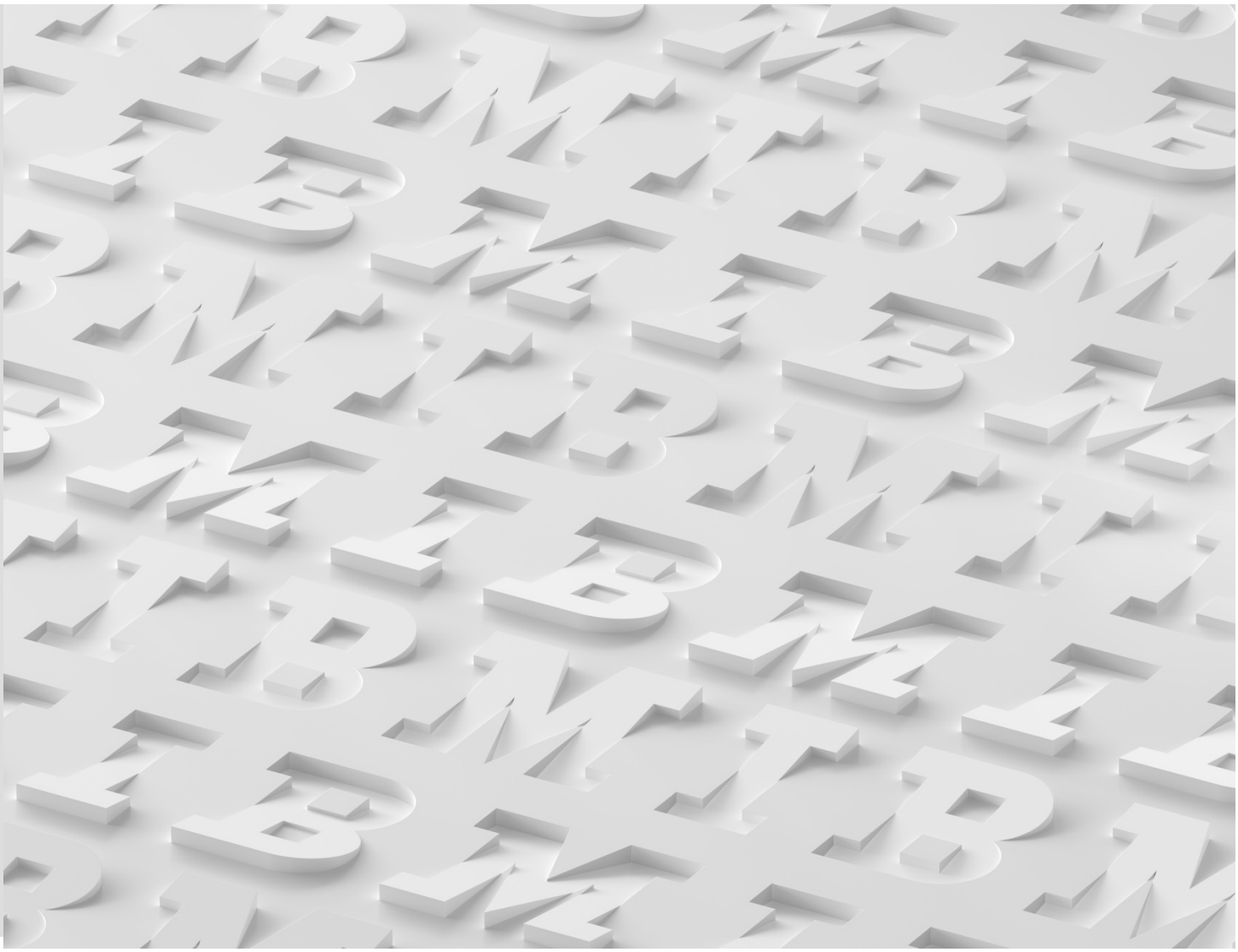

IBM Cloud support for DORA

Whitepaper on IBM Cloud support
for customers and partners for the
EU Digital Operational Resilience Act (DORA)

IBM

Disclosures

This document is provided for informational purposes only. IBM is committed to helping our clients and prospects with the knowledge to enable them to make decisions regarding the needs of their own client base.

