. Google Cloud provides a number of solutions that have features that are inherently better suited to this decoupled world.

- **Remote working with BeyondCorp**
  BeyondCorp Remote Access is a cloud solution — based on the zero-trust approach we've used internally for almost a decade — that lets employees and the extended workforce access internal web apps from virtually any device, anywhere, without a traditional remote-access VPN.
- **Google Workspace**
  Best-in-class collaboration features of Workspace ensure that a remote and distributed workforce is as productive as when in the office.
- **Rapid Response Virtual Agent**
  Quickly build and implement a customized Contact Center AI virtual agent to respond to questions your customers have due to a pandemic, or other situation, over chat, voice, and social channels.
- **Providing immediate burst capacity**
  Our burst capacity solution provides additional compute and analytics capabilities that can handle some of the most compute-intensive workloads. Our goal is to ensure your infrastructure can handle significant traffic spikes and support the most demanding workloads, securely, efficiently and at scale.

## Environmental and Infrastructure

Google designs and builds its own data centers, which incorporate multiple layers of physical security protections. Access to these data centers is limited to only a very small fraction of Google employees. We use multiple physical security layers to protect our data center floors and use technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems[21]. Google additionally hosts some servers in third-party data centers, where we ensure that there are Google-controlled physical security measures on top of the security layers provided by the data center operator. For example, in such sites we may operate independent biometric identification systems, cameras, and metal detectors. Equally as important, Google operates the cleanest cloud in the industry, allowing our customers to reduce their compute and data storage emissions to zero[22].

- **Global and Regional Resilience** Google Cloud operates multi-zone data centers all over the world, providing resilience in the event of localised or even region-wide environmental or infrastructure events.
- **Global Google Support** Google Cloud has a globally distributed support function, and the vast majority of our engineers are able to work remotely, meaning we are able to support you in adverse circumstances.
- **Cost Effective IT Resilience** Capacity on demand changes the cost profile of maintaining disaster recovery capabilities: your idle infrastructure is not paid for until needed.

## Geopolitical

Today, Google Cloud's baseline controls and security features offer strong protections, meet current robust security requirements, and, in most cases, fully address customer needs. We have a long history of supporting features that are most important to customers globally. This includes critical features such as data residency controls, default encryption for data-at-rest, organization policy constraints, and VPC Service Controls, among many others.

However, we understand that customers and policymakers, particularly in Europe, strive for even greater security and autonomy. At Google Cloud, we take these issues—often discussed under the umbrella term of digital sovereignty—seriously. We are working diligently across three areas: data sovereignty, operational sovereignty, and software sovereignty, to help address digital sovereignty in the cloud computing context.

---

[21] https://www.youtube.com/watch?v=kd33UVZhnAA

[22] https://cloud.google.com/sustainability

## Strategic Autonomy through Digital Sovereignty

We understand that customers have the following requirements for sovereignty: control over all access to their data by the provider, including what type of personnel can access and from which region; inspectability of changes to cloud infrastructure and services that impact access to or the security of their data, ensuring the provider is unable to circumvent controls or move their data out of the region; and survivability of their workloads for an extended period of time in the event that they are unable to receive software updates from the provider.

These requirements reflect three distinct pillars of sovereignty: data sovereignty, operational sovereignty, and software sovereignty.


**Data sovereignty** provides customers with a mechanism to prevent the provider from accessing their data, approving access only for specific provider behaviors that customers think are necessary. Examples of customer controls provided by Google Cloud include storing and managing encryption keys outside the cloud, giving customers the power to only grant access to these keys based on detailed access justifications, and protecting data-in-use. With these capabilities, the customer is the ultimate arbiter of access to their data.

**Operational sovereignty** provides customers with assurances that the people working at a cloud provider cannot compromise customer workloads. With these capabilities, the customer benefits from the scale of a multi-tenant environment while preserving control similar to a traditional on-premises environment. Examples of these controls include restricting the deployment of new resources to specific provider regions and limiting support personnel access based on predefined attributes such as citizenship or a particular geographic location.

