Google Cloud Whitepaper
September 2024

Google Cloud and the EU Digital Operational Resilience Act (DORA)

ICT Risk Management Customer Guide

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of September 2024 and represents the status quo as of the time it was written. Google Cloud's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

Chapter II of the European Union (EU) Digital Operational Resilience Act (Regulation (EU) 2022/2554 - 'DORA') requires financial entities in the EU to establish a comprehensive strategy for managing ICT risks. This involves identifying potential risks, implementing appropriate measures, and continuously evaluating their effectiveness. To ensure effective risk management, financial entities should implement a well-organized process that includes identifying, documenting, accepting, and regularly assessing residual risks. These risks should be incorporated into their comprehensive risk management framework.

As part of Google Cloud's Shared Fate model, Google Cloud provides services on a highly resilient, secure and controlled platform and offers a wide array of features from which customers can benefit. Shared fate includes Google Cloud building and operating a trusted cloud platform for your workloads and providing best practice guidance and secured, attested infrastructure code that you can use to deploy your workloads in a secure way.

Consistent with our belief in Shared Fate:

- Section 2 of this Customer Guide explains Google Cloud's approach to operational resilience in financial services, including regarding key operational risks, such as cybersecurity, third-party, environmental and infrastructure, and technology risks; and
- Section 3 of this Customer Guide offers solutions to assist customers in meeting their own ICT risk management via a comprehensive mapping of Chapter II requirements to Google Cloud offerings.

1. Overview of the EU Digital Operational Resilience Act

The European Union (EU) Digital Operational Resilience Act (Regulation (EU) 2022/2554 - 'DORA') standardizes how financial entities report cybersecurity incidents, test their digital operational resilience, and manage Information and Communications Technology (ICT) third-party risk across the financial services sector and EU member states. By January 17, 2025, EU financial entities and their critical ICT providers must be ready to comply with DORA.

DORA establishes an enhanced set of common requirements for financial entities in the EU to mitigate ICT risks and enhance digital resilience in the European financial system. In particular:

1. DORA contains detailed requirements for financial entities about ICT risk management.
2. DORA consolidates the financial sector incident reporting requirements under a single streamlined framework.
3. Drawing on existing EU initiatives like TIBER-EU, DORA establishes a new EU-wide approach to testing digital operational resilience, including threat-led penetration testing.
4. DORA builds on the strong foundation established by the European Supervisory Authorities' respective outsourcing guidelines by further coordinating ICT third-party risk management requirements across sectors, including the requirements for contracts with ICT providers.

DORA will also allow financial regulators to directly oversee critical ICT providers (including cloud services providers). Designation will be based on a number of factors, including the systemic impact of a failure of the ICT provider's services and the systemic importance of the financial entities that rely on those services. This mechanism will create a direct communication channel between regulators and designated ICT providers via annual engagements, including oversight plans, inspections, and recommendations.

Our compliance page provides customers with the most up to date resources relating to Google Cloud's support for customers' DORA compliance. This includes Google Cloud and Workspace mappings to support customers' risk management.

This Customer Guide focuses on Chapter II of DORA on ICT risk management.

2. Google Cloud's perspective on Operational Resilience

This section explains Google Cloud's point of view on operational resilience in financial services. We fully understand the continuing importance of operational resilience to the financial services sector, and firmly believe that a well-executed migration to Google Cloud can play a part in strengthening it.

What is operational resilience?

DORA defines 'digital operational resilience' as "the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions".

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 localized 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.

Migrating to Google Cloud provides operational resilience benefits

There is a growing recognition among policymakers and industry leaders that, far from creating unnecessary new risk, a well-executed migration to public cloud technologies 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.

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.

Equally important are the Google Cloud products, and our support for hybrid and multi-cloud, that help financial services customers manage various operational risks in a differentiated manner:

