EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

This document is designed to help EU financial entities (“**regulated entity**”) to consider the EU Digital Operational Resilience Act (“**framework**”) in the context of Google Workspace and the Google Cloud Financial Services Contract.. References to the Google Cloud Financial Services Contract in this document refer to the version updated to address DORA. If you need the updated version, please contact your Google Cloud representative.

We focus on the following requirements of the framework: Article 30 (Key contractual provisions). For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
1	1. The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall include the service level agreements and be documented in one written document which shall be available to the parties on paper, or in a document with another downloadable, durable and accessible format.	Rights and obligations The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract. The Google Cloud Financial Services Contract consists of the Order Form, General Terms, and the Google Workspace Services Schedule. Where the Google Workspace Services Schedule does not already incorporate the relevant language, Google also provides a Financial Services Addendum. The Google Workspace Services Schedule incorporates certain URL Terms, including the AUP, Cloud Data Processing Addendum, Google Workspace Service Specific Terms, Google Workspace Technical Support Services Guidelines, and SLAs. Format One of the key benefits of a public cloud service is that the service improves as technology evolves. To ensure customers benefit from these improvements, the Google Cloud Financial Services Contract must also evolve over time. This is not possible if the contract is documented in a static paper document. Instead, the Google Cloud Financial Services Contract is available in a downloadable, durable and accessible format. • The Order Form, the General Terms, the Google Workspace Services Schedule and (if applicable) the Financial Services Addendum are executed by Google and the customer and are available as PDFs, which customers can download and access at any time. Any changes to these documents must be made in writing and executed by both parties. • The URL Terms are available online at at g.co/cloud/workspace-directory-terms. Customers can access and download the content of these URLs at any time (e.g. by converting them to PDFs). As services and technology change, Google may update certain terms at URLs that apply to all our customers. Any updates must meet strict criteria. For example, they must not result in a material degradation of the overall security of the services or have a material adverse impact on your existing rights. To provide durability, Google will notify customers	Services Changes to Terms; Amendments

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		of any material changes to the URL Terms and such changes will only take effect 30 days after notice is received. Customers can access and download previous versions of the URL Terms at any time at the relevant URL.	
2	2. The contractual arrangements on the use of ICT services shall include at least the following elements:		
3	(a) a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;	Service Description The Google Workspace Services are described on our services summary page. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement. Subcontracting Google recognizes that regulated entities need to consider the risks associated with subcontracting. To ensure regulated entities retain oversight of any subcontracting, Google will comply with clear conditions designed to provide transparency and choice. In particular, Google will: • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give regulated entities the ability to terminate if they have concerns about a new subcontractor.	Definitions Subcontracting; Google Subcontractors

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
4	(b) the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity in advance if it envisages changing such locations;	To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities. -Information about the location of Google's facilities and where individual Google Workspace services can be deployed is available on our Global Locations page. -Information about the location of Google's subprocessors' facilities is available on our Google Workspace and Cloud Identity Subprocessors page. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular: -The same robust security measures apply to all Google facilities, regardless of country / region. -Google makes the same commitments about all its subprocessors, regardless of country / region. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Trusting your data Google Workspace whitepaper.	Data Transfers (Cloud Data Processing Addendum) Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms)
5	(c) provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;	Availability The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Workspace Service Level Agreement page. Authenticity, integrity and confidentiality This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The security / confidentiality of a cloud service consists of two key elements:	Services

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		(1) Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: Our infrastructure security page Our security whitepaper Our cloud-native security whitepaper Our infrastructure security design overview page Our security resources page In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security by default Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you:	Data Security; Google's Security Measures (Cloud Data Processing Addendum)

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		Encryption at rest. Google encrypts certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. For more information on Google Workspace encryption and key management tools provided by Google, see our Google Workspace encryption whitepaper. Encryption in transit. Google encrypts all data while it is "in transit"--traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data, at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. For more information on Google Workspace encryption and key management tools provided by Google, see our Google Workspace encryption whitepaper. (b) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Google Workspace security and data protection page. (c) Security resources Google also publishes guidance on: Security best practices Security use cases Security checklists	
6	(d) provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;	You retain all intellectual property rights in your data. Google will enable you to access and export your data throughout the duration of our contract and the transition term. You can export your data from the Services in a number	Intellectual Property Data Export (Cloud Data Processing Addendum)