**Software sovereignty** provides customers with assurances that they can control the availability of their workloads and run them wherever they want, without being dependent on or locked-in to a single cloud provider. This includes the ability to survive events that require them to quickly change where their workloads are deployed and what level of outside connection is allowed. This is only possible when two requirements are met, both of which simplify workload management and mitigate concentration risks: first, when customers have access to platforms that embrace open APIs and services; and second, when customers have access to technologies that support the deployment of applications across many platforms, in a full range of configurations including multi-cloud, hybrid, and on-premises, using orchestration tooling. Examples of these controls are: platforms that allow customers to manage workloads across providers; and orchestration tooling that allows customers to create a single API that can be backed by applications running on different providers, including proprietary cloud-based and open-source alternatives.

## Third Party Risk

We recognise that third party risk is a significant component of a firm's overall operational resilience posture. Given that, financial services customers will seek to ensure that their critical third parties can provide equal, if not better, operational resilience. We provide transparency to customers through various mechanisms including on-site audits and compliance certifications[23] such that they can build the necessary assurance.

But we also recognise that from a financial services firm's perspective, achieving its desired operational resilience may include solving for situations where their third parties are unable, for any reason, to provide the services contracted. Google Cloud believes in an open cloud[24] that supports multi-cloud, and hybrid cloud approaches, which if implemented through the use of open-source based technologies, can provide customers with the levels of portability, substitutability and survivability, required to fit their operational resilience risk appetite.

### Risks Mitigated by Multi-Cloud Strategy

Cloud Hyperscalers provide sufficiently robust services that, when correctly designed and configured, can offer a level of resilience which matches or exceeds what can be achieved in firms' own data centers[25].
A multi-cloud strategy is important in a number of areas as follows:


1. Ability to choose services which provide the maximum value and flexibility to the business;
2. Provide a level of assurance that exit strategy is possible from any specific provider, allow for switching and portability;
3. Remove or mitigate concentration of risk in a single service provider and decrease vendor dependencies;
4. Guarantee alignment to legacy workload and ability to gain more value with lower level of investment than with a single service provider.

In the context of operational resilience, use of cloud creates a dependence on a relationship with a third party, and a risk that either this relationship could fail, or that the third party could fail as a business or stop providing services as a result of a geo-political risk. Most firms develop exit strategies to mitigate these risks: in many jurisdictions this is a regulatory requirement for material outsourcing arrangements. Multi-cloud is a way to implement such an exit strategy, either by creating cloud-like capabilities within a firm's own data centers, or by establishing and proving relationships with more than one cloud provider (or both).

---

[23] https://cloud.google.com/security/compliance/financial-services
[24] https://cloud.google.com/blog/products/gcp/why-google-believes-in-open-cloud
[25] "Third-party dependencies in cloud services", Financial Stability Board

### Portability vs Cloud Native Services

Two of the key advantages to cloud platforms are access to fully managed services, and access to capabilities which are not available as on-premise solutions. However, such services are often proprietary to an individual cloud provider which can inhibit the ability to move services between cloud providers, and can reduce the value of a multi-cloud strategy.

Google recognises that most financial services firms will adopt a multi-cloud strategy, and that they will be obliged to develop exit plans as they move material workloads to cloud. Google offers a level of portability through support for open standards, through contributions to Open Source projects, and through the development of Anthos as a multi-cloud service: Google believes that this level of openness and support for multi-cloud is leading in the cloud industry. However, even when using these capabilities, portability should be treated as a means rather than an end: it is a tool to support exit plans, rather than an essential feature of cloud services. If treated as an essential feature of cloud services, portability will limit the services that can be used and limit the benefits of cloud.

- **Cloud Native Services** Use native services where possible, only limiting their use where they would prevent the creation of a viable exit plan for services requiring such a plan.
- **Exit Plans based on Open Source** Leverage Google Cloud's commitment to common and open standards to create an exit plan which could be executed in the required time.
- **Anthos Simplifies Multi-cloud** Establish common, compatible deployments of Kubernetes and other services on premise and across cloud platforms.

## Technology Risk

Financial services technology organizations are at an inflection point. In the 50 or so years since banks started using Mainframes, the industry has invested trillions of dollars in largely on-premise, self-managed technology. Historically, this meant building their own data centers, global networks, managing hundreds of thousands of servers and PCs, and writing proprietary applications. In addition, much of this technology was built to serve the "pre-digital era" of daily batches and asynchronous business driven by branch opening hours and the speed of cheques and letters delivered by post.

Customers now expect to be able to access financial services products and services at any time, through a range of digital and other channels. And as we have seen, the complexities of achieving this on top of existing technologies can result in technical and operational failures that are increasingly in focus for regulators that are concerned with financial stability and preventing customer harm[26].

