Bank of England
Prudential Regulatory Authority (PRA)
Supervisory Statements | SS1/21
Operational Resilience: Impact tolerances for important business services

April 2022

Overview

In March 2021, the Bank of England Prudential Regulatory Authority (PRA) published "Supervisory Statement | SS1/21 Operational resilience: Impact tolerances for important business services (SS1/21)." In this statement, the PRA requires UK financial sector firms to (i) **identify important business services; (ii) set impact tolerances for their important business services; (iii) take action to remain within impact tolerances; (iv) perform process mapping; (v) conduct scenario testing; (vi) establish governance structure; (vii) perform self-assessments; and (viii) identify groups for important business services.**

This document provides insight into the ways Google Cloud helps customers meet their obligations under PRA SS1/21.

Disclaimer

The contents of this document are accurate as of April 2022 and represent Google's products, systems and policies as of the time it was written. The analysis contained herein is limited to sections of the regulation relevant to Google Cloud and its customers, and is provided for informational purposes only. It does not constitute legal advice. For additional information, please see the full text of SS1/21.

Operational Resilience

The PRA defines operational resilience as “the ability of firms, their groups, and the financial sector as a whole to prevent, adapt to, respond to, recover from, and learn from operational disruptions”[1].

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

The PRA’s approach to operational resilience is based on the assumption that, from time to time, disruptions will occur which will prevent firms from operating as usual and see them unable to provide their services for a period[2].

This is consistent with one of Google's key principles for achieving extremely high service availability: plan for failure. While Google Cloud provides extremely reliable service, disasters will strike and these disasters cause outages. Planning for outages enables Google Cloud customers to build applications that perform predictably through these inevitable events.

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

---

[1]SS1 SS1/21 Operational resilience: Impact tolerances for important business services, para 1.5
[2]SS1 SS1/21 Operational resilience: Impact tolerances for important business services, para 1.5

Foundationally, Google Cloud's infrastructure and operating model is of a scale and robustness that can provide financial services customers a way to increase their resilience in a highly commercial way.

For more information about the operational resilience benefits from migrating to Google Cloud refer to our 'Strengthening operational resilience in financial services by migrating to Google Cloud' whitepaper.

Impact Tolerances

Firms must set an impact tolerance for each of their important business services. An impact tolerance is the maximum tolerable level of disruption to an important business service as measured by a length of time in addition to any other relevant metrics[3].

The PRA expects firms to be able to remain within impact tolerances for important business services, irrespective of whether or not they use third parties in the delivery of these services. This means that firms should effectively manage their use of third parties to ensure they can meet the required standard of operational resilience[4].

Google is committed to enabling firms to achieve their desired reliability outcomes on Google Cloud. To support you, we show you how to architect and operate reliable services on a cloud platform in the Google Cloud Architecture Framework. We also share information and resources on how to design applications that are resilient to cloud infrastructure outages in our Architecting disaster recovery for cloud infrastructure outages article, which is part of our Disaster Recovery Planning Guide. Specifically, this article walks through:

1. The Google Cloud infrastructure, how disaster events manifest as Google Cloud outages, and how Google Cloud is architected to minimize the frequency and scope of outages.
2. An architecture planning guide that provides a framework for categorizing and designing applications based on the desired reliability outcomes.
3. A detailed list of select Google Cloud products that offer built-in DR capabilities which you may want to use in your application.

We recognize that to remain within impact tolerances firms often need to be able to achieve specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). In business terms, RTO translates as "How long after a disaster before I'm up and running." RPO translates as "How much data can I afford to lose in the event of a disaster."

---

[3] SS1 SS1/21 Operational resilience: Impact tolerances for important business services, para 3.1
[4] SS1 SS1/21 Operational resilience: Impact tolerances for important business services, para 4.5

In our article we share information about how you can achieve your desired RTO and RPO for your applications on Google Cloud. If you would like more information about RTO and RPO, please get in touch with your Google Cloud account representative.

Mapping

Firms must identify and document the necessary people, processes, technology, facilities, and information (the 'resources') required to deliver each of their important business services. This identification process is referred to as 'mapping'[5].

The PRA expects firms to map the resources necessary to deliver important business services irrespective of whether the resources are being provided wholly or in part by a third party, which may be an intragroup or external service provider. Firms should understand how their outsourcing and third party dependencies support important business services[6].

Google offers a number of tools that firms can use to help with mapping both on-premises and on Google Cloud.

Even before you are on Google Cloud, you can use our Risk Assessment & Critical Asset Discovery solution to evaluate your organization's current IT risk, identify where your critical assets reside, and receive recommendations for improving your security posture and resilience.