The intended audience for this guide is legal and compliance experts seeking to understand the EU Digital Operational Resilience Act, or DORA and how IBM can support clients in their compliance journey. IBM Clients remain fully responsible for their own compliance with any applicable laws or regulations including DORA.

Table of contents

Introduction to EU DORA

Increased digitization and interconnectedness have enabled remarkable scale, speed, and cost efficiencies for businesses. However, the same technology can cause business disruptions. When disruption occurs in critical industries such as financial services, the results could be catastrophic– economic challenges, social unrest, and geopolitical upheaval – thus driving the increased regulations around digital operational resiliency.

The EU Digital Operational Resilience Act, or DORA, is a European Union (EU) regulation that creates a binding, comprehensive information and communication technology (ICT) risk-management framework for the EU financial services sector.

DORA has two main objectives:

- to comprehensively address ICT risk management in the financial services sector and
- to harmonize the ICT risk management regulations that already exist in individual EU member states.

DORA obligations are supplemented by Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS).

Financial Entities as defined by DORA (“FE”s) are required to comply with DORA by January 17, 2025. Enforcement will be handled by designated regulators in each EU member state, called “competent authorities” that mandate security measures and can impose penalties, including administrative and criminal, for non-compliance. Each state will set its own penalties.

Financial entities and their critical technology service providers are required to demonstrate that they can withstand, respond to, and recover from disruptions

DORA compliance deadline: 17 Jan 2025

The European Supervisory Authorities (ESAs) provide oversight of the EU financial system, including The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA).

The ESAs will designate the critical ICT third-party providers in scope of oversight. ICT providers deemed "critical" by the European Commission will be directly supervised by Lead Overseers from the ESAs.

DORA Requirements

DORA establishes technical requirements for financial entities across following domains:

- ICT risk management and governance
- Incident response and reporting
- Digital operational resilience testing
- Third-party risk management
- Information sharing is encouraged but not required.

ICT risk management and governance

The management body of Financial Entities (FEs) has the ultimate responsibility of managing and controlling the firm's ICT risk. Covered FEs are expected to develop comprehensive ICT risk management frameworks, map their ICT systems, identify, and classify critical assets and functions, and document dependencies between assets, systems, processes, and providers. FEs must conduct continuous risk assessments on their ICT systems, document and classify cyberthreats, and mitigation measures. FEs are required to maintain a register of information about contractual arrangements with third-party ICT service providers, conduct pre-contract due diligence and align its contractual provisions accordingly. FEs will also need to establish business continuity and disaster recovery plans.

RTSs specify the required elements of an entity's risk management framework, including design, procurement and implementation of ICT security policies, procedures, protocols and tools for areas such as ICT Risk Management, ICT Asset Management, Encryption and Cryptography, ICT Operations Security, Network Security, ICT Project and Change Management, Physical and Environmental Security.

Incident response and reporting

FEs are required to establish systems for monitoring, managing, logging, classifying, and reporting ICT-related incidents. As per the latest Regulatory Technical Standard (RTS) on major incidents, 'critical services affected' is treated as a mandatory condition for classifying a major incident and where either one of the following conditions is met:

- identification of any malicious unauthorized access to network and information systems or
- the materiality thresholds classification.

Depending on the severity of the incident, entities may need to make reports to both regulators and affected clients and partners. Entities will be required to file three different kinds of reports for critical incidents: an initial notification within 4 hours from the classification of the incident but no later than 24 hours

- an intermediate report at the latest within 72 hours from the submission of the initial report
- the final report within one month after the submission of the intermediate report

Reports from EU banks under the Single Supervisory Mechanism (SSM) show that the number of cyber incidents affecting financial institutions increased by around 78% in 2023, compared with previous years.

Source: 13th Annual Report of the European Systemic Risk Board (ESRB), covering the period between 1 April 2023 and 31 March 2024.

Digital operational resilience testing

FEs are required to test their ICT systems regularly to evaluate the strength of their protections and identify vulnerabilities. The results of these tests, and plans for addressing any weaknesses, need to be reported to, and validated by the relevant competent authorities.

FEs must carry out basic tests, like vulnerability assessments and scenario-based testing, once a year. FEs deemed as critical to the financial system will also be required to conduct advanced threat-led penetration testing (TLPT) every three years. DORA allows for the use of either internal or external testers to conduct the tests. External testers being required for every third TLPT.