- **Cybersecurity that is designed in, and from the ground up.** From encryption by default, to our Titan security chip, to high-scale DOS defenses, to the power of Google Cloud data analytics and Security Command Center our solutions help you secure your environment.
- **Solutions that decouple employees and customers from physical offices and premises.** This includes zero-trust based remote access that removes the need for complex VPNs, and rapidly deployed customer contact center AI virtual agents, and Google Workspace for best-in-class workforce collaboration.
- **Globally and regionally resilient infrastructure, data centers and support.** We offer a global footprint of 40 Regions and 121 Zones, allowing us to serve customers in over 200 countries, with a globally distributed support function so we can support customers even in adverse circumstances. Our data centers are certified as ISO 22301 compliant after undergoing an audit by an independent third party auditor.
- **Strategic autonomy through appropriate controls.** Our recognition that customers and policymakers, particularly in Europe, strive for even greater security and autonomy is embodied in our work on data sovereignty, operational sovereignty, and software sovereignty.
- **Portability, substitutability and survivability, using our open cloud.** We understand that from a financial services firm's perspective, achieving operational resilience may include addressing situations where their third parties are unable, for any reason, to provide the services contracted.
- **Reducing technical debt, whilst focusing on great financial products and services.** We provide a portfolio of solutions so that financial services firms' technology organizations can focus on delivering high-quality services and experiences to customers, and not on operating foundational technologies such as servers, networks and mainframes.

You can learn more about Google Cloud's point of view on operational resilience in financial services in our Strengthening Operational Resilience in Financial Services by Migrating to Google Cloud white paper.

Our Infrastructure Reliability Guide explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations and explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations..

Resilience Testing

Google recognizes the importance of regular testing in the context of operational resilience. We run 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 is a regular, coordinated set of both real and fictitious incidents and outages across the company to test everything from our technical systems to processes and people - we intentionally bring down parts of our production services as part of these exercises. To avoid affecting our customers, we use capacity that is unneeded at the time of the test; if engineers can't find the fix quickly, we'll stop the test before the capacity is needed again.

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. Generally available services are required to have ongoing, active DiRT testing and validation of their resilience and availability.

This blog post provides 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.

Financial entities can also request to review Google Cloud's testing results.

Independent Assurance

Google Cloud recognizes that you expect independent verification of our resilience, security, and compliance controls. We undergo several independent third-party audits on a regular basis to provide this assurance.

In particular, Google's data centers are certified as ISO 22301:2019 (Business Continuity Management Systems) compliant after undergoing an audit by an independent third party auditor. ISO 22301:2019 is an international standard for business continuity management that is designed to help organizations implement, maintain and improve a management system to prevent, prepare for, respond and recover from disruptions when they arise.

You can review Google Cloud's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources. Some of the other key international standards we are audited against are:

- ISO/IEC 27001 (Information Security Management Systems)
- ISO/IEC 27017 (Cloud Security)
- ISO/IEC 27018 (Cloud Privacy)
- PCI DSS
- SOC 1
- SOC 2
- SOC 3

We also participate in sector and country-specific frameworks, such as BSI C5 (Germany). In addition to certifications and audit reports, Google collaborates with third-party risk management (TPRM) providers to support your cloud assessments. TPRM providers perform regular assessments of Google Cloud's platform and services—they inspect hundreds of business continuity, operational resiliency, security and privacy controls aligned with industry standards and regulations such as NIST SP 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, CMMC, SOC2, CSA STAR, and more. Based on their observations

and assessments, TPRM providers develop independent audit reports that can help scale and accelerate your own risk assessment processes. For more information, refer to our Google Cloud risk assessment resources page.

3. How Google Cloud Helps Customers Meet their Risk Management Requirements

DORA Article	How Google Supports DORA Requirements
Governance & Organisation and ICT Risk Management Framework ● Article 5, 6, 16 Put in place an internal governance and control framework, including policies and procedures, that ensures effective and prudent management of ICT operational resilience risk and is subject to internal audit review.	**Governance of ICT operational risk** ● Google Cloud's Risk Governance of Digital Transformation in the Cloud whitepaper can help you understand what a cloud transformation means for risk, compliance, and audit functions, and how to best position those programs for success in the cloud world. ● Google Cloud's Risk Assessment & Critical Asset Discovery solution evaluates your organization's current IT risk, identifies where your critical assets reside, and provides recommendations for improving your security posture and resilience. **ICT control technologies and responsibilities** ● It is important that your organization's control functions re-evaluate ICT controls as they can be substantially different to those used for on-premise technologies. Refer to our Risk Governance of Digital Transformation in the Cloud whitepaper for more information, including about how control design and ownership evolves in the cloud. ● Customers must understand the boundaries of responsibility between your organization and the cloud service provider. Refer to the Consensus Assessment Initiative Questionnaire (CAIQ) response on our Cloud Security Alliance page for more information on the allocations of responsibility.
ICT Systems, Protocols and Tools ● Article 7 Maintain updated ICT systems, protocols and tools that are appropriate for use, reliable, and resilient.	**Migrating to and building in the cloud** ● Google Cloud's Migration to Google Cloud guide and Cloud Architecture Center helps you plan, design, and implement the process of migrating your workloads to Google Cloud to avoid and mitigate reliability, capacity and resiliency risk. In addition, our How to put your company on a path to successful cloud migration whitepaper provides guidance to help with the start of your digital transformation. ● The Google Cloud infrastructure reliability guide describes the building blocks of reliability in Google Cloud (zones, regions, and location-scoped resources) and the availability levels that they provide. This document also provides guidelines for assessing the reliability requirements of your workloads, and presents architectural recommendations for building and managing reliable infrastructure in Google Cloud.

	• Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud. 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.
	
	• Financial entities can use the following functionality to control the use, reliability and resilience of their Services:
	  ○ Cloud Console: A web-based graphical user interface that customers can use to manage their Google Cloud resources.
	  ○ gcloud Command Tool: A tool that provides the primary command-line interface to Google Cloud.
	  ○ Google APIs: Application programming interfaces which provide access to Google Cloud.
	
	Service performance and SLAs
	• Google Cloud gives you tools to monitor Google Cloud's performance of services (including SLAs). The following tools enable you to do so on an ongoing basis:
	  ○ The Service Health Dashboard provides status information on the Services.
	  ○ Personalized Service Health filters disruptive events that are relevant to your projects and includes information to help you assess impact, maintain business continuity, and track updates. You can fit Personalized Service Health into any alert, incident response, or monitoring workflow between the Service Health dashboard, configurable alerts, exportable logs with Cloud Logging.
	  ○ Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services.

Identification • Article 8 Document, inventory and periodically review and assess ICT functions, assets, risks and their internal and external interdependencies.	**Asset inventory and management** • Cloud Asset Inventory allows you to view, monitor, and analyze all your Google Cloud and Anthos assets across projects and services. You can export a snapshot of your entire inventory at any point of time. • Google Cloud provides billing tools that customers can use to obtain reports on their usage of the Services. Refer to our Cloud Billing documentation page and the Export Cloud Billing data to BigQuery page for more information. • Resource Manager allows you to programmatically manage Google Cloud container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud resources. **Risk review and assessment** • Google Cloud provides a 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. ● Google Cloud collaborates with third-party risk management (TPRM) providers to support your due diligence and cloud assessments. Refer to our Google Cloud risk assessment resources page for more information. ● Google Cloud undergoes several independent third-party audits on a regular basis to verify security, privacy, and compliance controls. Refer to our Compliance Resource Center for more information. ● Google Cloud's security tool, Risk Manager, offers insight into your organization's technical risk posture to help you understand where to focus your investments to reduce risk.
Protection and Prevention ● Article 9 Implement security tools that continually monitor and control ICT systems and ensure, but not limited to, privacy, availability, integrity and confidentiality.	For information on how Google Cloud provides customers with transparency and control over their data in Google Cloud, see our Trusting your data with Google Cloud whitepaper. Information on Google's security and identity products is available on our Cloud Security Products page. **Infrastructure security** ● Google Cloud manages the security of our infrastructure (i.e., the hardware, software, networking and facilities that support the services). Detailed information about our infrastructure security can be found in the Resources section of this guide. ● Robust operational resilience measures apply to all Google Cloud facilities. Google Cloud operates multi-zone data centers all over the world, providing resilience in the event of localized or region-wide environmental or infrastructure events. Google Cloud makes the same commitments about all its data centers, regardless of country / region. Refer to our Global Locations page for more information. **Encryption** ● Google Cloud uses encryption to enhance the security of your data and applications in the cloud: ○ Encryption at rest: Google Cloud encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page. ○ Encryption in transit: Google Cloud encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available on the Google Cloud Encryption in transit page. ○ Google Cloud provides customers with tools that facilitate ubiquitous data encryption which delivers unified control over data at-rest, in-use, and in-transit, all with keys that are under your control. ○ Google Cloud also offers a continuum of encryption key management options to meet your requirements for key