Once on Google Cloud, you can leverage these tools to map and manage your cloud resources on an ongoing basis:

- **Google Cloud Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP, including availability and uptime of the services.
- **Resource Manager** allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources.
- **Cloud Deployment Manager** is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.

[5]SS1 SS1/21 Operational resilience: Impact tolerances for important business services, para 5.1
[6]SS1 SS1/21 Operational resilience: Impact tolerances for important business services, para 5.5

- **Risk Manager** enables you to receive reports on the controls that impact your overall security posture to remediate issues such as misconfigurations, helping to reduce risk and reduce time spent on managing security settings.

Scenario Testing

Firms must regularly test their ability to remain within impact tolerances in severe but plausible disruption scenarios[7].

Google recognizes the importance of regular testing in the context of operational resilience. Google runs annual, company-wide, multi-day Disaster Recovery Testing events (DiRT) to ensure that Google's services and internal business operations continue to run during a disaster. DiRT was developed to find vulnerabilities in critical systems by intentionally causing failures, and to fix those vulnerabilities before failures happen in an uncontrolled manner. DiRT tests Google's technical robustness by breaking live systems and tests our operational resilience by explicitly preventing critical personnel, area experts, and leaders from participating. All generally available services are required to have ongoing, active DiRT testing and validation of their resilience and availability.

Refer to this blog post for more information about the resilience testing that Google performs as well as recommendations on how to train your first responders so they can react efficiently under pressure. You'll also find templates so you can get started testing these methods in your own organization. Firms can also request to review Google Cloud's testing results.

In addition to testing our own environments, we also provide a number of tools and resources that enable firms to independently test their Google Cloud deployments.

Our Disaster Recovery Scenarios for Data and Disaster Recovery for Applications articles provide information about common disaster scenarios for backing up and recovering data and for applications, respectively.

You can also implement the following to help with your own testing:

- **Automate infrastructure provisioning with Deployment Manager**. You can use Deployment Manager to automate the provisioning of VM instances and other Google Cloud infrastructure. If you're running your production environment on premises, make sure that you have a monitoring process that can start the

[7]SS1 SS1/21 Operational resilience: Impact tolerances for important business services, para 6.1

disaster recovery process when it detects a failure and can trigger the appropriate recovery actions.

- **Monitor and debug your tests with Cloud Logging and Cloud Monitoring**. Google Cloud has excellent logging and monitoring tools that you can access through API calls, allowing you to automate the deployment of recovery scenarios by reacting to metrics. When you're designing tests, make sure that you have appropriate monitoring and alerting in place that can trigger appropriate recovery actions.

The PRA expects contractual agreements for material outsourcing arrangements to include 'requirements for both parties to implement and test business contingency plans'[8].

Google commits to implement a business continuity plan for our services, review and test it at least annually and ensure it remains current with industry standards.

Our business continuity plan covers key personnel and all essential facility infrastructure, including power, water, cooling, fire alarms, physical networks and IT hardware. It is designed to minimize disruptions to the services caused by disaster or other events that disrupt the operations and resource required to provide the services, including:

- destruction of infrastructure required to provide the Services
- interruption to the operation of infrastructure required to provide the Services (including electrical and mechanical failures)
- unavailability of key personnel
- emergency weather conditions (e.g. tornado, hurricane, typhoon) and natural disasters (e.g. earthquake)
- pandemics

Firms can request to review Google Cloud's business continuity plan.

For more information about how Google can help you address the requirements in SS2/21 Outsourcing and Third Party Risk Management refer to our compliance mapping.

[8] SS1 SS1/21 Operational resilience: Impact tolerances for important business services, para 6.13

Conclusion

Google recognizes that operational resilience is a key focus for firms and supervisory authorities in the UK. We are committed to ensuring that Google Cloud solutions for financial services are designed in a manner that best positions the sector in all aspects of operational resilience. Furthermore, we recognize that this is not simply about making Google Cloud resilient: the sector needs autonomy, sovereignty and survivability. You can learn more about Google Cloud's point of view on operational resilience in financial services in our whitepaper.

Additional Resources

- PRA SS1/21 full text
- Strengthening Operational Resilience in Financial Services by Migrating to Google Cloud
- Google Cloud Architecture Framework
- Architecting disaster recovery for cloud infrastructure outages
- Disaster Recovery Planning Guide
- Security & Resilience Framework
- Cloud Monitoring
- Resource Manager
- Cloud Deployment Manager
- Risk Protection Program
- Shrinking the time to mitigate production incidents—CRE life lessons blog
- SS2/21 Outsourcing and Third Party Risk Management refer to our compliance mapping