97. GSE z/OS zExpertenforum
17.-18. October 2023

DORA – Digital Operational Resiliency Act

Christian Demmer
Principal IBM zSystems Technical Specialist
christian.demmer@de.ibm.com

Why new regulations?

Legacy of Financial Crash 2008

Financial Resilience

Innovation and Digital Transformation

Maintaining competition

Mitigation Risk

Harmonization of regulations

Worldwide regulation

United States
- Interagency paper 'Sound Practices to Strengthen Operational Resilience'
- National Cybersecurity Strategy
- SEC Proposed Ruling for Cybersecurity Risk Management Rule 10

Europe
- Digital Operational Resiliency Act (DORA)

United Kingdom
- FCA PS21/3 Building operational resilience policy statement
- Bank of England Operational resilience Statement of policy

Global
- Basel Committee on Banking Supervision issued 'Principles for Operational Resilience' and 'Principles on Outsourcing'

Singapore
- Monetary Authority of Singapore 'Guidelines on Risk Management Practices – Operational Risk'

Brazil
- Brazilian General Data Protection Law ("Lei Geral de Proteção de Dados" or "LGPD")
- Resolution 4.502/2016
- Central Bank of Brazil ('BACEN') Resolution 4.893/2021

South Africa
- South African Reserve Bank Prudential Authority 'Principles for operational resilience'

Australia
- Prudential Standard CPS 230 - Operational Risk Management

Ausflug in EU Rechtsvorschriften

Verordnung (Regulation)

Eine Verordnung ist ein verbindlicher Rechtsakt, den alle EU-Länder in vollem Umfang umsetzen müssen.

Richtlinie (Directive)

Eine Richtlinie ist ein Rechtsakt, in dem ein von allen EU-Ländern zu erreichendes Ziel festgelegt wird. Es ist jedoch Sache der einzelnen Länder, eigene Rechtsvorschriften zur Verwirklichung dieses Ziels zu erlassen.
Wird eine Richtlinie nicht fristgerecht oder nicht ordnungsgemäß umgesetzt, kann sie dennoch unmittelbar wirken und von Behörden angewendet werden.

Network and Information Systems Directive: NIS2

EU member states will have to transpose NIS2 into their national legislation by October 17, 2024. By April 17, 2025, the Member States must identify the entities in scope, applies to essential and important entities

Requirements:

- Cybersecurity risk management measures
- reporting obligations

Penalties:

- Fines up to 10M EUR or up to 2% of the total worldwide annual turnover

Additional actions for essential entities:

- suspend authorization for part or all the services or activities
- temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach

Essential entities
Energy Transport Banking Financial market infrastructures Health Drinking water Waste water Digital infrastructure Public administration Space
Important entities
Postal and courier services Waste management Manufacture, production and distribution of chemicals Food production, processing and distribution Manufacturing Digital providers

DORA - Financial Services – Resilience

The European Commission's **Digital Operational Resilience Act (DORA)** regulates the European Union financial services sector, imposing obligations in the following areas, among others:

1. ICT Risk Management & Governance,
2. Incident Reporting
3. Operational Resilience Testing
4. Management of ICT Third Party Risk

Information Sharing is encouraged, but not mandatory

When:	adopted by the EU on 28. November 2022 published on 27. December 2022 entry into force on 16. January 2023 enforceable on 17. January 2025
Who :	CRO, CISO, CFO, CEO
Sector:	Financial Services
Why:	Support the Potential of digital finance in terms of innovation and competition, while mitigating the risk arising from it