The technical standards on TLPTs are aligned with the TIBER-EU framework for threat intelligence-based ethical red-teaming. The active red teaming test must be a minimum of 12 weeks. Purple teaming, a collaborative testing activity that involves both the red team (the testers) and the blue team (the staff from the attacked financial entity) is made mandatory in the closure phase.

DORA allows EU Member States to designate a single public authority - who is then charged with all tasks and responsibilities related to TLPT in that Member State. DORA allows for:

- Joint testing – meant for multiple FEs that belong to the same group and use shared ICT systems
- Pooled testing - meant for multiple, possibly unrelated, financial entries and their external ICT third party provider (TPPs) will directly procure an external tester, but only if it is reasonably expected that the non-pooled test has an adverse impact on the quality or security of services delivered by the ICT third- party service provider, or the confidentiality of the data.

The TLPT authority will issue an attestation that the TLPT was carried out in accordance with this regulation, identifying which critical or important functions were in scope of the TLPT.

Third-party risk management

FEs are expected to play an active role in managing ICT third-party risk. When outsourcing critical or important functions, FEs must include specific contractual arrangements regarding exit strategies, audits and performance targets for service levels and security, among other things. FEs The competent authorities are empowered to suspend or terminate contracts that don't comply. A further step that DORA takes with respect to managing ICT third-party risk, is the designation of ICT third-party service providers as critical by the ESAs. Critical ICT third-party service providers based within or outside of the EU, will be subject to direct oversight from the ESAs, with one of the ESAs acting as the Lead Overseer for each individual ICT third-party service provider.

Financial institutions will also need to map their third-party ICT dependencies, and they'll be required to ensure their critical and important functions are not too heavily concentrated with a single provider or small group of providers.

Information sharing

DORA encourages financial entities to participate in voluntary threat intelligence sharing arrangements. Any information shared this way must still be protected under the relevant guidelines—for instance, personally identifiable information is still subject to General Data Protection Regulation (GDPR) considerations.

IBM Cloud's preparedness for DORA

IBM Cloud is committed to support our clients to strengthen their digital operational resilience in face of disruptions, and to help prepare them to meet their DORA obligations.

With our long history and deep expertise working with some of the world's most well-known financial services organizations on their journey to modernization, IBM is committed to supporting our customers drive growth while reducing risk and adapting to the evolving regulatory landscape, including compliance with DORA.

As a Cloud service provider, there are two ways DORA impacts IBM Cloud:

- indirectly, where both IBM and our FE clients will require actions like revising policies, processes, procedures and tools to manage the security (and the reliability) of ICT systems, as well as the content and overall handling of contractual agreements, both between clients and IBM, and between IBM and our Suppliers.
- directly, in the event IBM and IBM Cloud could be designated as a critical ICT third-party service provider (CTPP), requiring oversight, pursuant to DORA, where providing ICT services to FE customers.

IBM has not been officially designated as a critical ICT provider by regulators. However, IBM Cloud is proactively preparing to address potential direct requirements, in the event that IBM is designated as a critical third-party provider (CTTP) by the regulatory authorities.

IBM Cloud's progress on DORA

Operational Resilience Testing
Enabled customers with access to relevant resiliency testing documentation.

Incident Management
IBM has robust incident management processes to monitor, log, and classify ICT-related incidents, which are aligned with applicable DORA requirements.

Threat-Led Penetration Testing
IBM commits to participating in FE's Threat-Led Penetration Testing (TLPT) in accordance with DORA requirements.

Supply Chain Risk Management
Identified list of critical suppliers and managing related risks.

Client-Initiated Audits
Created a centralized hub to address DORA-related customer queries and requests for audits.

Contract Management
IBM will execute Client and Supplier addendums with the required obligations for CSPs and flow-down obligations to critical suppliers.

Regulatory Interface
Have a dedicated office to manage interactions with the regulators, in the event IBM gets designated as a critical third party.

DORA Article 30 mapping to IBM capabilities

The focus of this table is on Article 30 of DORA, which mandates contractual obligations FEs are required to have in place with their ICT third party service providers for the provision of ICT services. Relevant IBM offerings have been mapped to corresponding DORA requirements, these services are available for client use upon subscription.