	generation, storage, and rotation. More information is available on the Google Cloud Choosing an Encryption Option page. **Access control** ● 2-Step Verification puts an extra barrier between customer's business and cybercriminals who try to steal usernames and passwords to access business data. With 2-Step Verification, customer's users sign in to their account in two steps with something they know (their password) and something they have (their mobile phone with Google OTP installed) ● Identity and Access Management (IAM) can be used to assign roles and permissions to administrative groups, incorporating principles of least privilege and separation of duties. ● VPC Service Controls allow customers to address threats such as data theft, accidental data loss, and excessive access to data stored in Google Cloud multi-tenant services. It enables clients to tightly control what entities can access what services in order to reduce both intentional and unintentional losses. **Data location** ● Google Cloud provides you with choices about where to store your data. Once you choose where to store your data, Google Cloud will not store it outside your chosen region(s). You can also choose to use tools provided by Google Cloud to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. ● To manage concentration risk, you can choose to use GKE Enterprise to build, deploy and optimize your applications in both cloud and on-premises environments. Refer to the IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud for more information. **Data loss and anonymization** ● Google Cloud offers Data Loss Prevention, a service designed to help with discovery, classification, and anonymization of sensitive data via an API that can be used by most applications / services. **Credential management** ● Google Cloud shares best practices to help you manage your Google accounts. In addition, Google Cloud provides tools to help you secure your credentials. For example, Secret Manager is a secure and convenient storage system for API keys, passwords, certificates, and other sensitive data. Secret Manager provides a central place and single source of truth to manage, access, and audit secrets across Google Cloud. In addition, Certificate Authority Services enables you to simplify, automate, and customize the deployment, management, and security of private certificate authorities (CA). Further, Cloud External Key Manager allows you to use keys that you manage within a supported external key management partner to protect

	data within Google Cloud. **Protection from external threats** ● Cloud Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center helps you strengthen your security posture by evaluating your security and data attack surface, providing asset inventory and discovery, identifying misconfigurations, vulnerabilities, and threats, and helping you mitigate and remediate risks.
Detection ● Article 10 Implement mechanisms for prompt detection of anomalous activities and support ICT related incident response.	**Incident Response** ● Our guides on Incident Management and how to Build a collaborative incident management process provide best practices to manage services and define processes to respond to incidents. ● The Google CSH Dashboard keeps a record of disruptions and outages for the Google Cloud products for up to five years. The Overview tab of the dashboard shows the current status of the products by locale. To view information about product disruptions and outages in the last year, click View history on the dashboard. To view a product's outage history for the last five years, click “See more" for that product. ● Personalized Service Health lets you identify Google Cloud service disruptions relevant to your projects so you can manage and respond to them efficiently. These disruptions are called service health events, and are available in the Google Cloud console and a variety of integration points. ● You can use solutions and tools provided by Google Cloud to enhance and monitor the security of your data, including our Cyber Incident Response Service, which includes services on investigation and crisis management and 24/7 incident coverage. **Access Logs** ● Cloud Logging is a fully managed service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud and Amazon Web Services. ● Access Transparency maintains visibility of insider access to your data through near real-time logs. **Detection of Threats** ● Our Autonomic Security Operations (ASO) solution delivers exceptional threat management delivered through a modern, Google Cloud-native stack, and includes deep, rich integrations with third-party tools and a powerful engine to create connective tissue and stitch your defenses together. It enables threat hunting, integrated threat intelligence, and playbook automation through SOAR partnerships to manage incidents from identification to resolution.

	• Virtual Machine Threat Detection is a built-in service of Security Command Center Premium, which provides threat detection through hypervisor-level instrumentation.
	• Event Threat Detection automatically scans various types of logs for suspicious activity in your Google Cloud environment.
	• Cloud Security Scanner automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities.
	
	Monitoring
	• Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud resources and changes to resources including VM instances, images, and operating systems.
	• Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on Google Cloud, including availability and uptime of the services.
	• Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more.
	• You can use Chronicle and VirusTotal to monitor and respond to many types of malware:
	  ○ Google Cloud Threat Intelligence for Chronicle is a team of threat researchers who develop threat intelligence for use with Chronicle.
	  ○ VirusTotal is an online service that analyzes files and URLs to identify viruses, worms, trojans, and other malicious content that's detected by antivirus engines and website scanners. Refer to our security whitepaper for more information.
	  ○ Google Cloud also offers control and monitoring functionality via the Cloud Console.

Response and Recovery **Backup** • Articles 11, 12, 14 Establish, test and maintain business continuity and response and recovery plans, backup systems, and a crisis communication function. Maintain redundant ICT capacities.	**Building resilient and reliable applications** • The Architecting disaster recovery for cloud infrastructure outages article describes how to design applications that are resilient and meet your desired recovery time and recovery point objectives. • The Google Cloud Architecture Framework shows you how to architect and operate reliable services on a cloud platform. The Google Cloud infrastructure reliability guide describes the building blocks of reliability in Google Cloud (zones, regions, and location-scoped resources) and the availability levels that they provide. This document also provides guidelines for assessing the reliability requirements of your workloads, and presents architectural recommendations for building and managing reliable infrastructure in Google Cloud.