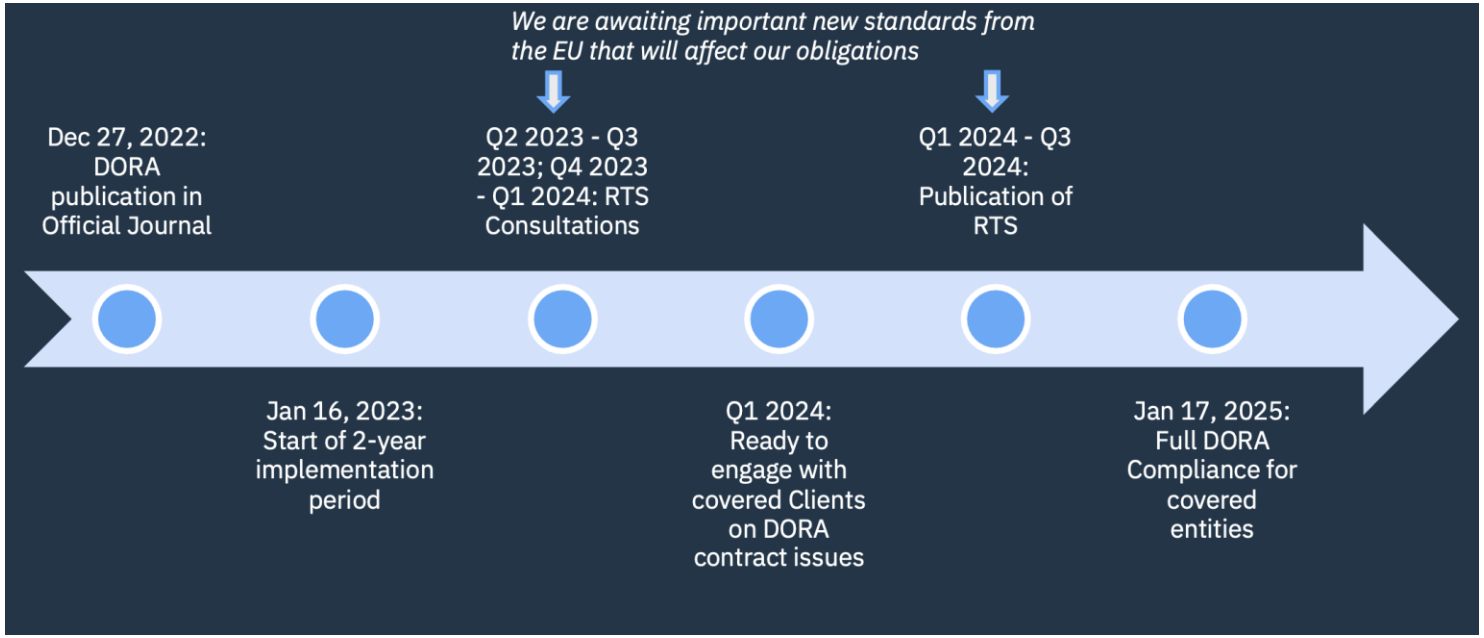
IBM RESOURCES

What is DORA? - IBM web page
IBM Promontory Article
DORA Action Guide – IBM PoV page

Time Line for DORA

While the EU has officially adopted DORA, key details are still being ironed out by the European Supervisory Authorities (ESAs).

The ESAs are the regulators that oversee 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 are in charge of drafting the regulatory technical standards (RTS) and implementing technical standards (ITS) that covered entities must implement. These standards are expected to be finalised in 2024. The European Commission is developing an oversight framework for critical ICT providers, which is also expected to be finalised in 2024.

To whom does DORA apply

DORA applies to all financial institutions in the EU. That includes traditional financial entities, like banks, investment firms and credit institutions and non-traditional entities, like crypto-asset service providers and crowdfunding platforms.

Notably, DORA also applies to some entities typically excluded from financial regulations. For example, ICT third-party service providers that supply financial firms with ICT systems and services – like cloud service providers and data centers – must follow DORA requirements. DORA also covers firms that provide critical information services, like credit rating services and data analytics providers.

What DORA is about

DORA is divided across **5 core pillars** that address various aspects or domains within ICT and cyber security, providing a comprehensive digital resiliency framework for the relevant entities.

ICT risk management requirements (Articles 5 to 14)

Financial entities are required to

- set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk,
- identify on a continuous basis all sources of ICT risk,
- set-up protection and prevention measures,
- promptly detect anomalous activities,
- put in place dedicated and comprehensive business continuity policies and disaster recovery plans as an integral part of the operational business continuity policy.

Reporting of ICT-related incidents (Articles 15 to 20)

Harmonising and streamlining the reporting of ICT-related incidents is achieved thru

- a management process to monitor and log ICT-related incidents,
- an obligation to classify them based on criteria detailed in the regulation and further developed by the ESAs through to specify materiality thresholds.

Only major incidents major must be reported.

The reporting using a common template and following a harmonised procedure.

