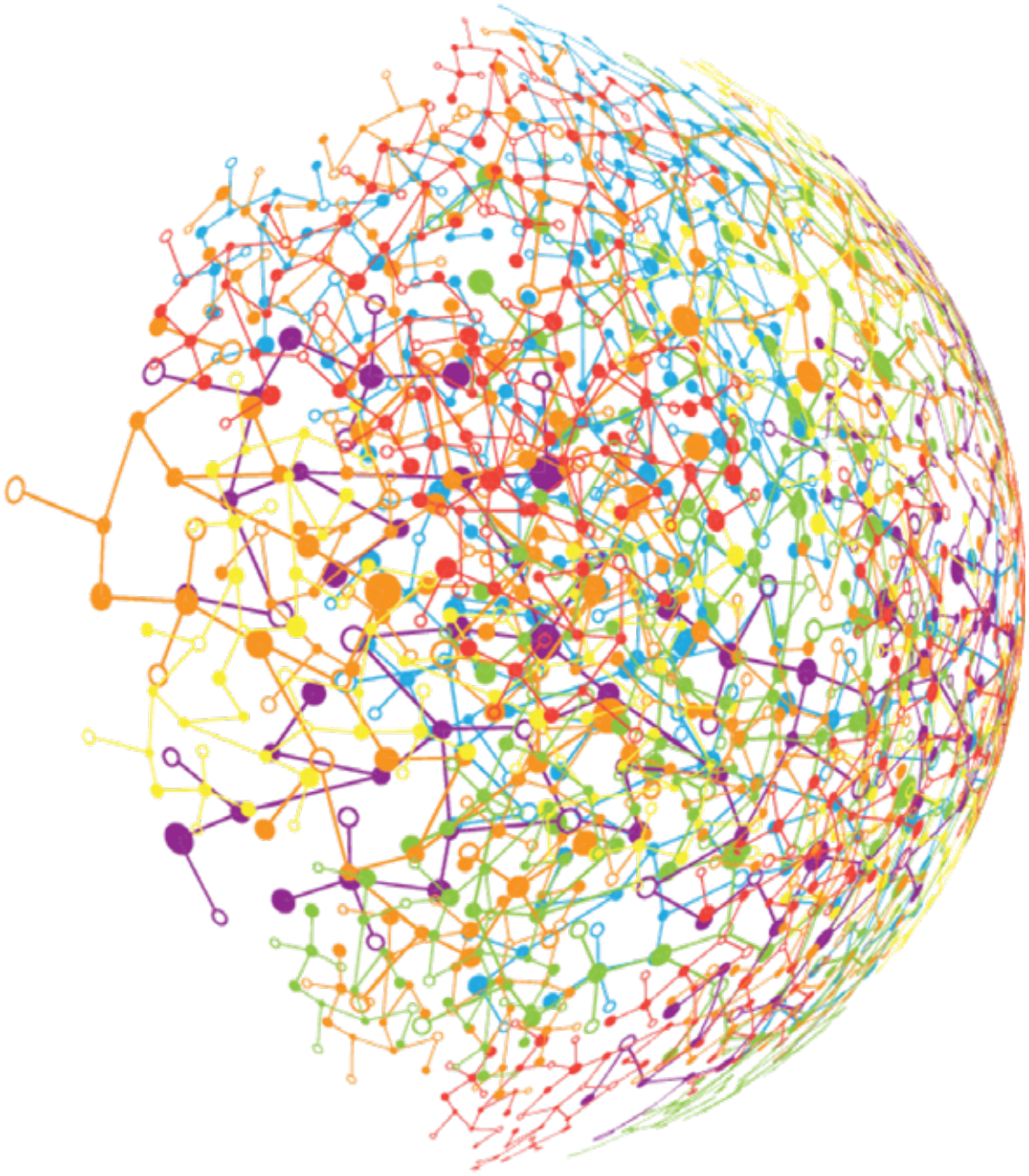
Deloitte.
デロイト トーマツ



Operational resilience for financial institutions

Implications from the European Union's Digital Operational Resilience Act (DORA)

March 2023

MAKING AN IMPACT THAT MATTERS since 1845

Table of contents

1. Recent trends in regulation and supervision on operational resilience

1.1 Increasing importance of operational resilience

Ensuring the resilience of financial institutions and the financial system is one of the most important mandates of the supervisory authorities in each jurisdiction. This is evident from the relevant authorities' mandates and missions. For instance, the Basel Committee on Banking Supervision (BCBS) aims to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability. The mission of the International Association of Insurance Supervisors (IAIS) is to promote effective supervision of insurance companies for the protection of policyholders and contribute to financial stability.

