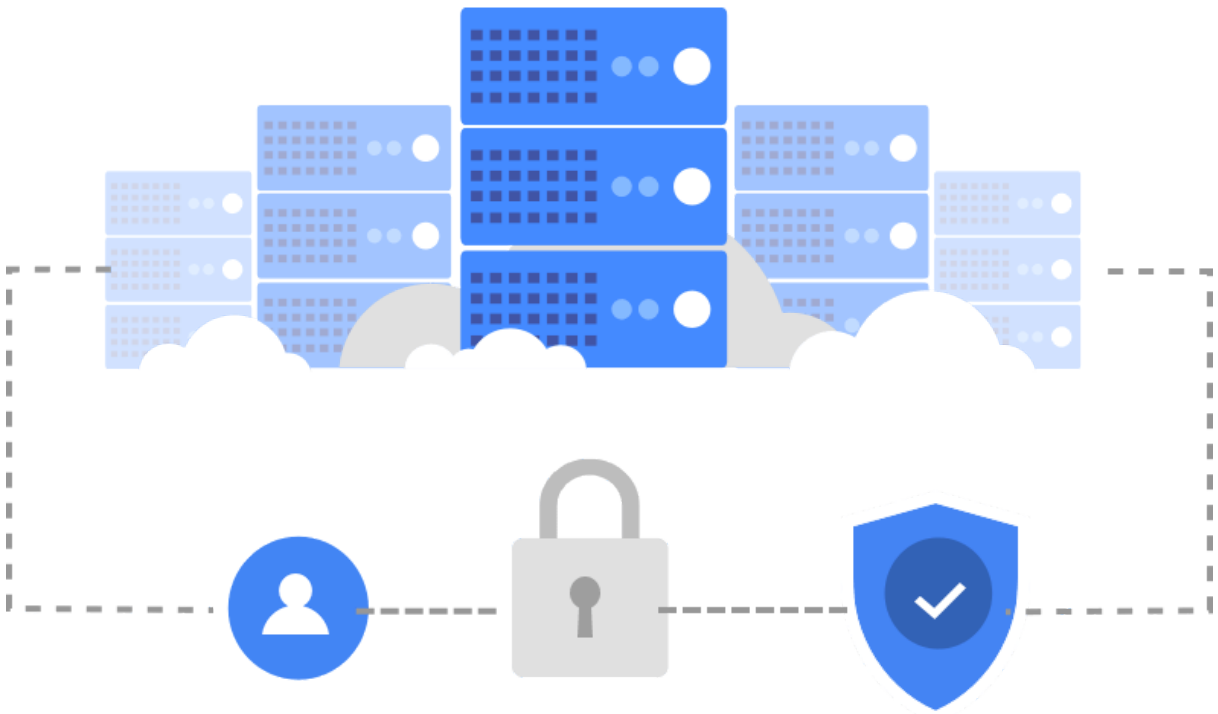
Google Cloud FAQ
January 2023

EU DORA
Google Cloud Customer Guide



Overview

The EU Digital Operational Resilience Act (DORA) is a new regulation that aims to improve information and communications technology (ICT) and security risk management requirements. Its objective is to ensure a common set of standards to mitigate ICT risks and enhance digital resilience in the European financial system.

DORA creates new obligations for financial entities in the EU across a wide range of topics, including incident management, operational resilience testing, and third party risk management. DORA also introduces a new framework for direct oversight of critical ICT service providers by financial regulators in the EU. Where the criteria are met, this would apply to cloud service providers like Google Cloud.

DORA will go into effect on 17 January 2025.

Google Cloud firmly believes that DORA will be crucial to the acceleration of digital innovation in the European financial services sector. It creates a solid framework to enhance understanding, transparency, and trust among ICT providers, financial entities, and financial regulators.