	Recovery and backup ● 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. Information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. In addition, customers should refer to our Architecting disaster recovery for cloud infrastructure outages guide. ● Google Cloud offers solutions for customers to design and implement proactive, tactical approaches to ransomware recovery. ● 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 disaster recovery process when it detects a failure and can trigger the appropriate recovery actions. ● Google Cloud has industry-leading 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. ● Customers can also use Google Cloud Back Up and Disaster Recovery to manage backups. Also see the Protection and Prevention and Detection section of this table to learn more about how to protect backup data from unauthorized access. **Testing** ● Refer to this blog post for more information about the disaster recovery and resilience testing that Google Cloud 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. Financial entities can also request to review Google Cloud's testing results. **Data portability and retention** ● Google Cloud enables customers to access and export their data throughout the duration of their contract and during the post-termination transition term. ● You can export your data from a number of Google Cloud services in a number of industry standard formats: For example: ○ Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. ○ GKE Enterprise allows you to move and convert workloads directly into containers in Google Kubernetes Engine.

	○ You can export/import an entire VM image in the form of a .tar archive. Find more information on images here and on storage options here. ○ In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our services. ○ Google Cloud also supports free network data transfers for customers migrating out of Google Cloud. ● Google Cloud provides functionality to delete customer data put into our systems. If customers delete their data, we commit to deleting it from our systems within 180 days. To learn more about data deletion, refer to our Data deletion on Google Cloud whitepaper.
Learning and Evolving ● Article 13 Gather information on vulnerabilities, cyber threats, ICT related incidents, and data that impacts operational resilience. Put in place post ICT incident related reviews and incorporate learnings into the ICT risk management framework.	You can leverage the following Google Cloud resources to supplement your cyber threat information gathering and to evolve your risk management practices. ● Google Cloud's M-Trends report provides an inside look at the evolving cyber threat landscape, with data drawn directly from frontline incident response investigations and threat intelligence findings of high-impact attacks and remediations around the globe. ● Mandiant (now part of Google Cloud) offers Risk Management services including Cyber Risk Management Operations Service, Threat Modeling Security Service, Cyber Security Due Diligence Service, and a Cyber Security Program Assessment.

Conclusion

Google Cloud understands the importance of managing operational risk in maintaining the stability of the financial system and the need for the right regulatory frameworks in this space. We are committed to helping our customers achieve their operational resilience goals and to working with policymakers and regulators to develop and implement appropriate 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.

As we approach January 17, 2025, Google Cloud continues to focus on operational resilience, security, and compliance controls to support customers' DORA compliance.

This includes offering tools and solutions designed to address our customers' requirements under DORA in a manner that best positions the financial services sector in all aspects of operational resilience.

Resources

The below guides and whitepapers are provided as support and guidance to help facilitate customers' compliance with DORA using Google Cloud.

Risk Management
Risk Governance of Digital Transformation in the Cloud
IDC Whitepaper on How A Multicloud Strategy Can Help Regulated Organizations Mitigate Risks In Cloud
Board of Directors Handbook for Cloud Risk Governance

Compliance
Cloud compliance
Compliance Reports Manager
Assuring Compliance in the Cloud

Security
Security overview
Security and IAM resources
Security Resources Hub
Trusted infrastructure page
Google security overview
Google Workspace security whitepaper
Infrastructure security design overview

Architecture
Cloud Architecture Center
Architecture fundamentals

Resilience
Strengthening Operational Resilience in Financial Services by Migrating to Google Cloud
Reliability and disaster recovery resources
Cloud infrastructure reliability guide
Disaster Recovery Scenarios for Data
Disaster Recovery for Applications
Planning for the Worst whitepaper

Incidents and Cyber Threats
Data incident response process
Threat Detection, Investigation, and Response in the Cloud
Trusting your data with Google Cloud whitepaper
Trusting your data with Google Workspace whitepaper
Build a collaborative incident management process

Data Protection
Data residency, operational transparency, and privacy for European customers on Google Cloud
Data deletion on Google Cloud whitepaper

Migration
Hybrid and multicloud resources
Migrate to Google Cloud
How to put your company on a path to successful cloud migration