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		of industry standard formats. More information is available on our Google Account help page. In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Services. Neither of these commitments are disapplied on Google's insolvency. Nor does Google have the right to terminate for Google's own insolvency - although you can elect to terminate. In the unlikely event of Google's insolvency, you can refer to these commitments when dealing with the appointed insolvency practitioner. Refer to Rows 22 to 24 on exit planning.	Term and Termination
7	(e) service level descriptions, including updates and revisions thereof;	The SLAs provide measurable performance standards for the services and are available on our Google Workspace Service Level Agreements page. Google may update certain terms at URLs that apply to all our customers, including the SLAs. Any updates must meet strict criteria. For example, they must not result in a material degradation of the overall security of the services or have a material adverse impact on your existing rights. Google will notify customers of any material changes to the URL Terms and such changes will only take effect 30 days after notice is received. Customers can access and download previous versions of the URL Terms at any time at the relevant URL.	Services Changes to Terms
8	(f) the obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs;	Google will assist regulated entities with ICT incidents that are related to our services as follows: 1. Google will notify you of ICT incidents promptly and without undue delay. Google's notification will describe: ● the nature of the incident including the Customer resources impacted; ● the measures Google has taken, or plans to take, to address the incident and mitigate its potential risk; ● the measures, if any, Google recommends that Customer take to address the incident; and ● details of a contact point where more information can be obtained.	ICT Incidents

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		2. Google will take steps to minimize harm and secure the impacted Google network and information systems. More information on Google's incident response process is available in our Incident Response whitepaper. Google will provide the assistance above at no additional cost beyond the agreed fees for Technical Support Services. In addition to the other tools and practices available to you outside Google, you can choose to use solutions and tools provided by Google to enhance and monitor the security of your data. Our Google Workspace security center provides advanced security information and analytics, and added visibility and control into security issues affecting your domain. The security center expands on advanced settings in the Google Admin console to surface your security data.	
9	(g) the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them;	Google will fully cooperate with supervisory authorities, resolution authorities and their appointees exercising their information, audit and access rights.	Enabling Customer Compliance
10	(h) termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities;	Regulated entities can terminate our contract with advance notice: ● for Google's material breach after a cure period; ● for change of control; and ● for Google's insolvency. Regulated entities can elect to terminate our contract for convenience with advance notice, including: ● if necessary to comply with law, including the grounds in DORA Article 28(7); and ● if directed by a supervisory authority.	Term and Termination; Termination by Customer
11	(i) the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6).	Regulated entities may request Google personnel whose roles require interaction with Customer ICT systems, protocols and tools to participate in their ICT security awareness programmes and digital operational resilience training. However, it is important to note that customers operate the services independently without action by Google personnel. Although Google personnel manage and maintain	Customer Security Training

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		the hardware, software, networking and facilities that support the Services, given the one-to-many nature of the services, there are no Google personnel dedicated to delivering the services to an individual customer other than in the implementation services context.	
12	3. The contractual arrangements on the use of ICT services supporting critical or important functions shall include, in addition to the elements referred to in paragraph 2, at least the following:		
13	(a) full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met;	The SLAs provide measurable performance standards for the services and are available on our Google Workspace Service Level Agreement page. Google may update certain terms at URLs that apply to all our customers, including the SLAs. Any updates must meet strict criteria. For example, they must not result in a material degradation of the overall security of the services or have a material adverse impact on your existing rights. Google will notify customers of any material changes to the URL Terms and such changes will only take effect 30 days after notice is received. Customers can access and download previous versions of the URL Terms at any time at the relevant URL. You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services. For example: Status Dashboard provides status information 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. Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	Services Changes to Terms Ongoing Performance Monitoring
14	(b) notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material	Google recognizes that to effectively manage your use of the Services you need	Significant Developments