Since the financial crisis of 2008, supervisory authorities have been focusing on strengthening capital regulations for and building frameworks for the resolution of financial institutions to address the root causes of the crisis and to ensure the resilience of the financial system as well as financial institutions[1]. The former includes the development of Basel III standards by the BCBS and the establishment of the Principles for Sound Compensation Practices by the Financial Stability Board (FSB); the latter does the development of the Key Attributes of Effective Resolution Regimes for Financial Institutions and assessment of their implementation by the FSB. The FSB stated that the 'implementation of these reforms called for by the G20 after the global financial crisis is contributing to an open and resilient financial system' in its annual report published in 2019[2].

In the midst of these efforts, the environment surrounding the financial sector is constantly changing. Ensuring 'operational resilience' in addition to 'financial resilience' has therefore become a top priority for the supervisory authorities. For example, in 2018, the Bank of England, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) jointly published a discussion paper on operational resilience[3], pointing out that operational disruptions to the products and services that financial institutions provide have the potential to cause harm to consumers and market participants, threaten the viability of financial institutions and lead to instability in the financial system. The supervisory authorities also listed several factors that threaten the operational resilience of financial institutions, which include: (i) technical innovation such as fintech, artificial intelligence, distributed ledgers and crypto-assets, (ii) changes in behaviours such as increased ease of access and transaction speed, (iii) skill gaps and obsolescence caused by the speed of change, (iv) environmental changes such as an increase in cyber incidents and pressure to reduce costs and (v) system complexities such as increased use of third parties, concentration risks and cross-border dependencies.

Digitalisation, which has been greatly accelerated during the recent pandemic, also poses a threat to

[1] Financial Stability Board 'Post-2008 financial crisis reforms' (last updated on 13 June 2022), https://www.fsb.org/work-of-the-fsb/market-and-institutional-resilience/post-2008-financial-crisis-reforms/.

[2] Financial Stability Board (2019) 'Implementation and Effects of the G20 Financial Regulatory Reforms', https://www.fsb.org/wp-content/uploads/P161019.pdf.

[3] Bank of England, Prudential Regulation Authority and Financial Conduct Authority (2018) 'Discussion Paper: Building the UK financial sector's operational resilience', https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.

operational resilience. On the one hand, the use of Big Tech services, such as cloud computing, can contribute to cost reductions, flexibility, scalability and standardisation, as well as improvements in security and operational resilience of financial institutions. On the other hand, increased reliance on technology may create new vulnerabilities, such as cyberattacks, increased complexity in the structure of the financial services sector and concentration risks resulting from the reliance on a limited number of service providers[4], and thus present challenges to the operational resilience of financial institutions.

1.2 Regulatory developments in major jurisdictions

As ensuring operational resilience of financial institutions becomes an important supervisory task, frameworks for the regulation and supervision of financial institutions' operational resilience are being developed.

Global

The BCBS established the 'Principles for Operational Resilience' in March 2021, stating that while significantly higher levels of capital and liquidity have improved banks' ability to absorb financial shocks through regulatory reforms after the financial crisis, further work is necessary to strengthen their ability to absorb operational-related events, such as pandemics, cyber incidents and technology failures[5]. The BCBS sets out seven principles related to operational resilience (Table 1), defining operational resilience as the ability of a bank to deliver critical operations through disruptions.

Table 1. Structure of the BCBS's Principles for Operational Resilience

Principle 1: Governance
Principle 2: Operational risk management
Principle 3: Business continuity planning and testing
Principle 4: Mapping interconnections and interdependencies
Principle 5: Third-party dependency management
Principle 6: Incident management
Principle 7: ICT including cyber security

Europe

The U.K. PRA formulated a new regulation on operational resilience of financial institutions titled 'Operational resilience: Impact tolerances for important business services' [6] in March 2021 (subsequently updated in March 2022), together with regulations on outsourcing and third-party risk management [7]. The new regulation on operational resilience, which came into effect in March 2022, requires financial institutions to strengthen their operational resilience through meeting its requirements (Table 2).