Digital operational resilience testing (Articles 21 to 24)

The capabilities and functions included in the ICT risk management framework need to be periodically tested for preparedness and identification of weaknesses, deficiencies or gaps, as well as the prompt implementation of corrective measures.

Testing requirements depending on the size, business and risk profiles of financial entities: while all entities should perform a testing of ICT tools and systems

Significant and cyber mature financial entities should be required to conduct advanced testing.

Management of ICT third-party risk (Articles 25 to 39)

Ensure a sound monitoring of ICT third-party risk thru

- A set of principle-based rules for risk monitoring,
- Harmonising key elements of the service and relationship with ICT third-party provider.

to enable a complete monitoring throughout the conclusion, performance, termination and post-contractual stages of the relationship.

Contracts that govern that relationship will be required to contain a complete description of services, indication of locations where data is to be processed, full service level descriptions, ...

Information sharing arrangements (Article 40)

DORA enables financial entities to share among themselves cyber threat information and intelligence to strengthen digital operational resilience. This includes indicators of compromise, tactics, techniques, procedures, cybersecurity alerts, and configuration tools.
new supervisory framework provides for critical ICT third-party service providers to be monitored in the future by one of the European Supervisory Authorities (ESAs)

Examples of statements in DORA

Erwägungen:

(20) Anbieter von Cloud-Computing-Diensten sind eine Kategorie digitaler Infrastruktur, die unter die Richtlinie (EU) 2022/2555 fällt. Der mit dieser Verordnung geschaffene Überwachungsrahmen der Union (im Folgenden „Überwachungsrahmen") gilt für alle kritischen IKT-Drittdienstleister, einschließlich Anbietern von Cloud-Computing-Diensten, die Finanzunternehmen IKT-Dienstleistungen bereitstellen, und sollte als Ergänzung zu der Beaufsichtigung gemäß der Richtlinie (EU) 2022/2555 betrachtet werden. Darüber hinaus sollte der mit dieser Verordnung geschaffene Überwachungsrahmen für Anbieter von Cloud-Computing-Diensten gelten, wenn es keinen horizontalen Rahmen der Union gibt, mit dem eine Behörde für die digitale Überwachung eingerichtet wird.

(82) Die Anforderung, in der Union ein Tochterunternehmen zu gründen, sollte den kritischen IKT-Drittdienstleister nicht daran hindern, IKT-Dienstleistungen und damit verbundene technische Unterstützung von außerhalb der Union gelegenen Einrichtungen und Infrastruktur aus bereitzustellen. Diese Verordnung auferlegt keine Verpflichtung zur Lokalisierung von Daten, da sie keine Speicherung oder Verarbeitung von Daten in der Union vorschreibt.

Artikel 5:

Governance und Organisation

(1) Finanzunternehmen verfügen über einen internen Governance- und Kontrollrahmen, der im Einklang mit Artikel 6 Absatz 4 ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(2) Das Leitungsorgan des Finanzunternehmens definiert, genehmigt, überwacht und verantwortet die Umsetzung aller Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen nach Artikel 6 Absatz 1.

(3) Finanzunternehmen stellen ausreichende Ressourcen und Kapazitäten bereit, um Nutzeraktivitäten, das Auftreten von IKT-Anomalien und IKT-bezogenen Vorfällen, darunter insbesondere Cyberangriffe, zu überwachen.

Artikel 10:

Erkennung

(1) Finanzunternehmen verfügen über Mechanismen, um anomale Aktivitäten im Einklang mit Artikel 17, darunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle, umgehend zu erkennen und potenzielle einzelne wesentliche Schwachstellen zu ermitteln.

Artikel 7:

IKT-Systeme, -Protokolle und -Tools

Um IKT-Risiken zu bewältigen und zu managen, verwenden und unterhalten Finanzunternehmen stets auf dem neuesten Stand zu haltende IKT-Systeme, -Protokolle und -Tools, die

a) dem Umfang von Vorgängen, die die Ausübung ihrer Geschäftstätigkeiten unterstützen, im Einklang mit dem Grundsatz der Verhältnismäßigkeit nach Artikel 4 angemessen sind;

b) zuverlässig sind;

c) mit ausreichenden Kapazitäten ausgestattet sind, um die Daten, die für die Ausführung von Tätigkeiten und die rechtzeitige Erbringung von Dienstleistungen erforderlich sind, genau zu verarbeiten und Auftragsspitzen, Mitteilungen oder Transaktionen auch bei Einführung neuer Technologien bewältigen zu können;

d) technologisch resilient sind, um dem unter angespannten Marktbedingungen oder anderen widrigen Umständen erforderlichen zusätzlichen Bedarf an Informationsverarbeitung angemessen zu begegnen.