Here are a few key benefits of DORA:

- **Coordinated ICT incident reporting:** DORA consolidates financial sector incident reporting requirements under a single streamlined framework. This means financial entities operating in multiple sectors or EU member states should no longer need to navigate parallel, overlapping reporting regimes during what is necessarily a time-sensitive situation. DORA also aims to address parallel incident reporting regimes like NIS2. Together these changes help get regulators the information they need while also allowing financial entities to focus on other critical aspects of incident response.
- **New framework for digital operational resilience testing:** 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. By clarifying testing methodology and introducing mutual recognition of testing results, DORA will help financial entities continue to build and scale their testing capabilities in a way that works throughout the EU. Importantly, DORA addresses the role of the ICT provider in testing and permits pooled testing to manage the impact of testing on multi-tenant services like public clouds.
- **Coordinated ICT third party risk management:** 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. By helping to ensure that similar risks are addressed consistently across sectors and EU member states, DORA will enable financial entities to consolidate and enhance their ICT third-party risk management programs.
- **Direct oversight of critical ICT providers:** DORA will allow financial regulators to directly oversee critical ICT providers. This mechanism will create a direct communication channel between regulators and designated ICT providers via annual engagements, including oversight plans, inspections, and recommendations. We're confident that this structured dialogue will help to improve risk management and resilience across the sector.

While this customer guide provides information on the tools and resources offered by Google Cloud, please note that, as a provider of cloud services, we are not in a position to provide our customers with legal advice - that is something only legal counsel can provide.

Frequently Asked Questions

What is the Digital Operational Resilience Act (DORA)?

DORA is a new EU regulation. It will apply across the financial services sector in all EU member states. DORA updates existing rules and establishes an enhanced set of common requirements to mitigate ICT risks and enhance digital resilience in the European financial system. Importantly, DORA also introduces a new framework for direct oversight of critical ICT service providers by financial regulators in the EU.

What are the key requirements under 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. This mechanism will create a direct communication channel between regulators and designated ICT providers via annual engagements, including oversight plans, inspections, and recommendations.

Which organisations does DORA apply to?

DORA primarily applies to financial entities in the EU. However, part of DORA applies directly to ICT providers (including cloud services providers) who are designated "critical" by financial regulators in the EU following an official process. 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.

Does DORA apply to Google Cloud?

Like previous ICT risk management requirements, DORA contains requirements about how financial entities in the EU should manage their ICT providers (including cloud services providers). Though these requirements don't apply to ICT providers directly, Google Cloud recognises that we will need to enable our customers to address these expectations comprehensively to ensure their continued success whilst using our services.

Although DORA will not apply to Google Cloud directly unless and until an official designation as a critical ICT provider by EU regulators, we are already preparing to address potential direct requirements and intend to engage openly with regulators about designation.

What is the implementation deadline for DORA?

DORA will take effect on 17 January 2025 (2 years and 20 days after it was published in the Official Journal of the EU).

DORA only applies directly to critical ICT providers after they are designated "critical" by financial regulators in the EU. Therefore, the deadline for compliance for critical ICT providers depends on the timing of designation. Although DORA will not apply to Google Cloud directly unless and until an official designation, we are already preparing to address potential direct requirements.

How is Google Cloud preparing for DORA?

We have been engaging with the policymakers on the DORA proposal since it was tabled in September 2020. In parallel we set up a readiness program to analyse potential customer expectations and our own responsibilities as DORA evolved during the legislative process.

Now that the text of DORA is finalised, a cross-functional team at Google Cloud (including subject matter experts from Risk & Compliance, Security, Legal, Government Affairs and Product) is reviewing the details and preparing compliance plans where needed. These plans build upon our strong foundation in areas like security, resilience and third party risk management that already enable our customers to address the rigorous expectations under the EBA outsourcing guidelines, the EIOPA cloud outsourcing guidelines, the ESMA cloud outsourcing guidelines.

We intend to use the implementation period to further enhance our capabilities in each of the DORA focus areas. Our goal is to make Google Cloud the best possible service for sustainable, digital transformation for European organisations on their terms.