[26] IT failures in the Financial Services Sector, UK House of Commons Treasury Select Committee

So there are compelling arguments for a strategic overhaul of financial services technology. However the costs, and timescales, involved with refactoring existing technologies using the traditional methods of delivering IT (on premise and/or using traditional outsourcing models) are such that it is unlikely to be an achievable strategy for most firms. In part this is because the traditional models involve the financial services firm managing, as we have discussed, everything from the data center upwards.

By migrating to Google Cloud, financial services firms can ensure that their technology organisations are focussed on delivering high-quality services and experiences to customers, and not on operating foundational technologies, and materially reduce their Technology Risk profile as a consequence. For example:

- **Operate Above the Infrastructure** By migrating to Google Cloud,whilst customers retain control over the Google Cloud products deployed, they no longer have to dedicate resources to managing data centers, physical servers and network equipment, nor do they have to worry about patching or maintaining core operating systems and hypervisor services.
- **Use Containers to Reduce Debt** Even if a given application is not going to be fully modernised - perhaps it will be demised in the foreseeable future - firms can reduce the technical debt associated (e.g. unsupported hardware or operating system) with it by migrating it into a container image and managing it using Google Kubernetes Engine (GKE).
- **Mainframe Modernisation** Through the use of automated processes Google Cloud tools can break down your Cobol, PL/1, or Assembler programs into services and then make them cloud native, such as within a managed, containerized environment.

## Conclusion

Operational resilience is critically important to maintaining financial stability.  Financial services firms, their customers and counterparties, and policymakers are all therefore, quite rightly, focused on strengthening operational resilience.

Google Cloud is supportive of the approaches being developed and will continue to engage with policy makers and our customers to ensure they can achieve the desired outcomes. We understand the myriad complexities of financial services technology, and the journey ahead of the industry in order to provide the products and services customers need, whilst addressing the requirements for operational resilience.

We are committed to ensuring that Google Cloud solutions for financial services are designed to address these requirements in a manner that best positions the financial services sector in all aspects of operational resilience. Furthermore, we recognise that this is not simply about making Google Cloud resilient: the sector needs autonomy, sovereignty and survivability.

# Appendix

## Regulator Perspectives on Operational Resilience

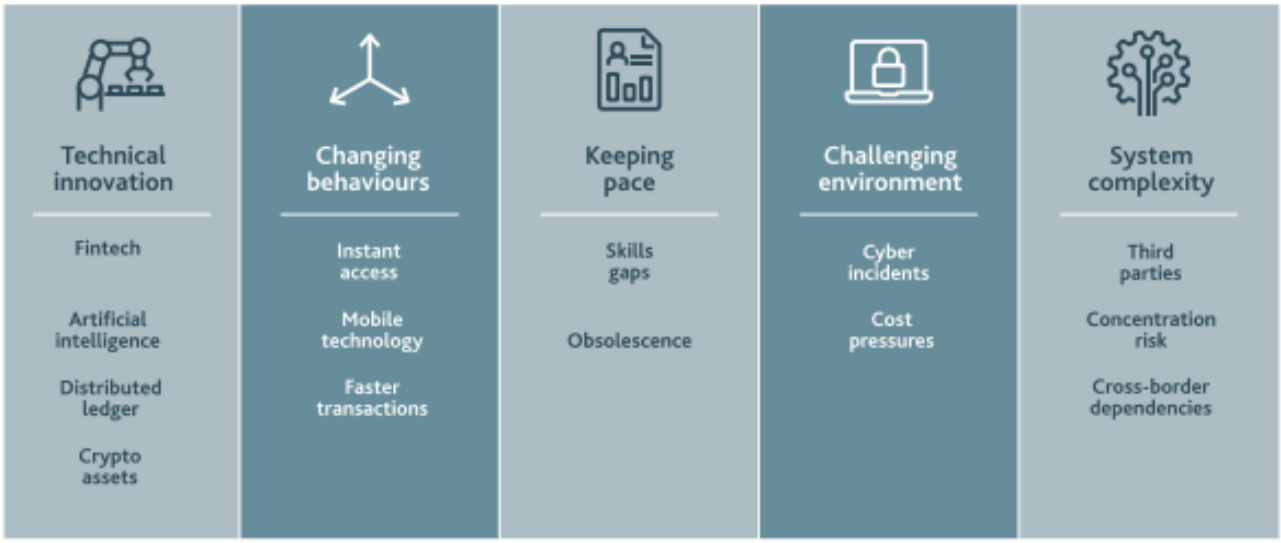
Global Regulators recognise the importance of operational resilience, and that it can have as significant a bearing on financial stability as Financial Resilience (i.e., credit risk, market risk, liquidity risk), and that strengthening operational resilience requires the effective management of multiple operational risks.