DORA Article No.	DORA Requirements	IBM Capabilities
30.1	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.	IBM's DORA Addendum applies if and to the extent IBM Services are Information and Communication Technology (ICT) Services ("ICT Services") as defined by the European Digital Operational Resilience Act (EU 2022/2554) ("DORA") and the Client is a financial entity as defined by DORA and subject to DORA's requirements. IBM contractual documents are available in IBM Terms site. This Cloud Services Agreement (CSA), its Appendix, applicable Attachments and Transaction Documents are the complete agreement under which Client may order Cloud Services from IBM legal entities per Country. Transaction Documents (TDs) provide the specifics of the contract such as, charges, description and information about the Cloud Services.
30.2	The contractual arrangements on the use of ICT services shall include at least the following elements:	
30.2.(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	The full description of IBM public cloud products are available via the Service Description (SD) and the Data Processing Addendum (DPA) Exhibit. The two documents must be used together to understand the complete descriptions of services. All IBM Cloud service descriptions are available in IBM Terms site > Cloud Services > Service descriptions > IBM Cloud SDs. The subcontracting of ICT Services, including ICT Services supporting Critical or Important Functions, or material parts thereof, is permitted. Any subcontractors used to deliver a particular Cloud service will be documented within the IBM Cloud SDs. IBM maintains formal agreements with its subcontractors.

		IBM has a corporate Third-Party Supplier Risk Management (TPSRM) program to provide oversight of subcontractors. It includes a risk assessment of the subcontractor covering both organizational risks associated with the subcontractor and service risks associated with any third-party service being consumed by IBM Cloud. Subcontractor relationships and processes are reviewed by an independent auditor as part of SOC2 compliance audit.
30.2.(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	IBM maintains a list of countries where it provides the ICT Services and where Client data may be processed, including the storage location. This information is described in the applicable DPA Exhibits/Datasheets or the applicable Transaction Document. IBM shall notify Client in advance of changing such locations via a self-service notification portal. IBM Cloud Global Data Centers are deployed locally and scale globally. Built for local access, low latency and certified security, IBM Cloud® offers a range of choices about where and how clients can run workloads and store data. The availability zone design can make applications and databases highly available, fault tolerant and scalable.
30.2.(c)	provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data	Provisions on availability, authenticity, integrity and confidentiality in relation to the protection of Client data including personal data are in IBM's Data Security and Privacy Principles (DSP). The Security and Privacy Principles (DSP) apply to generally available standard IBM Cloud Services and other Services. Specific security features and functions of an IBM Cloud Service or other Services will be described in the applicable Transaction Document. IBM® Confidential computing solutions offer FEs, upon subscription, with technical assurance achieving total data privacy assurance, even while systems and cloud administrators continue to manage the infrastructure without having access to the data.

30.2.(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;	IBM Cloud enables FE access and export its data in industry standard format throughout the duration of the contract and during the transition phase upon contract termination. IBM Cloud ensures data is in easily accessible format by using open standards as described here: https://www.ibm.com/cloud/open Data protection while in transit is offered, upon subscription, by the use of quantum-safe TLS mode in IBM Cloud Key Protect
30.2.(e)	service level descriptions, including updates and revisions thereof;	IBM Cloud® aims to deliver the highest levels of availability and offers a service level agreement (SLA).For more information, see IBM Cloud Service Level Agreements.
30.2.(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	IBM Cloud's incident response plan was developed on the foundation of NIST 800-53 with special consideration of other relevant standards, such as ISO 27001. IBM will investigate ICT incidents of which IBM becomes aware, and, within the scope of the IBM Services, IBM will define and execute an appropriate response plan. IBM Cloud will notify the client without undue delay upon confirmation of an ICT incident that is related to the ICT service provided to the FE. IBM Cloud will take steps to minimize the impact of the incident and restore services as quickly as possible, providing reasonably requested information about the incident and the status of any IBM remediation and restoration activities. The IBM Cloud platform status page is used for all client notifications including "general" security related notifications. A client may notify IBM of a suspected vulnerability or incident by submitting a request through the incident reporting process specific to the IBM Service or, in the absence of such process, by submitting a technical support request.
30.2.(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	IBM will fully cooperate with the competent authorities and resolution authorities of Client, including persons appointed by them.