What are Google Cloud's key areas of focus / development under DORA?

In addition to preparing for potential designation as a critical ICT provider, Google Cloud is focused on a number of the new or updated operational requirements under DORA for financial

entities using our services. In particular, we are focused on how we can support customers with the phased incident reporting and threat led penetration testing. As a lot of the detail in these areas is still to be developed under Regulatory Technical Standards and Implementing Technical Standards contemplated by DORA, we are following those discussions closely.

What is Google Cloud's opinion of direct regulatory oversight of critical ICT providers under DORA?

The oversight framework for critical ICT providers under DORA creates a genuine opportunity to enhance understanding, transparency, and trust among ICT providers, financial entities, and financial regulators, and ultimately stimulate innovation in the financial sector in Europe. DORA will create a direct communication channel between regulators and designated ICT providers via annual engagements, including oversight plans, inspections, and recommendations. We're confident that this structured dialogue will help to improve risk management and resilience across the sector.

Is Google Cloud ready for direct regulatory oversight under DORA?

Google Cloud is committed to enabling regulators to effectively supervise a financial entity's use of our services. We grant information, audit and access rights to financial entities, their regulators and their appointees, and support our customers when they or their regulators choose to exercise those rights. We would approach a relationship with a Lead Overseer with the same commitment to ongoing transparency, collaboration, and assurance.

Though we are very focused on planning for direct requirements, how regulatory oversight will work in practice still needs to be defined in more detail in the regulatory technical standards contemplated by DORA and during the designation process.

Will Google Cloud update its contracts with financial entities in the EU because of DORA?

Google Cloud's contracts for financial entities in the EU already address the contractual requirements in the EBA outsourcing guidelines, the EIOPA cloud outsourcing guidelines, the ESMA cloud outsourcing guidelines, and other member state requirements. We recognise that DORA also contains requirements for contracts with ICT providers. We are reviewing these closely to understand the changes we may need to introduce to our contracts for financial entities under DORA. Before we can finalise any changes and discuss them with customers, we are waiting to see how the European Supervisory Authorities will address requirements in their outsourcing guidelines that now overlap with DORA requirements. We are following those discussions closely.

How is Google Cloud engaging in countries outside the EU where legislators are considering proposals similar to DORA?

We engage on financial services sector policy developments that significantly impact Google Cloud and our customers' use of our services globally.

Where policymakers are considering an approach similar to DORA, they often first consider how that approach fits into the existing local regulatory framework, including any perceived areas for improvement. The European Commission consulted on this issue in 2020 before proposing the initial DORA draft.

Where policymakers have confirmed the need for a different (and potentially direct) regulatory approach, we engage to share our technological expertise vis-a-vis cloud services and consistently advocate for:

- harmonisation and deduplication of requirements (both within and between countries)
- requirements that are proportionate and fit-for-purpose
- a technology neutral approach that encourages innovation
- an approach that respects the security and integrity of our services for all our customers

The UK is an example of another country currently considering a direct regulatory framework for critical third party providers to the financial sector. We are engaging on the Discussion Paper based on the principles above.

It is important to keep in mind that DORA is not the only regulation that would apply to cloud providers in Europe. The NISD2 Directive will also introduce sector-agnostic supervision for critical third parties, and there are many national requirements that apply to cloud services in regulated industries.

Cloud adoption in financial services is still new, and forthcoming regulation needs to stimulate this type of innovation. Different countries will take different approaches to ensuring security and operational resilience of the financial services ecosystem, and direct regulation or oversight is not the only solution that fits different markets. We understand that regulators in other jurisdictions are equally focused on standards, horizontal rules and self-regulatory practices. Whichever approach policymakers take, it is important to ensure regulatory consistency and harmonisation of the applied principles across the board as they impact global technology players and the cross-border digital finance ecosystem.