There is also a growing recognition that, far from creating unnecessary new risk, a well executed migration to cloud technology over the coming years will provide capabilities to financial services that will enable them to strengthen their operational resilience in ways that are not otherwise achievable.

Google Cloud understands the importance of this risk in maintaining the stability of the global financial system, the need for the right regulatory frameworks to manage it, and is committed to helping our customers achieve their operational resilience goals and to working with policymakers to develop standards.

### United Kingdom

In 2018, the Bank of England, Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA) released a joint discussion paper[27] describing several new concepts described in the above sections. The need to adopt a more expansive approach was identified because financial services firms face "numerous challenges to making sure their businesses are resilient to operational disruption. These challenges have become more complex and intense in recent years, during a period of technological change and in an increasingly hostile cyber environment." Some of these challenges are represented in the following diagram, taken from the paper.



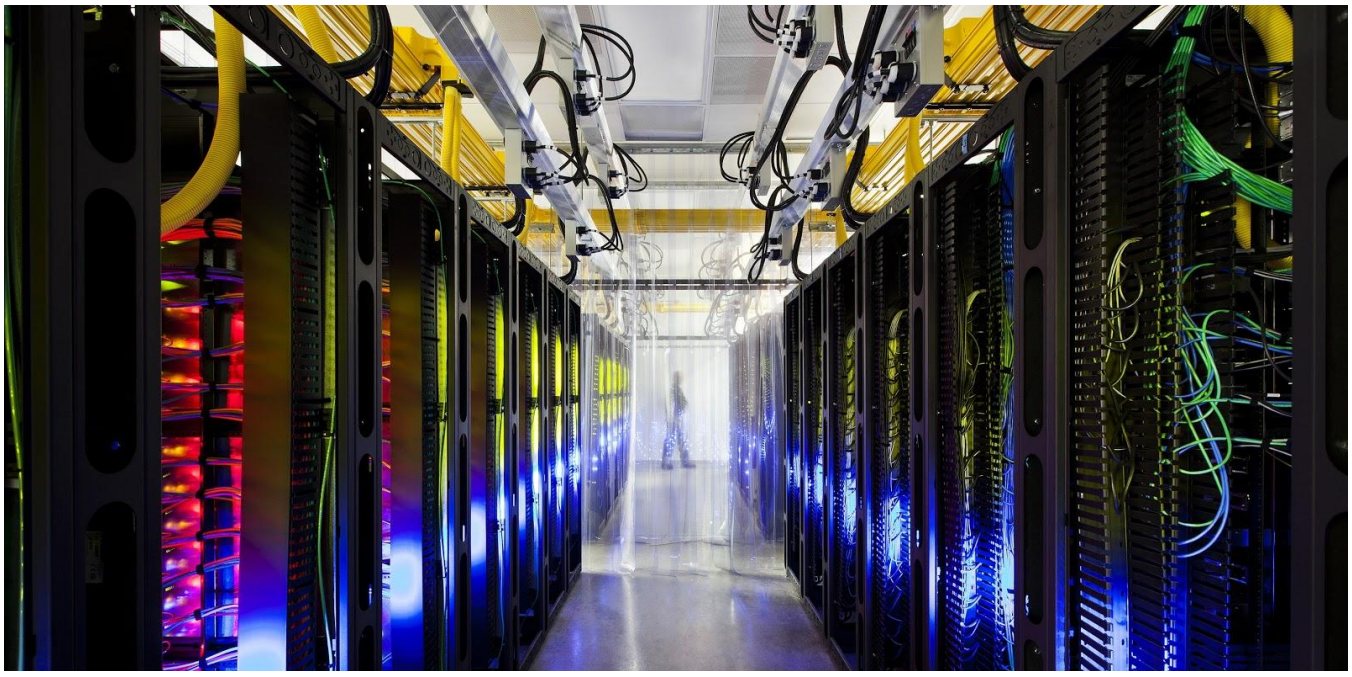

[27] "Building the UK financial sector's operational resilience", Bank of England, PRA, FCA