Artikel 12:

Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung

(2) Finanzunternehmen richten Datensicherungssysteme ein, die in Übereinstimmung mit den Richtlinien und Verfahren zur Datensicherung sowie den Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung aktiviert werden können. Die Aktivierung von Datensicherungssystemen darf die Sicherheit der Netzwerk- und Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten nicht gefährden. Die Datensicherungsverfahren sowie die Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden sind regelmäßig zu testen.

(3) Bei der Wiedergewinnung gesicherter Daten mithilfe eigener Systeme verwenden Finanzunternehmen IKT-Systeme, die von ihrem Quellsystem physisch und logisch getrennt sind. Die IKT-Systeme müssen sicher vor unbefugtem Zugriff oder IKT-Manipulationen geschützt sein und die rechtzeitige Wiederherstellung von Diensten ermöglichen, wobei erforderlichenfalls Daten- und Systemsicherungen (Backups) zu nutzen sind.

(4) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, unterhalten redundante IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen, die für die Deckung des Geschäftsbedarfs ausreichen und angemessen sind. Kleinstunternehmen bewerten auf der Grundlage ihres Risikoprofils, ob diese redundanten IKT-Kapazitäten unterhalten werden müssen.

(5) Zentralverwahrer unterhalten mindestens einen sekundären Verarbeitungsstandort, dessen Ressourcen, Kapazitäten, Funktionen und Personalressourcen angemessen sind, um den Geschäftsbedarf zu decken.

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

DORA: Classification of Incidents

Artikel 18:

Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen

(1) Finanzunternehmen klassifizieren IKT-bezogene Vorfälle und bestimmen deren Auswirkungen anhand folgender Kriterien:

a) Anzahl und/oder Relevanz der Kunden oder anderer Gegenparteien im Finanzbereich, die von dem IKT-bezogenen Vorfall betroffen sind, und gegebenenfalls des Werts oder der Anzahl der davon betroffenen Transaktionen und ob der IKT-bezogene Vorfall einen Reputationsschaden verursacht hat;

b) Dauer des IKT-bezogenen Vorfalls, einschließlich der Ausfallzeiten des Dienstes;

c) geografische Ausbreitung der von dem IKT-bezogenen Vorfall betroffenen Gebiete, insbesondere wenn mehr als zwei Mitgliedstaaten betroffen sind;

d) die mit dem IKT-bezogenen Vorfall verbundenen Verfügbarkeits-, Authentizitäts-, Integritäts- oder Vertraulichkeitsverluste von Daten;