[4] Financial Stability Board (2022) 'FinTech and Market Structure in the COVID-19 Pandemic – Implications for financial stability', https://www.fsb.org/wp-content/uploads/P210322.pdf.

[5] Basel Committee on Banking Supervision (2021) 'Principles for Operational Resilience', https://www.bis.org/bcbs/publ/d516.pdf.

[6] Prudential Regulation Authority (2022) 'Supervisory Statement | SS1/21 – Operational resilience: Impact tolerances for important business services', https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-22.pdf?la=en&hash=ED32FF8608D88C585FD47B82F0C5FF0A3751E4EE.

[7] Prudential Regulation Authority (2021) 'Supervisory Statement | SS2/21 – Outsourcing and third party risk management', https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf?la=en&hash=5A029BBC764BCC2C4A5F337D8E177A14574E3343.

Table 2. Overview of the requirements in the U.K. PRA's supervisory statement on operational resilience

- To identify important business services, which are defined as the services a firm provides that, if disrupted, could pose a risk to a firm's safety and soundness or, if a firm is systemically important, the financial stability of the UK.
- To set an impact tolerance for each of their important business services, which means the maximum tolerable level of disruption to an important business service as measured by length of time, etc.
- To ensure being able to deliver important business services within impact tolerances in severe but plausible scenarios, which includes developing effective remediation plans, managing their use of third parties effectively and developing communication strategies for both internal and external stakeholders.
- To identify and document the necessary people, processes, technologies, facilities and information required to deliver each of their important business services.
- To regularly test the ability to remain within impact tolerances in severe but plausible disruption scenarios.
- To obtain approval from the Board on the important business services identified and the impact tolerances set for each of these services.

The Central Bank of Ireland published a guidance titled 'Cross Industry Guidance on Operational Resilience' in December 2021, which organises operational resilience into three pillars: (i) identification and preparation, (ii) response and adaptation and (iii) recovery and learning [8]. The guidance sets out 15 guidelines, covering, for instance, the identification of critical or important business services and setting impact tolerances (1st pillar), business continuity management and incident management (2nd pillar) and continuous improvement (3rd pillar).

The Swiss Financial Market Supervisory Authority (FINMA) made extensive revisions to its circular on operational risks for banks and published it as the 'Circular on Operational Risks and Resilience' in December 2022 (Table 3) [9]. The circular requires banks to identify their critical functions and tolerance levels for disruptions and test their ability to provide critical functions during a disruption, etc, defining operational resilience as the bank's ability to restore its critical functions in case of a disruption within the tolerance levels for disruptions.

[8] Central Bank of Ireland (2021) 'Cross Industry Guidance on Operational Resilience', https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cross-industry-guidance-on-operational-resilience.pdf?sfvrsn=bd29921d_5.

[9] Swiss Financial Market Supervisory Authority (2023) 'Circular 2023/1 Operational risks and resilience – banks', https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf?sc_lang=en&hash=1529FC7CCFD70F24BCC75C4D1B033ECF.

Table 3. Structure of the FINMA's circular on operational resilience

n Operational risk management
Ÿ Overarching operational risk management
Ÿ ICT risk management
- ICT strategy and governance
- Change management
- ICT operations
- Incident management
Ÿ Cyber risk management
Ÿ Critical data risk management
Ÿ Business continuity management
n Ensuring operational resilience
n Continuation of critical services during the resolution and recovery of systemically important banks

The Council of the European Union adopted the 'Regulation on digital operational resilience for the financial sector', which is commonly referred to as DORA, in November 2022. The next section of this article will provide an overview of the DORA.

Asia Pacific

The Monetary Authority of Singapore (MAS) revised its Business Continuity Management (BCM) guidelines in June 2022[10] for the first time in about 15 years. The new guidelines require financial institutions to (i) identify critical business services and functions, (ii) establish Service Recovery Time Objectives (SRTO) for each identified critical business service, (iii) map resources (people, technologies, data, etc.) and third-party dependencies, (iv) develop and update a BCM, including policies, plans and procedures, as well as test their preparedness and (v) establish incident and crisis management capabilities.