In 2019, in addition to publishing an update to this discussion paper, in the form of a modified but materially similar consultation paper[28], the Bank of England also published the report of a review it commissioned regarding the Future of UK Finance[29]. In this report, and the Bank of England's response[30] it was noted that it is important that firms embrace the use of cloud technology in order to benefit from greater resilience:

> *"Another priority should be for financial services to embrace cloud technologies, which have matured to the point they can meet the high expectations of regulators and financial institutions. Shifting from in-house data storage and processing to cloud environments can speed up innovation, enable use of the best analytical tools, increase competition and build resilience."*

> *"Cloud service providers offer ready-made solutions that can accelerate time to market. With the benefit of their scale, they also offer leading-edge analytics, enabling businesses to learn and adjust their business models almost in real time. And they can offer greater resilience"*

Finally in December 2019, the PRA issued a consultation regarding outsourcing, in part to "facilitate greater resilience and adoption of the cloud and other new technologies", but noting that firms needed to be able to address concentration risk and the potential for vendor lock-in by focusing on the ability to exit from an arrangement (see **Third Party Risk** for how Google Cloud is inherently equipped to help customers manage this risk). The regulators are planning to issue the final guidance in early 2021.



[28] "Operational resilience: Impact tolerances for important business services", Bank of England, PRA, FCA
[29] "Review on the outlook for UK Financial Services: What it means for the Bank of England", van Steenis
[30] "New economy, new finance, new Bank" Bank of England

## European Union

EU Financial Services regulators have, over the course of 2019 and 2020, published guidelines on key aspects of operational resilience, such as Information and Communications Technology (ICT)[31] and Outsourcing. Outsourcing guidelines from the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) (currently at the drafting stage) all reflect the interdependencies between operational resilience and a well-defined and managed approach to outsourcing, requiring financial services firms to address a number of operational risks, for example:

**Third Party Risk** Managing supply chain risk, and in particular of critical outsourced functions by addressing vendor lock in, survivability and portability.

> *"with regard to the outsourcing of critical or important functions, they are able to undertake at least one of the following actions, within an appropriate time frame:*
> *i. transfer the function to alternative service providers;*
> *ii. reintegrate the function; or*
> *iii. discontinue the business activities that are depending on the function"* [32]

**Cybersecurity** Continuously adjusting key controls, people, processes and technology to prevent, detect and react to external threats and malicious insiders.

> *"consider specific measures, where necessary, for data in transit, data in memory and data at rest, for example, the use of encryption technologies in combination with an appropriate keys management;"*[33]

**Geopolitical** Understanding and managing risks associated with geographic and political boundaries between intragroup and third-party dependencies

> *"consider the political stability and security situation of the jurisdictions in question, including:*
> *i. the laws in force, including laws on data protection;*
> *ii. the law enforcement provisions in place; and*
> *iii. the insolvency law provisions that would apply in the event of a service provider's failure and any constraints that would arise in respect of the urgent recovery of the institution's or payment institution's data in particular;"* [34]

[31] "Guidelines on ICT and security risk management" European Banking Authority
[32] "Guidelines on Outsourcing Arrangements" European Banking Authority
[33] "Guidelines on Outsourcing to Cloud Service Providers", European Insurance and Occupational Pensions Authority
[34] "Guidelines on Outsourcing Arrangements" European Banking Authority

In 2020, European policymakers took a step to more directly address the needs for operational resilience in financial services, through a new regulatory proposal — Digital Operational Resilience for the Financial Sector (DORA)[35].

DORA addresses a number of important topics for financial entities using ICT services, with the objective of enhancing the digital resilience of the European financial system from incident reporting to operational resilience testing and third party risk management. As we have discussed, resilience and security are at the core of Google Cloud's operations. And we firmly believe that migration to the public cloud can help financial entities improve their operational resilience and security posture. At the same time, the oversight framework for critical third-party providers under DORA could create a genuine opportunity to enhance understanding, transparency, and trust among ICT service providers, financial entities, and financial regulators, and ultimately stimulate innovation in the financial sector in Europe.