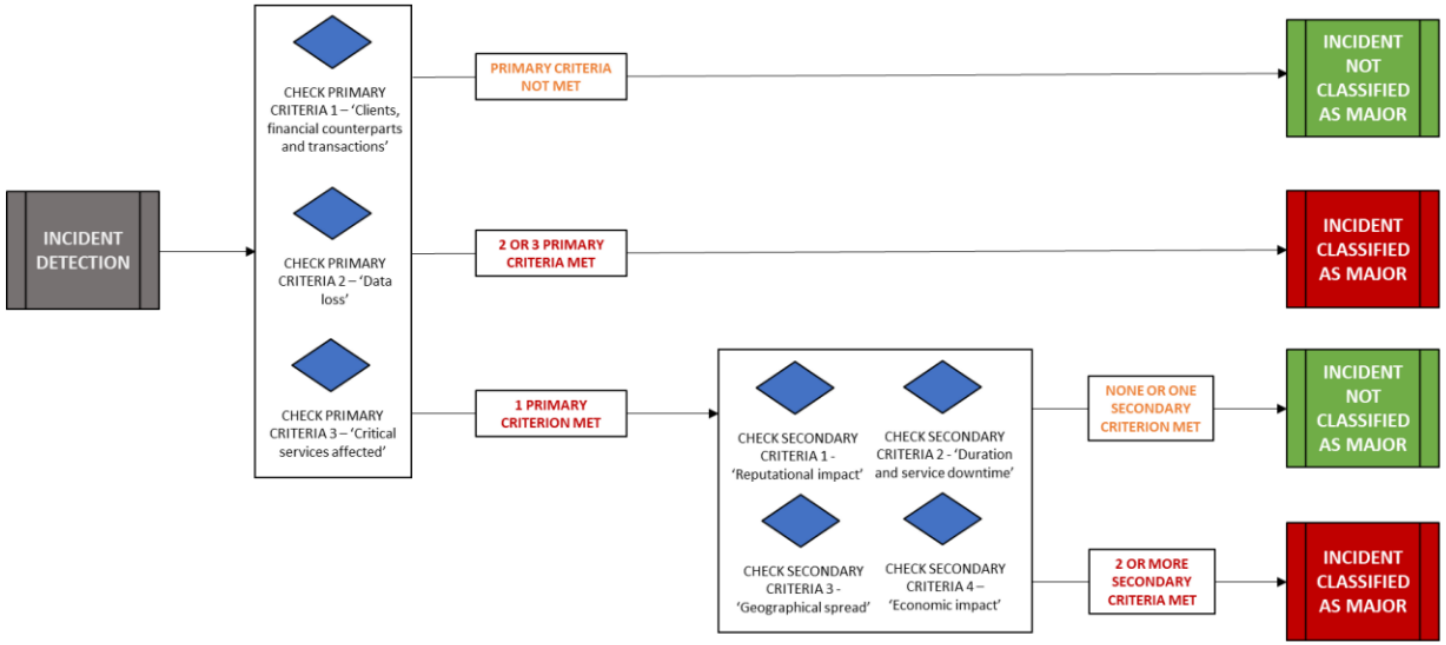
e) Kritikalität der betroffenen Dienste, einschließlich der Transaktionen und Geschäfte des Finanzunternehmens;

f) wirtschaftliche Auswirkungen — insbesondere direkte und indirekte Kosten und Verluste — des IKT-bezogenen Vorfalls auf absoluter und relativer Basis.

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

Regulatory Technical Standard (RTS)

Figure 1 – Incident classification chart



Extract from *Draft Regulatory Technical Standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554*

"19. .... The ESAs have, therefore, arrived at the view that, to ensure a balanced approach and taking into account that the 'number of clients affected' component of the criterion will not by itself trigger the reporting of a major incident, a threshold of 10% is most appropriate. The relative threshold will have to be calculated based on the number of clients affected by the incident (or an estimation in case data is not available) divided by all clients using the affected service of the financial entity.

20. The absolute threshold for the "number of clients affected" criterion has been set proportionately with the aim to apply to large FEs only where a significant number of clients are affected but the relative threshold is not being met. In the latter case, the ESAs propose to use a high absolute number of 50 000 clients, leveraging on the EBA Guidelines on major incident reporting under PSD2."

https://www.esma.europa.eu/press-news/esma-news/esas-consult-first-batch-dora-policy-products

Risk Plan and ICT Response and Recovery Plan

DORA Artikel 6:

IKT-Risikomanagementrahmen

(1) Finanzunternehmen verfügen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der Teil ihres Gesamtrisikomanagementsystems ist und es ihnen ermöglicht, IKT-Risiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten.

(2) Der IKT-Risikomanagementrahmen umfasst mindestens Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools, die erforderlich sind, um alle Informations- und IKT-Assets, einschließlich Computer-Software, Hardware und Server, ordnungsgemäß und angemessen zu schützen sowie um alle relevanten physischen Komponenten und Infrastrukturen, wie etwa Räumlichkeiten, Rechenzentren und ausgewiesene sensible Bereiche zu schützen, damit der angemessene Schutz aller Informations- und IKT-Assets vor Risiken, einschließlich der Beschädigung und des unbefugten Zugriffs oder der unbefugten Nutzung, gewährleistet ist.

(3) Im Einklang mit ihrem IKT-Risikomanagementrahmen minimieren Finanzunternehmen die Auswirkungen von IKT-Risiken, indem sie geeignete Strategien, Leit- und Richtlinien, Verfahren, IKT-Protokolle und Tools einsetzen. Sie legen den zuständigen Behörden auf Anfrage vollständige und aktuelle Informationen über IKT-Risiken und ihren IKT-Risikomanagementrahmen vor.