The Australian Prudential Regulation Authority (APRA) released its proposed prudential standards for operational risk management for banks and insurers for public consultation in July 2022[11]. The APRA plans to finalise the standards in early 2023 and apply them from 2024. The proposed standards require financial institutions to (i) effectively manage operational risks, (ii) maintain their critical operations within approved tolerance levels through severe disruptions and (iii) manage risks associated with the use of service providers, etc.

North America

The Federal Reserve Board (FRB), **the Office of the Comptroller of the Currency** (OCC) and **the Federal Deposit Insurance Corporation** (FDIC) jointly published a paper titled 'Sound Practices to Strengthen Operational Resilience' in November 2020. The paper summarises existing regulations and guidance that address operational resilience for large and complex banks in the United States[12]. The main text is comprised of seven sections, i.e., (i) governance, (ii) operational risk management, (iii) business continuity management, (iv) third-party risk management, (v) scenario analysis, (vi) secure and resilient information systems management and (vii) surveillance and

[10] Monetary Authority of Singapore (2022) 'Business Continuity Management Guidelines', https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/bcm-guidelines/bcm-guidelines-june-2022.pdf.

[11] Australian Prudential Regulation Authority (2022 'Prudential Standard CPS 230: Operational Risk Management', https://www.apra.gov.au/sites/default/files/2022-07/Draft%20Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management.pdf.

[12] Board of Governors of the Federal Reserve System (2022) 'SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience', https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm.

reporting, which is supplemented with an appendix regarding cyber risk management.

The U.S. Department of the Treasury stated in a report titled 'the Financial Services Sector's Adoption of Cloud Services' published in February 2023 that it recognises the importance of assessing the impact of new technologies, such as cloud services, on the operational resilience of the U.S. financial services sector[13].

The Office of the Superintendent of Financial Institutions (OSFI) in Canada is currently amending its guidelines on operational risk management (E-21) and plans to release a draft for public consultation in the spring of 2023. The OSFI defines several terms, such as operational resilience, critical operations and tolerance for disruption, and clarifies that operational resilience includes resilience to technology and cyber risks[14].

[13] U.S. Department of the Treasury (2023) 'The Financial Services Sector's Adoption of Cloud Services', https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

[14] Office of the Superintendent of Financial Institutions (2022) 'Operational resilience key definitions', https://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/20221206_let.aspx.

2. Overview of the European Union's Digital Operational Resilience Act (DORA)

The European Commission adopted a new Digital Finance Package in September 2020, which is aimed at boosting responsible innovation in the EU's financial sector as well as mitigating any potential risks related to investor protection, money laundering and cyber-crime. The package includes (i) Europe's digital finance strategy, (ii) legislative proposals on crypto-assets and (iii) the proposed Digital Operational Resilience Act (DORA) [15]. Subsequently, the DORA was finalised in December 2022 and will come into effect on 17 January 2025.

2.1 Overview of the DORA

The DORA consists of nine chapters and 64 articles (Table 4). Its aim is to achieve a high common level of digital operational resilience by setting uniform requirements concerning the security of networks and information systems supporting the business processes of financial entities.

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

The DORA applies to a wide range of entities in the financial services sector, including credit institutions, investment firms, payment institutions, central counterparties, insurers, insurance intermediaries and credit rating agencies. These entities to which the DORA is applicable are referred to as financial entities. The DORA is applied in a proportional manner.

[15] European Commission (2020) 'Digital finance package', https://finance.ec.europa.eu/publications/digital-finance-package_en.