30.2.(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	Subject to Client's payment obligations and the termination provisions in the Agreement, Client may terminate the Agreement for, and only in respect of, the affected ICT Service in the following circumstances: - significant breach by IBM of applicable laws, regulations or the Agreement; - circumstances identified throughout the monitoring of ICT third-party risk that are deemed by the parties capable of negatively altering the performance of the functions provided through the Agreement, including material changes that negatively affect the Agreement or IBM's situation as an ICT third-party service provider; - IBM's evidenced weaknesses, pertaining to its overall ICT risk management and, in particular, in the way it ensures the availability, authenticity, integrity, and confidentiality of data, whether personal or otherwise sensitive data, or non-personal data; or - where the competent authority notifies the parties that it can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement In the event of any such Client termination above or a similar termination of a Non-IBM Product, IBM will refund a portion of any prepaid amounts for the applicable Cloud Service for the period after the date of termination. Upon termination, IBM may assist Client in transitioning Content to an alternative technology for an additional charge and under separately agreed terms.
30.2.(i)	the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programs and digital operational resilience training in accordance with Article 13(6)	Where appropriate, Client shall include IBM in its relevant ICT security awareness programs and/or digital operational resilience training. If IBM's participation is requested by Client, the parties will discuss and specify in the relevant TD, the conditions for the participation in such training schemes related to the ICT Services, including but not limited to scheduling, number of IBM participants and charges.

30.3	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:	
30.3.(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;	IBM Cloud aims to deliver the highest levels of availability and offers a service level agreement (SLA), which provides credits against service charges should a service fail to meet its stated availability target. The IBM Cloud Service Level Agreements defines the service level descriptions, including updates and revisions, with quantitative and qualitative performance targets. IBM Cloud provides the ability for FEs to monitor the current status of IBM Cloud® platform and services via the IBM Cloud platform status page. This tool can be leveraged to monitor performance against agreed-upon Cloud service levels in real time. FE's can also set up notifications to get alerts on outages and incidents affecting their workloads. In the event that IBM Cloud does not meet agreed upon SLAs, FEs are able to request an SLA claim by using the form at https://cloud.ibm.com/unifiedsupport/supportcenter. IBM will validate SLA claims based upon information provided by FE and IBM system records and will notify FE of approved credits via the Cloud UI or email.
30.3.(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 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;	IBM Cloud will provide at least 12 months' notice of any discontinuation of material functionality of a Cloud Service, or modification to an API in a way that is not backwards compatible unless IBM must act sooner to comply with applicable laws, legal obligations, or regulations, to address a security issue, or to avoid undue economic burden.

30.3.(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	IBM Cloud enables FEs with high availability and disaster recovery, supports Disaster Recovery (DR) testing using DR dry-test, simulation and switch-over to a DR site. IBM Cloud® Backup, a full-featured, agent-based backup and recovery system can be managed through a web interface . IBM Cloud maintains internal encrypted backups of FEs content within the same geography where the regional or zonal service is located for recovery in case of data corruption or a major data center disaster. IBM Cloud has Contingency Planning governance via a dedicated Business Continuity Management System that includes a dedicated workgroup with coordination of the plan(s) development, with all the elements of the organization. The contingency planning process includes identification of Critical information system assets supporting critical missions and Business functions. IBM Cloud's business continuity plans define roles and responsibilities and detailed procedures for recovery per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) per service. Plans are reviewed and tested at least annually, using testing exercises that follow industry standard practices, to assess their effectiveness in an adverse situation. Test results are reviewed, and corrective actions are taken as appropriate, and plans and processes are updated according to lessons learned. IBM Cloud maintains capacity and resource planning in alignment with ISO27001 and these efforts are validated by external auditors to confirm IBM Cloud is ISO27001 compliant.