## United States

In late 2020, the Federal Reserve Board, Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation (collectively, the agencies), published an interagency paper[36] designed to strengthen operational resilience in financial services. This reflects that:

> *"In recent years, firms have experienced significant challenges from a wide range of disruptive events including technology-based failures, cyber incidents, pandemic outbreaks, and natural disasters. While advances in technology have improved firms' ability to identify and recover from various types of disruptions, increasingly sophisticated cyber threats and growing reliance on third parties continue to expose firms to a range of operational risks. These operational risks underscore the importance for firms of all sizes to strengthen their operational resilience."*

As stated, the paper emphasises that the management of a number of operational risks is key to strengthening operational resilience. For example:

**Environmental and Infrastructure** Designing and locating facilities to mitigate the effects of localised weather and infrastructure events, and to be resilient to physical attack.

> *"The firm has (an) alternate site(s) that has sufficient resources (including personnel), technology capabilities, and functionality to execute the firm's critical operations and core business lines in the event of a disruption. The alternate site(s) is (are) located at a sufficient geographical distance from the primary site and has (have) a distinct risk profile"*

---

[35] "Draft Regulation on digital operational resilience for the financial sector", European Commission

[36] "Sound Practices to Strengthen Operational Resilience", FRB, OCC, FDIC

**Pandemics** Sustaining business operations in scenarios where people cannot, or will not, work in close proximity to colleagues and customers.

> *"The firm's business continuity management includes remote-access contingencies that allow personnel to continue delivering the firm's critical operations and core business lines through a disruption.The management of contingencies prioritize critical operations and core business lines and provide personnel adequate connectivity, communication, and collaboration tools, essential technology resources, and access to network systems."*

**Third Party Risk** Managing supply chain risk, and in particular of critical outsourced functions by addressing vendor lock in, survivability and portability.

> *"The firm identifies other third parties that may be available to assist in the event its current third parties are unable to continue delivering services. The firm assesses the substitutability of third parties that provide services supporting the firm's critical operations and core business lines including the possibility of bringing a service back in-house."*

**Cybersecurity** Continuously adjusting key controls, people, processes and technology to prevent, detect and react to external threats and malicious insiders.

> *"The firm's information systems architecture for critical operations and core business lines incorporates the firm's cyber resilience requirements and is secure by design. The firm also accounts for interdependency, interconnectivity, scale, and complexity risks."*

**Technology Risk** Designing and operating technology services to provide the required levels of availability, capacity, performance, quality and functionality.

> *"The firm has and enforces defined processes for technology acquisition, development, testing, and integration that incorporate the firm's resilience requirements throughout the processes' lifecycles."*

> *"The firm upgrades or replaces information system components before technical support is no longer available from the developer, vendor, or manufacturer."*

## Singapore

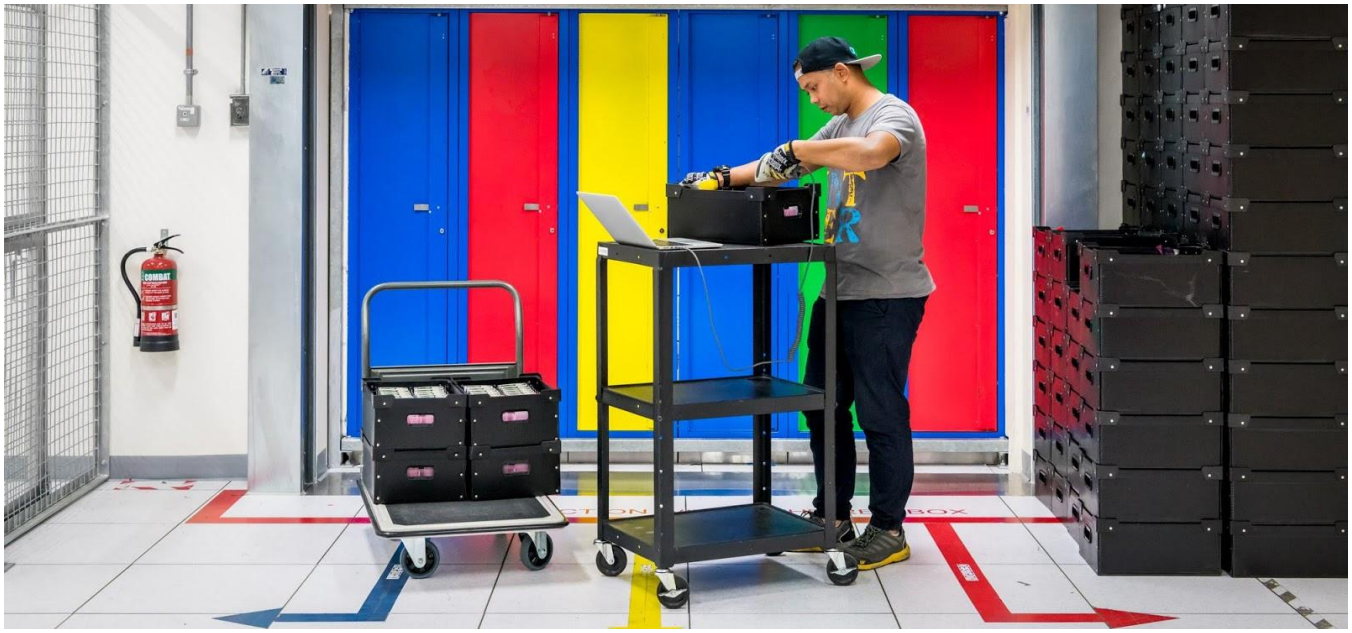
The Monetary Authority of Singapore, in its Guidelines on Outsourcing[37], recognise the significance that outsourcing can have on the financial institution's risk profile, requiring that firm consider this by