Table 4. Structure of the DORA

Chapter I: General provisions	
Article 1	Subject matter
Article 2	Scope
Article 3	Definitions
Article 4	Proportionality principle
Chapter II: ICT risk management	
Article 5	Governance and organisation
Article 6	ICT risk management framework
Article 7	ICT systems, protocols and tools
Article 8	Identification
Article 9	Protection and prevention
Article 10	Detection
Article 11	Response and recovery
Article 12	Backup policies and procedures, restoration and recovery procedures and methods
Article 13	Learning and evolving
Article 14	Communication
Article 15	Further harmonisation of ICT risk management tools, methods, processes and policies
Article 16	Simplified ICT risk management framework
Chapter III: ICT-related incident management, classification and reporting	
Article 17	ICT-related incident management process
Article 18	Classification of ICT-related incidents and cyber threats
Article 19	Reporting of major ICT-related incidents and voluntary notification of significant cyber threats
Article 20	Harmonisation of reporting content and templates
Article 21	Centralisation of reporting of major ICT-related incidents
Article 22	Supervisory feedback
Article 23	Operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions
Chapter IV: Digital operational resilience testing	
Article 24	General requirements for the performance of digital operational resilience testing
Article 25	Testing of ICT tools and systems
Article 26	Advanced testing of ICT tools, systems and processes based on threat-led penetration testing (TLPT)
Article 27	Requirements for testers for the carrying out of TLPT
Chapter V: Managing of ICT third-party risk	
Article 28	General principles
Article 29	Preliminary assessment of ICT concentration risk at entity level
Article 30	Key contractual provisions
Article 31	Designation of critical ICT third-party service providers
Article 32	Structure of the Oversight Framework
Article 33	Tasks of the Lead Overseer
Article 34	Operational coordination between Lead Overseers
Article 35	Powers of the Lead Overseer
Article 36	Exercise of the powers of the Lead Overseer outside the Union
Article 37	Request for information
Article 38	General investigations
Article 39	Inspections
Article 40	Ongoing oversight
Article 41	Harmonisation of conditions enabling the conduct of the oversight activities
Article 42	Follow-up by competent authorities
Article 43	Oversight fees
Article 44	International cooperation
Chapter VI: Information-sharing arrangements	
Article 45	Information-sharing arrangements on cyber threat information and intelligence
Chapter VII: Competent authorities	
Article 46	Competent authorities
Article 47	Cooperation with structures and authorities established by Directive (EU) 2022/2555
Article 48	Cooperation between authorities
Article 49	Financial cross-sector exercises, communication and cooperation
Article 50	Administrative penalties and remedial measures
Article 51	Exercise of the power to impose administrative penalties and remedial measures
Article 52	Criminal penalties
Article 53	Notification duties
Article 54	Publication of administrative penalties
Article 55	Professional secrecy
Article 56	Data protection
Chapter VIII: Delegated acts	
Article 57	Exercise of the delegation
Chapter IX: Transitional and final provisions	
Article 58	Review clause
Articles 59 to 63	Amendments to relevant regulations
Article 64	Entry into force and application

2.2 Key requirements under the DORA

The DORA has the following five core components: (i) ICT risk management; (ii) ICT-related incident management, classification and reporting; (iii) digital operational resilience testing; (iv) ICT third-party risk management; and (v) oversight of critical ICT TPSPs. Key requirements provided by the respective core components can be summarised as follows.

2.2.(i) ICT risk management

- **Governance and ICT risk management framework**
  - Financial entities have in place (i) an internal governance and control framework and (ii) an ICT risk management framework, including a digital operational resilience strategy.
- **Identification of business functions and information/ICT assets**
  - Financial entities identify (i) all ICT supported business functions and the information/ICT assets supporting those functions, (ii) all processes that are dependent on ICT TPSPs and (iii) all sources of ICT risk, including cyber threats and ICT vulnerabilities relevant to their ICT supported business functions and information/ICT assets.
- **Protection, prevention and detection**
  - Financial entities have in place ICT security policies, procedures, protocols and tools to ensure the resilience, continuity and availability of ICT systems that support, in particular, critical or important functions.
- **Response and recovery**
  - Financial entities put in place and test (i) ICT business continuity policy and plans and (ii) response and recovery plans.
  - Financial entities assess the potential impact of severe business disruptions quantitatively and qualitatively through a business impact analysis (BIA).

2.2.(ii) ICT-related incident management, classification and reporting

- **ICT-related incident management process**
  - Financial entities establish an ICT-related incident management process to detect, manage and notify ICT-related incidents.
  - Incidents are classified according to their priority, severity and the criticality of the services impacted.
- **ICT-related incidents and cyber threats**
  - Financial entities (i) report major ICT-related incidents to the relevant competent authority and (ii) may, on a voluntary basis, notify significant cyber threats to the relevant authority.