(8) Der IKT-Risikomanagementrahmen umfasst eine Strategie für die digitale operationale Resilienz, in der dargelegt wird, wie der Rahmen umgesetzt wird. Zu diesem Zweck schließt die Strategie für die digitale operationale Resilienz Methoden, um IKT-Risiken anzugehen und spezifische IKT-Ziele zu erreichen, ein, indem

a) erläutert wird, wie der IKT-Risikomanagementrahmen die Geschäftsstrategie und die Ziele des Finanzunternehmens unterstützt;

b) die Risikotoleranzschwelle für IKT-Risiken im Einklang mit der Risikobereitschaft des Finanzunternehmens festgelegt und die Auswirkungsstoleranz mit Blick auf IKT-Störungen untersucht wird;

c) klare Ziele für die Informationssicherheit festgelegt werden, einschließlich der wesentlichen Leistungsindikatoren und der wesentlichen Risikokennzahlen;

d) die IKT-Referenzarchitektur und etwaige Änderungen erläutert werden, die für die Erreichung spezifischer Geschäftsziele erforderlich sind;

e) die verschiedenen Mechanismen dargelegt werden, die eingesetzt wurden, um IKT-bezogene Vorfälle zu erkennen, sich davor zu schützen und daraus entstehende Folgen zu verhindern;

f) der aktuelle Stand bezüglich der digitalen operationalen Resilienz anhand der Anzahl gemeldeter schwerwiegender IKT-Vorfälle und bezüglich der Wirksamkeit von Präventivmaßnahmen dargelegt wird;

g) Tests der digitalen operationalen Resilienz gemäß Kapitel IV dieser Verordnung durchgeführt werden;

h) für IKT-bezogene Vorfälle eine Kommunikationsstrategie dargelegt wird, die gemäß Artikel 14 offengelegt werden muss.

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

More Statements in DORA especially on Testing

Artikel 24:

Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz

(1) Um die Vorbereitung auf die Handhabung IKT-bezogener Vorfälle zu bewerten, Schwächen, Mängel und Lücken in Bezug auf die digitale operationale Resilienz zu erkennen und Korrekturmaßnahmen umgehend umzusetzen, erstellen, pflegen und überprüfen Finanzunternehmen, die keine Kleinstunternehmen sind, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien ein solides und umfassendes Programm für das Testen der digitalen operationalen Resilienz als integraler Bestandteil des in Artikel 6 genannten IKT-Risikomanagementrahmens.

(2) Das Programm für Tests der digitalen operationalen Resilienz umfasst eine Reihe von Bewertungen, Tests, Methoden, Verfahren und Tools, die gemäß den Artikeln 25 und 26 anzuwenden sind.

(3) Bei der Ausführung des in Absatz 1 genannten Programms für das Testen der digitalen operationalen Resilienz wenden Finanzunternehmen, die keine Kleinstunternehmen sind, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien einen risikobasierten Ansatz an, wobei sie die sich entwickelnden IKT-Risikolandschaften, etwaige spezifische Risiken, denen das betreffende Finanzunternehmen ausgesetzt ist oder ausgesetzt sein könnte, die Kritikalität von Informationsassets und erbrachten Dienstleistungen sowie alle sonstigen Faktoren, die das Finanzunternehmen für angemessen hält, gebührend berücksichtigen.

(4) Finanzunternehmen, die keine Kleinstunternehmen sind, stellen sicher, dass Tests von unabhängigen, internen oder externen Parteien durchgeführt werden. Werden die Tests von einem internen Tester durchgeführt, stellen die Finanzunternehmen ausreichende Ressourcen bereit und tragen dafür Sorge, dass während der Konzeptions- und Durchführungsphase der Prüfung keine Interessenkonflikte entstehen.

(5) Finanzunternehmen, die keine Kleinstunternehmen sind, legen Verfahren und Leitlinien zur Priorisierung, Klassifizierung und Behebung aller während der Durchführung der Tests zutage getretenen Probleme fest und legen interne Validierungsmethoden fest, um sicherzustellen, dass alle ermittelten Schwächen, Mängel oder Lücken vollständig angegangen werden.