> *"analysing the impact of the outsourcing arrangement on the overall risk profile of the institution, and whether there are adequate internal expertise and resources to mitigate the risks identified;"*

Other guidelines, including those on Technology Risk Management[38], and Business Continuity Management[39] include various requirements regarding **technology risk**, **cybersecurity** and **third party risk** that an adoption of cloud could simplify for the organization.

It is also noted that a well-managed migration to "Cloud services (CS)" could bring operational resilience benefits.

> *"CS can potentially offer a number of advantages, which include economies of scale, cost-savings, access to quality system administration well as operations that adhere to uniform security standards and best practices. CS may also be used to provide the flexibility and agility for institutions to scale up or pare down on computing resources quickly as usage requirements change, without major hardware and software outlay as well as lead-time. In addition, the distributed nature of CS may enhance system resilience during location-specific disasters or disruptions"*



[37] "Guidelines on Outsourcing", Monetary Authority of Singapore
[38] "Guidelines on Technology Risk Management", Monetary Authority of Singapore
[39] "Guidelines on Business Continuity Management", Monetary Authority of Singapore

## Hong Kong

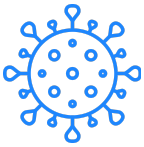
The Hong Kong Monetary Authority's Supervisory Policy Manual module on Operational Risk[40] notes that a firm's operational risk profile will be "particularly" driven by a number of factors including **Technology Risk**, **Outsourcing** and business continuity, all of which are subject to specific further modules[41] in the supervisory policy manual.

## Australia

The Australian Prudential Regulation Authority (APRA) maintains a number of papers and standards relevant to operational resilience, including cloud outsourcing[42], information security[43], and business continuity[44]. It notes that

> *"From APRA's perspective, the core of operational resilience is the ability of regulated entities to continue to deliver business services in the face of potential shocks, including:*

man-made shocks, such as physical and cyber-attacks, IT system outages and third-party supplier failure,



natural disasters such as fire, flood, severe weather and pandemics, and

situations and events that require a more strategic response, such as regulatory developments, new competitors with more efficient operating models, risks associated with climate change, and innovative technology solutions."[45]

[40] "Supervisory Policy Manual: OR-1 Operational Risk Management", Hong Kong Management Authority (HKMA)
[41] "SA-2 Outsourcing", "TM-G-1 "General Principles for Technology Risk", TM-G-2 " Business Continuity Planning", HKMA
[42] "Outsourcing involving cloud computing services", Australian Prudential Regulation Authority
[43] "Prudential Standard CPS 234 Information Security", Australian Prudential Regulation Authority
[44] "Prudential Standard CPS 232 Business Continuity Management", Australian Prudential Regulation Authority
[45] https://www.apra.gov.au/covid-19-a-real-world-test-of-operational-resilience

## International

In mid 2020, the Basel Committee on Banking Supervision published a consultative document on operational resilience[46], reflecting that while "significantly higher levels of capital and liquidity have improved banks' ability to absorb financial shocks" that further work is needed to

> *"strengthen banks' ability to absorb operational risk-related events, such as pandemics, cyber incidents, technology failures or natural disasters, which could cause significant operational failures or wide-scale disruptions in financial markets"*

The paper note that the essential elements of operational resilience include the effective management of operational risk, and specifically identifies the following risks as key: business continuity (including the dependencies on people, process, technology, facilities and third parties, and the operational risks involved such as **Pandemics** and **Environmental and Infrastructure events**); **Third Party** dependency management, and ICT including **Cybersecurity**.