2.2.(iii) Digital operational resilience testing

- **Testing of ICT tools and systems**
  - Financial entities establish a digital operational resilience testing programme and test all ICT systems and applications supporting critical or important functions at least annually. The test is undertaken by internal or external independent experts.
- **Threat-led penetration testing (TLPT)**
  - Financial entities identified by the competent authority carry out TLPT at least every three years and report the results to the authority.
  - Each TLPT, which is supposed to be performed by external experts, covers critical or important functions.

2.2.(iv) ICT third-party risk management

- **Key principles for the management of ICT third-party risk**
  - Financial entities develop a strategy on ICT third-party risk that includes a policy on the use of ICT services supporting critical or important functions provided by ICT TPSPs.
  - Financial entities may only enter into contractual arrangements with ICT TPSPs that comply with appropriate information security standards, after undertaking due diligence on prospective ICT TPSPs.
  - Financial entities ensure that contractual arrangements on the use of ICT services may be terminated in certain circumstances, such as in the case of a significant breach of applicable laws and regulations by the ICT TPSP.
  - For ICT services supporting critical or important functions, financial entities put in place exit strategies that enable them to exit contractual arrangements without disruption to their business activities.
- **Key contractual provisions**
  - The contractual arrangements on the use of ICT services supporting critical or important functions include at least the right to monitor the ICT TPSP's performance, including unrestricted rights of access, inspection and audit by the financial entity as well as the competent authority.

2.2.(v) Oversight framework for critical ICT TPSPs

- **Designation of critical ICT TPSPs**
  - The European Supervisory Authorities (ESAs) designate the ICT TPSPs that are critical for financial entities based on certain criteria, such as the systemic impact of a failure of the ICT TPSP on the continuity of the provision of financial services and the systemic importance of the financial entities relying on the ICT TPSP.
  - The Lead Overseer appointed for each critical ICT TPSP may request the critical ICT TPSP to submit all relevant information and conduct inspections.

2.3 Development of technical standards, etc.

The DORA requests that the ESAs draft Regulatory Technical Standards (RTSs) and Implementing Technical Standards (ITSs) on certain requirements and submit proposals to the European Commission as shown in Table 5.

The European Commission will carry out a review, for example, of the criteria for the designation of critical ICT TPSPs and the voluntary nature of the notification of significant cyber threats and will submit a report to the European Parliament and the Council by January 2028.

Table 5. RTSs and ITSs to be developed

Main items	Type	Consultation[16]	EC submission
Further elements to be included in the ICT security policies, procedures, protocols and tools, etc. (Article 15 of the DORA)	RTS	June 2023	17 January 2024
Criteria for the classification of major ICT-related incidents and significant cyber threats (Article 18)	RTS	June 2023	17 January 2024
The content of the major ICT-related incident reports and notifications for significant cyber threats, as well as the time limits for incident reporting (Article 20)	RTS	November 2023	17 July 2024
Standard forms, templates and procedures to report a major ICT-related incident and to notify a significant cyber threat (Article 20)	ITS	NA	17 July 2024
Details of requirements related to the TLPT (Article 26)	RTS	NA	17 July 2024
Templates for the register of information (Article 28)	ITS	June 2023	17 January 2024
Detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT TPSPs (Article 28)	RTS	June 2023	17 January 2024
Further elements that a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions (Article 30)	RTS	November 2023	17 July 2024

16 European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities Markets Authority and Joint Committee of the European Supervisory Authorities (2022) 'Joint ESAs public event on DORA, technical discussion', https://www.esma.europa.eu/sites/default/files/2023-02/Joint_ESAs_DORA_event_-_ESAs_slides.pdf.

3 Discussion

Ensuring operational resilience is not necessarily a new challenge for financial institutions. Particularly in the field of ICT, efforts have been continuously made to ensure ICT security. In Japan, financial institutions have implemented measures to keep their ICT systems safe and secure, referring to the 'Security Guidelines on Computer Systems for Banking and Related Financial Institutions' developed by the Center for Financial Industry Information Systems (FISC).