30.3.(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	IBM Cloud will perform penetration testing of Cloud Services at least annually. Such testing may be carried out by qualified IBM testers, including IBM X-Force, or by qualified third-party providers. IBM Cloud supports FEs conducting penetration testing of VPC or Classic Infrastructure resources on IBM Cloud. IBM Cloud agrees to participate and fully cooperate in FE's TLPT for the use of ICT Services supporting Critical or Important Functions of the FE. The Client will notify their IBM Account Team Representative, as soon as possible upon notification from the competent authorities that the Client is validated as in scope of TLPT and they determined that IBM, as an ICT third-party services provider, will be in scope as a result of the Clients use of an IBM ICT Service supporting Critical or Important Functions.
30.3.(e)	the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following: (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; (ii) the right to agree on alternative assurance levels if other FEs' rights are affected; (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 (iv) the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;	FEs leveraging IBM Cloud to support Critical or Important Functions have the right to monitor, on an ongoing basis, IBM Cloud's performance. IBM has established audit types, procedures and audit best practices for executing client's DORA audit rights in a manner that protects the data and rights of all clients. The types of audits, parties will undertake for executing the audit rights, include: 1. Client Vendor Assessment Audit, 2. Security and Compliance Workshop Audit, 3. Pooled Audit or Client Audit Review Options, 4. Data Center Audit Reviews (where applicable).

30.3.(f)	exit strategies, in particular the establishment of a mandatory adequate transition period: (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; (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.	The FE may terminate the IBM Cloud Services upon 30 days' notice. Upon FE request, IBM Cloud may support FE develop its exit strategy, including a transition period for ICT Services, during which IBM will continue providing the relevant ICT Services. IBM Cloud may charge Client a reasonable fee to perform transition to an alternative solution, such charges to be agreed in writing by both parties.
	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.	IBM maintains corporate policies and standards which support data and system security, privacy, confidentiality, integrity and availability. IBM's Security and Compliance Center provides a single dashboard to help monitor security and compliance postures. A third-party assessor performs periodic, rigorous assessments of IBM Cloud to ensure continuous alignment with industry best practices. This benefits FEs by offering more visibility and transparency into the effectiveness of IBM Cloud controls. IBM Cloud maintains compliance with various compliance programs such as: - ISO/IEC 22301(Business Continuity Management System) - ISO/IEC 27001 (Information Security Management Systems) - ISO/IEC 27017 (Cloud Security) - ISO/IEC 27018 (Cloud Privacy) - ISO/IEC 27701 (Privacy Information Management Systems) - PCI DSS - SOC 1 - SOC 2 - SOC 3 The complete listing of the compliance programs which IBM Cloud maintains is available via: https://www.ibm.com/cloud/compliance

30.4	When negotiating contractual arrangements, financial entities and ICT third-party service providers will consider the use of standard contractual clauses developed by public authorities for specific services.	IBM has prepared a DORA Addendum to be executed with FEs that need to comply with DORA. The DORA addendum will connect to the existing base contract for the FE. IBM remains responsible for the obligations under the Cloud Services Agreement, even if IBM uses a sub-contractor.

Related offerings

IBM Cloud for Financial Services®

Speed up innovation while addressing your security and compliance needs. IBM Cloud for Financial Services is designed to help FEs mitigate risk and accelerate cloud adoption for their most sensitive workloads.

Explore IBM Cloud for Financial Services →

IBM Cloud Security and Compliance Center Workload Protection

Workload Protection offers a CNAPP with ready-made DORA policies that help FEs stay compliant.

Explore IBM Cloud Security and Compliance Center Workload Protection →

IBM Cloud Compliance Programs for global, regional and industry specific compliance programs.

IBM Cloud Well-Architected Framework is a structured collection of materials to help architects create hybrid cloud solutions

IBM Cloud Deployable architectures are cloud automations for deploying a common architectural pattern that combines one or more cloud resources.

Next Steps

As we transition to the new phase of the DORA compliance, it is important that Financial Entities engage with their technology partners third-party service providers on strengthening operational resilience and risk management capabilities. IBM has made significant investments in its DORA preparedness ensuring our readiness to partner with FE clients in meeting their DORA obligations. IBM continues to actively monitor the finalization of important details on DORA such as the Regulatory Technical Standard on Subcontracting and maintain dialogue with the policy makers to ensure that the requirements are understood. We remain committed to being the premier for regulated industries.

About the authors

Sumit Yadav
Program Director, Product Management
IBM Cloud Security

Uto Akah Ifudu
Head, Regulatory Compliance Management
IBM Cloud

Vivek Kinra
Director, Product Management, IBM Cloud Platform, Security and Compliance

IBM Corporation

New Orchard Road
Armonk, NY 10504