Additionally, the International Organisation of Securities Commissions (IOSCO)[47] has published a consultation paper on outsourcing and third party management. In common with other regulatory papers, this notes both the potential benefits of leveraging cloud-based services, whilst needing to manage the attendant risks:

> *"One example of the potential benefits of outsourcing is evident in the use of cloud-based services or infrastructure. Based upon" .... "interactions with cloud computing experts, proponents of cloud-based infrastructures highlight several advantages:*

**Improved accessibility**
Services are accessible from a wide variety of devices and from any location with network access to the cloud.

**Cost efficiency**
Cloud provider resources are pooled to serve multiple clients, which creates economies of scale. This reduces the cost of data storage.

**Demand scalability**
The cloud provides a flexible platform that can grow and shrink to match the client's needs.

**Always-on availability**
Applications running on a cloud infrastructure are rarely offline and are accessible whenever there is an internet connection.

**Improved Security**
A key concern of a cloud provider is to carefully monitor the cloud's security, which is more efficient than security monitoring a conventional in-house system."

---

[46] "Principles for operational resilience", Basel Committee on Banking Supervision
[47] "Principles on Outsourcing", International Organisation of Securities Commissions

Finally, the Financial Stability Board has published two papers that are relevant to this topic, and both note the potential for improved operational resilience in financial services through the use of cloud

> *"Cloud services may present a number of benefits over previous technology, such as on-premises data centres. By creating geographically dispersed infrastructures, and investing heavily in security, cloud service providers may offer significant improvements in resilience for individual institutions."*[48]

And that as the significance of cloud services increase, that the approach to managing the associated risks, and regulating the firms adopting cloud, continues to evolve

> *"The evolving landscape of FIs' third-party relationships has prompted several supervisory authorities to update or consider updating their regulatory and supervisory framework on outsourcing, third-party risk management and related areas, such as business continuity planning, cybersecurity, data protection, operational resilience and risk management."*[49]

[48] "Third-party dependencies in cloud services", Financial Stability Board

[49] "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships", Financial Stability Board

## References


Resilience and continuity in an interconnected and changing world
Speech by Lyndon Nelson, Bank of England

Sound Practices to Strengthen Operational Resilience
FRB, OCC, FDIC

Operational resilience: Impact tolerances for important business services
Bank of England, PRA, FCA

Draft Regulation on digital operational resilience for the financial sector
European Commission

Building the UK financial sector's operational resilience
Bank of England, PRA, FCA

Review on the outlook for UK Financial Services: What it means for the Bank of England
Report by Huw van Steenis

New economy, new finance, new Bank
Bank of England

Guidelines on ICT and security risk management
European Banking Authority

Guidelines on Outsourcing Arrangements
European Banking Authority

Guidelines on Outsourcing to Cloud Service Providers
European Insurance and Occupational Pensions Authority

Draft Guidelines on Outsourcing to Cloud Service Providers
European Securities and Markets Authority

Principles for operational resilience
Basel Committee on Banking Supervision

Principles on Outsourcing
International Organisation of Securities Commissions

IT failures in the Financial Services Sector
UK House of Commons Treasury Select Committee

Guidelines on Outsourcing
Monetary Authority of Singapore

Guidelines on Technology Risk Management
Monetary Authority of Singapore

Guidelines on Business Continuity Management
Monetary Authority of Singapore

Supervisory Policy Manual
Hong Kong Monetary Authority

Third-party dependencies in cloud services
Financial Stability Board

Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships
Financial Stability Board

Outsourcing involving cloud computing services
Australian Prudential Regulation Authority

Prudential Standard CPS 234 Information Security
Australian Prudential Regulation Authority

Prudential Standard CPS 232 Business Continuity Management
Australian Prudential Regulation Authority