Nevertheless, 'not necessarily a new challenge' does not mean that financial institutions do not need to upgrade what they have been doing. ICT-related incidents and cyber threats can have a greater impact on the operations of financial institutions (and even on the stability of the financial system). International organisations, such as the Financial Stability Board (FSB) and the Basel Committee on Banking Supervision (BCBS), as well as supervisory authorities in major jurisdictions, such as Europe, the U.K., Australia, Canada and Singapore, are hence strengthening regulations and supervision related to operational resilience. Ensuring operational resilience has become a top business issue for the management of financial institutions.

The fact that the DORA has been formulated as a Regulation, rather than a Directive or Supervisory Standard, also has meaning. Although there might be different opinions on such an approach in Europe, ensuring operational resilience has now become an urgent issue at least for European financial institutions. This means that the leadership and involvement of the management of financial institutions is essential.

How should Japanese financial institutions view the DORA? Many Japanese financial institutions are unlikely to be directly affected by the DORA. Nevertheless, it is considered beneficial for them to benchmark their current level of operational resilience against the DORA and promote further enhancements, assuming that similar levels of operational resilience will be required in Japan. It is particularly important for the management of financial institutions to recognise their 'As-Is' and 'To-Be' states with regard to the core components of the DORA, such as building and practicing an ICT risk management framework, managing and classifying ICT-related incidents, conducting digital operational resilience testing and managing ICT third-party risk. In this regard, utilising external experts will be an option.

For supervisory authorities, one challenge is to enhance their capabilities to effectively supervise the operational resilience of financial institutions. In December 2022, the Financial Services Agency (FSA) of Japan published a discussion paper titled 'Considerations for Ensuring Operational Resilience,' outlining its current thinking and future supervisory approach [17]. In order for the FSA to effectively encourage financial institutions to search for best practices, 'in-depth dialogue' between the supervisory authority and financial institutions is essential.

There may also be a need for a governmental response. The DORA adopts an approach of designating important ICT TPSPs and regulating and supervising them intensively. A similar approach is also being considered in the U.K. The U.K. PRA has proposed to

[17] Financial Services Agency (2022) 'Draft discussion paper: Considerations for ensuring operational resilience' (in Japanese), https://www.fsa.go.jp/news/r4/ginkou/20221216-2/01.pdf.

identify Critical Third-party Providers (CTPs) from the perspective of 'materiality and concentration' in its discussion paper 'Operational resilience: Critical third parties to the UK financial sector' published in July 2022[18], in which a draft of the minimum resilience standards that CTPs should meet is presented. Following the financial crisis, Global Systemically Important Financial Institutions (G-SIFIs) have been designated by financial supervisory authorities. For designating and supervising critical third-party service providers effectively, which could not be performed by a single authority, coordination among relevant authorities will be important.

End of article

Note: The opinions expressed in this article are those of the author and do not represent the official views of the organisation to which the author belongs.

[18] Prudential Regulation Authority (2022) 'DP3/22 – Operational resilience: Critical third parties to the UK financial sector', https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector.

Author

Shinya Kobayashi
Managing Director
Centre for Risk Management Strategy
Deloitte Touche Tohmatsu LLC

Deloitte.
デロイト トーマツ

Deloitte Tohmatsu Group (Deloitte Japan) is a collective term that refers to Deloitte Tohmatsu LLC, which is the Member of Deloitte Asia Pacific Limited and of the Deloitte Network in Japan, and firms affiliated with Deloitte Tohmatsu LLC that include Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu Consulting LLC, Deloitte Tohmatsu Financial Advisory LLC, Deloitte Tohmatsu Tax Co., DT Legal Japan, and Deloitte Tohmatsu Corporate Solutions LLC. Deloitte Tohmatsu Group is known as one of the largest professional services groups in Japan. Through the firms in the Group, Deloitte Tohmatsu Group provides audit & assurance, risk advisory, consulting, financial advisory, tax, legal and related services in accordance with applicable laws and regulations. With more than 15,000 professionals in about 30 cities throughout Japan, Deloitte Tohmatsu Group serves a number of clients including multinational enterprises and major Japanese businesses. For more information, please visit the Group's website at www.deloitte.com/jp/en.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.
Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's more than 345,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301