(6) Finanzunternehmen, die keine Kleinstunternehmen sind, stellen sicher, dass bei allen IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, mindestens einmal jährlich angemessene Tests durchgeführt werden.

Artikel 25:

Testen von IKT-Tools und -Systemen

(1) Das in Artikel 24 genannte Programm für die Tests der digitalen operationalen Resilienz beinhaltet im Einklang mit den in Artikel 4 Absatz 2 aufgeführten Kriterien die Durchführung angemessener Tests, wie etwa Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.

(2) Zentralverwahrer und zentrale Gegenparteien führen Schwachstellenbewertungen durch, bevor Anwendungen und Infrastrukturkomponenten sowie IKT-Dienstleistungen, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen, eingesetzt oder wieder eingesetzt werden.

Artikel 26:

Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT

(2) Jeder bedrohungsorientierte Penetrationstest schließt mehrere oder alle kritischen oder wichtigen Funktionen eines Finanzunternehmens ein und wird an Live-Produktionssystemen durchgeführt, die derartige Funktionen unterstützen.

Finanzunternehmen ermitteln alle relevanten zugrunde liegenden IKT-Systeme, -Prozesse und -Technologien, die kritische oder wichtige Funktionen und IKT-Dienstleistungen unterstützen, einschließlich derer, die diejenigen kritischen oder wichtigen Funktionen unterstützen, die an IKT-Drittdienstleister ausgelagert oder per Vertrag vergeben wurden.

(8) Finanzunternehmen beauftragen Tester für die Zwecke der Durchführung von TLPT gemäß Artikel 27. Ziehen Finanzunternehmen für die Zwecke der Durchführung von TLPT interne Tester heran, so beauftragen sie für jeden dritten Test einen externen Tester.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, ziehen nur externe Tester gemäß Artikel 27 Absatz 1 Buchstaben a bis e heran.

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

RTS: ICT Risk Management Tools Methods Processes Policies

Article 27

ICT response and recovery plans

1. Financial entities shall develop ICT response and recovery plans taking into account the results of the BIA. The ICT response and recovery plans shall:

(a) specify the conditions prompting their activation and any exceptions;

(b) describe what actions shall be taken to ensure the availability, integrity, continuity and recovery of at least the critical ICT systems and service of the financial entities;

(c) be designed to meet the recovery objectives of the operations of financial entities;

(d) be documented and made available to the staff involved in the execution of the plan and readily accessible in case of emergency. Financial entities shall clearly define roles and responsibilities to that extent;

(e) provide for both short-term and long-term recovery options including partial systems and recovery;

(f) lay down the objectives of the plan and the conditions to declare successful execution of the plan;

(g) be updated in accordance with lessons derived from ICT-related incidents, results of tests, newly identified risks and threats, and recovery objectives and priorities amended in accordance with recommendations stemming from audit checks or supervisory reviews.

2. The ICT response and recovery plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. The scenarios shall include all of the following:

(a) cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities;

(b) scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency, or other failures, of any relevant ICT third-party service provider;

(c) partial or total failure of premises, including office and business premises, and data centres;

(d) substantial failure of ICT assets or of the communication infrastructure;

(e) the non-availability of a critical number of staff or key staff members;

(f) natural disasters, pandemic situations and physical attacks, including intrusions and terrorist attacks;

(g) insider attack;

(h) political and social instability, including, where relevant, in the jurisdiction from where the ICT third-party service provider provides its services and the location where the data is stored and processed;

(i) widespread power outage.

https://www.esma.europa.eu/sites/default/files/2023-06/CP_-_Draft_RTSs_ICT_risk_management_tools_methods_processes_and_policies.pdf

DORA : What are the main needs?

Risk Management - Assess the effectiveness of the risk management measures that have been undertaken. **ICT governance and control frameworks**

How do I quantify and prioritize the top risks?
Can I **centralize and monitor risk management while meeting compliance and reporting needs?**
How do I prepare for audits?
How do I proactively monitor risk?
Do I know all all my risks?

Incident Response and Management - reporting requirements imposed on an entity.

How can I detect and respond to security risks?
How quickly can we recover from a cyber breach?
Do we have a good test plan with incident response plan in place?
How can I minimize the impact of a cyberbreach?
How do I ensure data integrity after a security breach?

3rd Party Risk Management - Have a strategy on ICT Third Party risk.

Can I classify my vendors according to risk?
Can I assess 3rd party risk?
Can I assess 3rd party compliance?
Do I have a strong governance model?
Can I automate the process of managing vendors?

Operational Resilience Testing - Disaster recovery, communications and crisis management

Are we protected against a cyber breach?
How do I respond during a cyber breach?
Can I accelerate the incident response time?
Can I automate and orchestrate the response?

IBM Technologies addressing key needs

Risk Management - Assess the effectiveness of the risk management measures that have been undertaken. **ICT governance and control frameworks**

IBM – Strategy & Risk Services (Risk Quantification, Risk Assessments, GRC, Supply Chain & Third-Party Security
Security Attack Surface Management, Data
Data – Watson Knowledge Catalog
Automation – Process Mining, Instana, SevOne, Turbonomic

Incident Response and Management - reporting requirements imposed on an entity.

IBM – X-Force Exchange
Security – EDR, XDR, SIEM, SOAR
Automation – IBM Process Mining, SevOne, Turbonomic
IBM Control Desk & Maximo Application Suite

3rd Party Risk Management - Have a strategy on ICT Third Party risk.

Operational Resilience Testing - Disaster recovery, communications and crisis management

IBM – CyberResilience Services (X-force)
Security – Incident Response Solutions (SOAR)
Automation – IBM Process Mining

IBM – Supply Chain & Third Party Cyber Risk Management, AGS, Security Awareness & Training
Security – QRadar
Data – OpenPages
Automation –SevOne, Turbonomic

Infrastructure solutions (HW, SW and Services) to support clients in Cyber Resilience (cross 4 areas)
IBM zSystems & LinuxONE (GDPS, Recovery Automation, Data Immutability, Air-GAP & CyberVault)
IBM Storage FlashSystem & IBM Storage Defender
IBM Cloud for Financial Services with Security Compliance Centre
IBM Power with PowerSC
IBM Technology Lifecycle Services

IBM Z Cyber Resiliency advanced hardware offerings

IBM GDPS

Article 11

- end-to-end application and data availability solution for IBM Z
- Automated recovery procedures, including cyber attacks
- Infrastructure monitoring
- Simplification for Sysplex and server management tasks
- easier-to-use interface from a central point of control

MIPS Flexibility
IBM Z Flexible Capacity for Cyber Resiliency

Article 10 & 11

- Dynamically shift production capacity between z16 systems at different sites
- Flexibility for DR test, planned maintenance, proactive outage avoidance, and actual DR scenarios
- Works in conjunction with other temporary record types and Tailored Fit Pricing for Hardware
- No on-site personnel (IBM or customer) required after initial set up
- Flexible duration of capacity transfer, up to 24 hours after record activation
- Swap and stay for up to 1 year
- Automate using solutions such as GDPS

IBM Z Cyber Resiliency advanced hardware offerings

Data Corruption
IBM Z Cyber Vault

Article 11 & 22

- IBM Z Solution that extends Safeguarded Copy on IBM storage to protect clients from malicious or accidental data corruption
- Uses multiple Logical Partitions (LPARs) to automate the detection and analysis of data corruption for the purposes of assessing data integrity and data recovery actions
- GDPS LCP Manager – a separate, priced feature of GDPS to provide a cyber resiliency capability for IBM Z.

Standard DR & DR Testing
Capacity Backup (CBU)

Article 10 & 11

- Traditional approach to provide replacement capacity in case of a machine or site outage
- Solution for unplanned events
- 10 days of testing per event
- Pricing based on number of CBU Engines

Unpredictable, high spiking workloads
Tailored Fit Pricing for IBM Z Hardware (TFP-HW)

Article 6

- Fixed size capacity corridor on top of customer owned capacity
- Always-on / activated 365/7/24
- Subscription fee for the always-on capacity
- Cloud-like usage charge granularity of 1 hour, based on actual MSU usage measured, not full engine capacity

Quality Assurance
IBM Z Business Resiliency Stress Test (zBuRST)

Article 21 & 22

- Solution for clients looking to increase DevOps code quality by introducing massive quality assurance and/or stress tests
- Can also be used in a QA or a DR configuration
- Pricing based on number of Tokens
- Special On/Off Capacity on Demand (OOCoD) Tokens priced at 80% off regular OOCoD pricing


IBM