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
	impact on the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels;	sufficient information about the Services on a regular basis. We provide a number of mechanisms to assist you to effectively oversee the Services on an ongoing basis. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Google Workspace Status dashboard page. In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	
15	(c) requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework;	Business contingency plans Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results. Google's data centers are certified as ISO 22301 compliant after undergoing an audit by an independent third party auditor. More information on the reliability of the Services is available on our Google Cloud Help page. Security This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security.	Business Continuity and Disaster Recovery Data Security; Google's Security Measures; Customer's Security Assessment (Cloud Data Processing Addendum)
16	(d) the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27;	You can perform penetration testing of the Services at any time without Google's prior approval or participation. Given the one-to-many nature of public cloud services, TLPT by a regulated entity of the services may have an adverse impact on the quality or security of the services that Google provides to other customers. If a regulated entity requires Google's participation in TLPT, then Google will participate and cooperate in such TLPT by engaging an external tester to perform pooled testing in accordance with DORA Article 26(4).	Customer Penetration Testing Pooled Threat-Led Penetration Testing
17	(e) the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following:	You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.	Ongoing Performance Monitoring

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		For example: Status Dashboard provides status information 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. Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	
18	(i) unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;	Google recognizes that regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants access, inspection and audit rights to regulated entities, supervisory authorities, and both their appointees. This includes the ability to take copies of relevant documentation if it is critical to Google's operations for providing the Services. Nothing in our contract is intended to limit or impede a regulated entity's or the supervisory authority's ability to audit our services effectively.	Regulator Information, Audit and Access; Customer Information, Audit and Access Enabling Customer Compliance
19	(ii) the right to agree on alternative assurance levels if other clients' rights are affected;	If information, audit and access rights affect the rights of Google's other customers, then Google and the regulated entity may agree alternate assurance methods.	Arrangements
20	(iii) the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and	Google will fully cooperate with supervisory authorities, resolution authorities and their appointees exercising their information, audit and access rights.	Enabling Customer Compliance; Google's DORA Compliance
21	(iv) the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;	Scope and Frequency The regulated entity is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit regulated entities to a fixed number of audits or a pre-defined scope. Procedures Reasonable notice enables Google to deliver an effective audit. For example, we can ensure the relevant Google experts are available and prepared to make the most of your time. Notice also enables Google to plan the audit so that it does not create undue risk to your environment or that of any other Google customer.	Customer Information, Audit and Access Arrangements

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		It is extremely important to Google that what we do with one customer should not put any other customers at risk. This applies when you perform an audit. It also applies when any other customer performs an audit. When a regulated entity performs an audit we will work with them to minimize the disruption to our other customers. Just as we will work with another auditing customer to minimize the disruption to the regulated entity. In particular, we will be careful to comply with our security commitments at all times.	
22	(f) exit strategies, in particular the establishment of a mandatory adequate transition period:	Google Cloud is committed to addressing customers' needs for portability and interoperability, and promoting openness to drive innovation. We provide organizations with tools to view, delete, download, and transfer their content. Cloud customers fully control their data and have the ability to take it out of Google Workspace and Google Cloud should they decide to switch to other platforms and/or store and process it on their own premises. Google believes in an open cloud that supports multi-cloud and hybrid cloud approaches. If implemented through the use of open-source based technologies, these approaches can provide customers with the levels of portability, substitutability and survivability, required for robust exit planning. Refer to our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper for more information.	Data Export (Cloud Data Processing Addendum)
23	(i) during which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring;	Transition Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. To help regulated entities achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract. Our Services enable you to transfer your data independently. You do not need Google's permission to do this. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services. Resolution Google recognizes that regulated entities and any resolution entity must be able to carry	Transition Term Transition Assistance

EU - Digital Operational Resilience Act (DORA)

Google Workspace Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		on business during resolution. To provide support through resolution, Google commits to continue providing the Services during resolution.	Support through Resolution
24	(ii) allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.	See above	N/A
25	By way of derogation from point (e), the ICT third-party service provider and the financial entity that is a microenterprise may agree that the financial entity's rights of access, inspection and audit can be delegated to an independent third party, appointed by the ICT third-party service provider, and that the financial entity is able to request information and assurance on the ICT third-party service provider's performance from the third party at any time.	Google recognizes that you expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Google commits to comply with the following key international standards during the term of our contract with you: -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -SOC 1 -SOC 2 -SOC 3 You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports