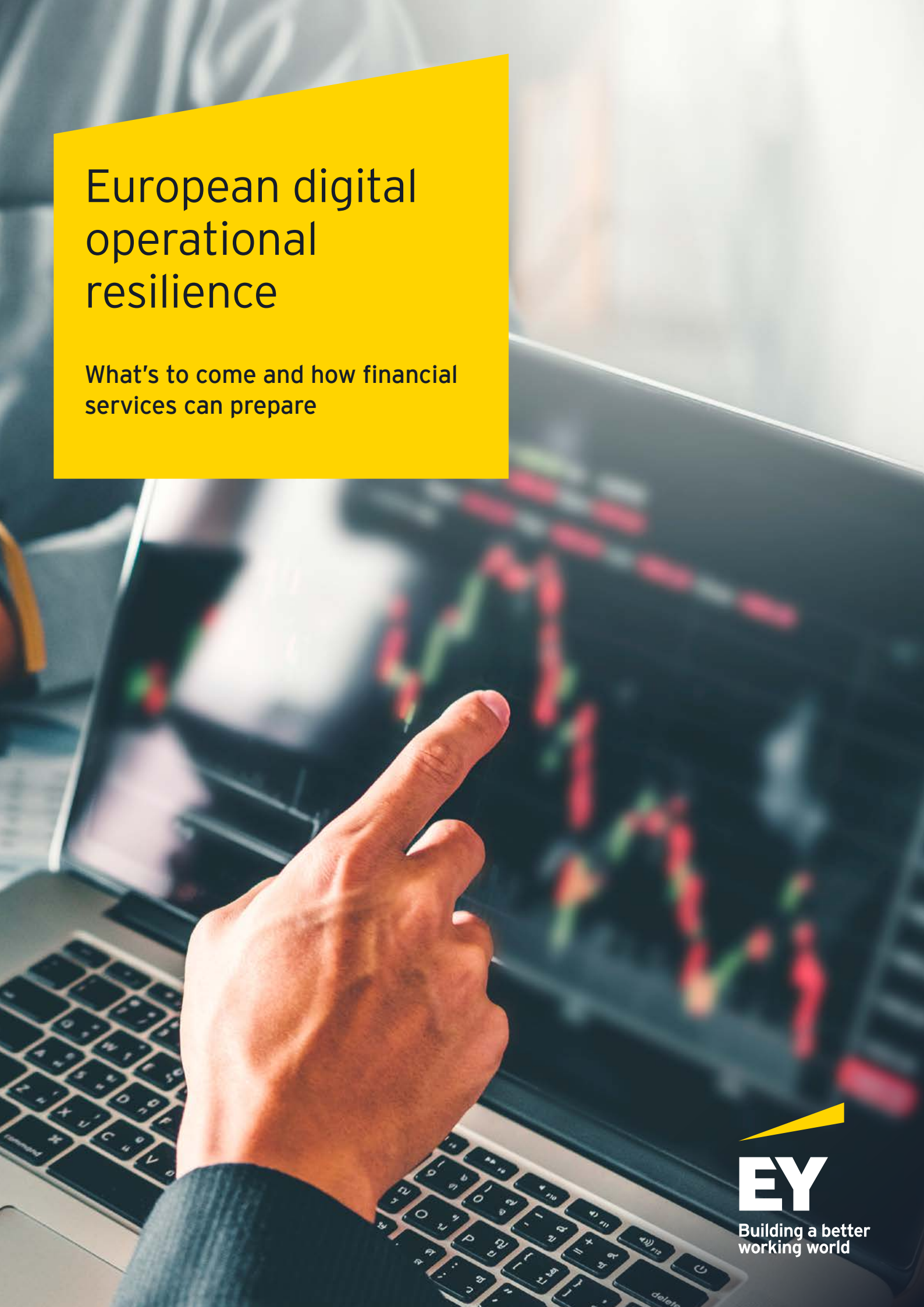
European digital operational resilience

What's to come and how financial services can prepare



Building a better working world

Introduction

Regulators across the globe are shifting their focus to make certain that financial services firms can deliver important services to their customers and withstand disruptions. Over the past few years, different regulatory regimes have developed their own definitions and expectations of operational resilience.

At the global level, the Basel Committee on Banking Supervision (BCBS) published its 'Principles for Operational Resilience' in March 2021.[1]

These principles focus on:

1. Governance
2. Operational risk management
3. Business continuity planning and testing
4. Mapping interconnections and interdependencies
5. Third-party dependency management
6. Incident management
7. Resilient cyber security and Information Communication Technology (ICT)

This paper looks at the digital angle of operational resilience. It seeks to provide financial firms with:

- An overview of regulatory regimes in Europe (the EU), the UK, and Switzerland
- A summary of its interlinkages with pending cybersecurity policy proposals
- Considerations for firms as they prepare to implement these regimes within their organizations

[1] Press release: Basel Committee issues principles for operational resilience and risk (bis.org)

Regulatory proposals

European Union (EU)

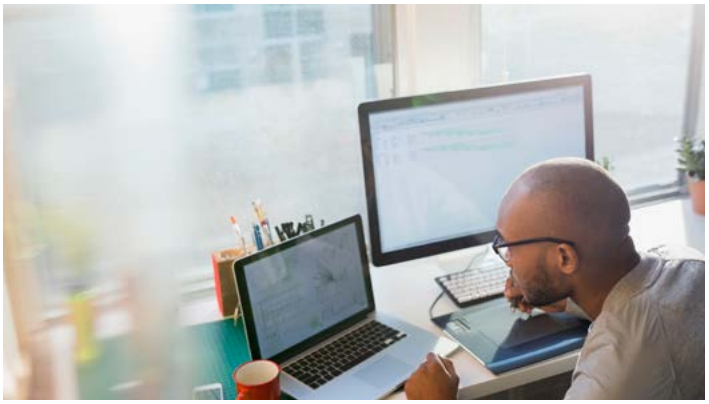
DORA

The Digital Operational Resilience Act (DORA) seeks to provide a unified approach for mitigating ICT-related incidents and ensuring the financial sector in Europe can maintain resilient operations through a severe operational disruption. The European Parliament and the Council have reached a technical agreement on DORA, and the final publication is due in early 2023. Financial services firms will then have two years for implementation.

DORA creates uniform requirements for the security of network and information systems of financial services firms. It aims to create a robust framework for the management of ICT related risks in the financial sector, whereby all firms will need to make sure that they can withstand, respond to, and recover from all types of ICT-related disruptions and threats. These requirements will be the same for all EU countries.

Key points to note:

- DORA will apply to financial entities regulated at an EU level, and to critical ICT third-party providers (TPPs). The designation of TPPs is part of the Regulatory Technical Standards that are still to be defined.
- DORA is capabilities led; therefore, a digital resilience strategy and related testing strategy will need to be defined and implemented.[2]
- Critical third-country ICT service providers to financial entities in the EU will need to establish a subsidiary within the EU so that oversight can be suitably implemented.
- Critical ICT TPPs including cloud service providers will be supervised by one of the European Supervisory Authorities (ESAs).
- Penetration testing will be carried out in functioning mode and Member States' authorities may also be involved in the test procedures, in addition to ESAs.



How to prepare

Two main approaches we would recommend when preparing to comply with DORA:

- **Purely aligning to DORA:** this would be suitable for firms operating solely within a European country and that do not have any cross-border activity.
- **Use an overarching Operational Resilience Framework:** integrating all regulatory requirements and core principles into the business. This is a possible option for firms operating outside of the EU and/or in EU countries that have more stringent requirements.

[2] How will the Digital Operational Resilience Act impact your organization? (ey.com)

From our practical experience, we have noticed that a 'no one size fits all' approach can be taken. However, the clear first step to take is to **perform an impact assessment** of the new regulation as compared to the current operations. Depending on the approach chosen, the impact assessment can be aligned with the DORA requirements alone or perform under an overarching (maturity) assessment, using operational resilience framework enablers such as detailed questionnaires and roadmap material.

NIS2

The current NIS Directive on security of network and information systems entered into force in August 2016. It sets requirements regarding national cybersecurity capabilities of EU countries; rules for their cross-border cooperation; and requirements regarding national supervision of operators of essential services and key digital service providers.

The proposed NIS2 Directive evolves the current state of play and aims to set the baseline for cybersecurity risk management and reporting obligations across a range of sectors, including energy, transport, health, and digital infrastructure. The revised directive seeks to remove deviations in cybersecurity measures across EU countries.

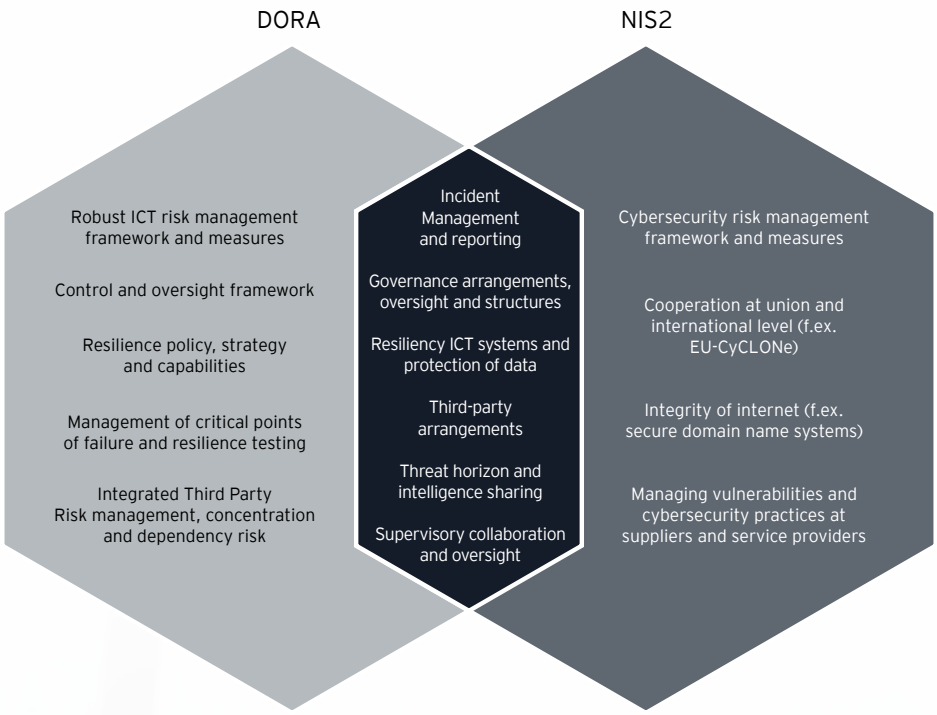
It also aims to achieve harmonization by setting out minimum rules for a regulatory framework and mechanisms for effective co-operation among authorities in EU member states.

The Council and the European Parliament approved measures for a common level of cybersecurity across the EU under the NIS2 Directive. The final text is expected to be published in early 2023. EU countries will have 21 months from the entry into force to incorporate its provisions into their national law.

Interaction of DORA with NIS2

DORA

- Focuses on organizations in the financial industry
- Focuses on ICT governance, risk, resilience and ICT outsourcing
- Prescriptive on procedures, controls
- Enhances testing and focuses on stress testing continuity and security
- Focuses on concentration risk and incident reporting/ communications
- Builds on the NIS Directive and addresses possible overlaps via a lex specialis exemption



NIS2

- Focuses on national level, EU level and international level and applies to more variety of industries
- Baseline for cybersecurity risk management and reporting obligations and focuses on network security and information security of essential and important services
- Focuses on many authoritive entities such as the CISRT, ENISA and the commission
- Focuses on aligning policies, authorative process of cyber security on a national level

Main differences

	DORA	NIS2
Focus area	Organization	National, EU, International
Scope	Financial organizations	Diverse industries/sectors
Topic(s)	Range of topics relating to operational resilience	Network and Information Security
Objective	Implementing controls and activities	Aligning national policies and national EU authorities

Building operational resilience – PS21/3 and Critical Third Parties Act

UK

PS21/3

In March 2021, the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA) and the Bank of England (the Bank) confirmed a new operational resilience framework for firms and Financial Market Infrastructures (FMIs). The new rules and guidance came into force on March 31, 2022.

The regulators have also set out specific expectations for the management of outsourcing arrangements, including the PRA Supervisory Statement outsourcing and third-party risk management[3] and FCA Guidance for firms outsourcing to the "cloud" and other third-party IT services[4].

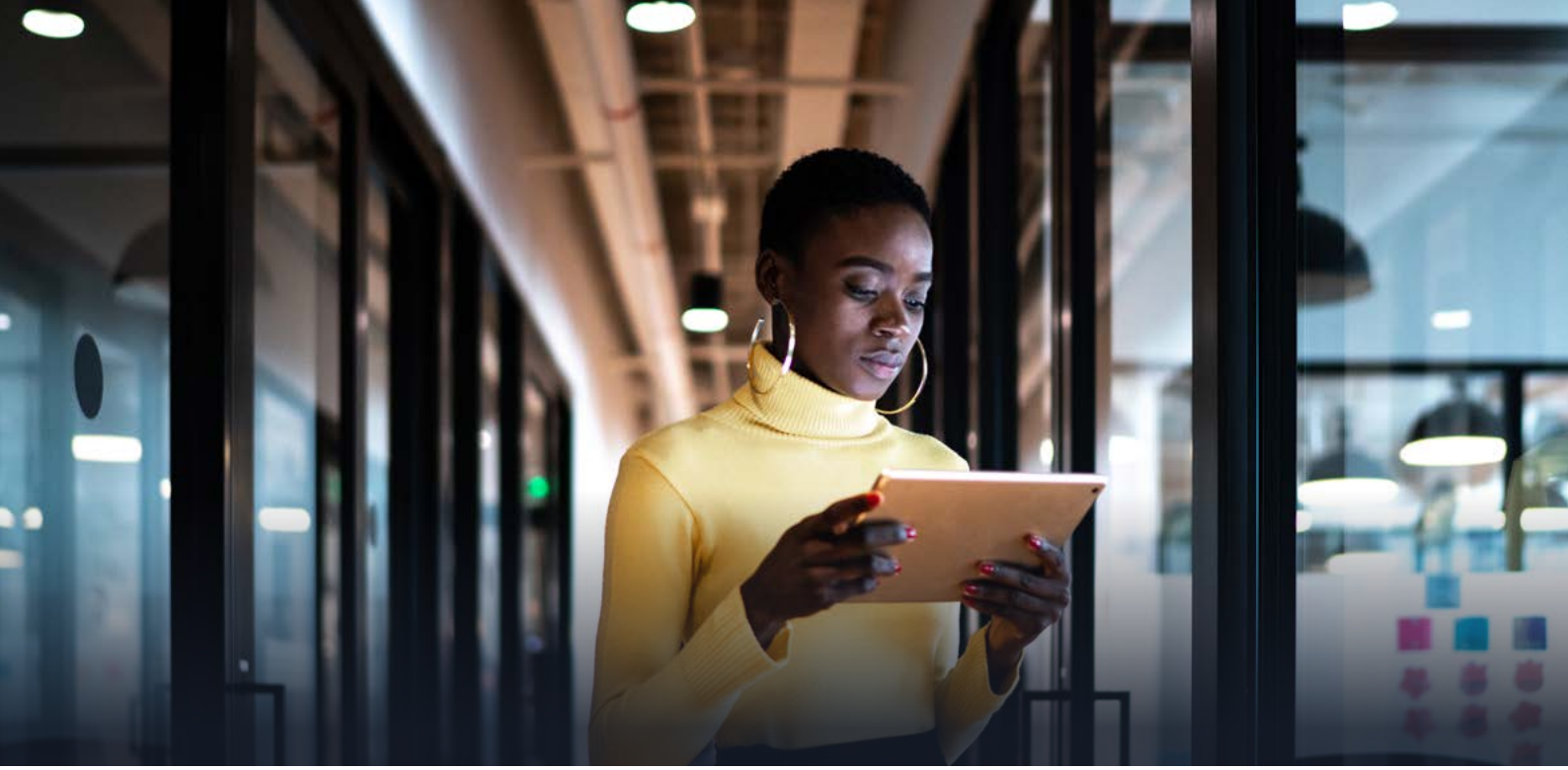
Critical Third Parties Act

Financial services firms increasingly rely on third parties to provide important business services. There are concerns that, if multiple firms rely on the same critical third-party, a disruption to its services could create systemic risks and threaten the stability of the UK's financial services sector.

The Financial Services and Markets Bill (FSM Bill), which is currently on its passage through the UK Parliament, will, therefore, provide the FCA, PRA and the Bank with the power to regulate third parties designated as "critical" in connection with the provision of services to financial service firms (firms) and financial market infrastructure entities (FMIs).

In July 2022, following the publication of the FSM Bill, the FCA, the PRA and the Bank published a Discussion Paper (DP) on Operational resilience: Critical third parties to the UK financial sector.[5] The DP sets out how the regulators might use their new statutory powers over CTPs, including minimum resilience standards, resilience testing and how they might identify potential CTPs for review and designation by HMT. The regulators anticipate consulting on the proposed measures in 2023 once the FSM Bill receives royal assent.

[3] https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss
[4] https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
[5] DP22/3: Operational resilience: critical third parties to the UK financial sector | FCA



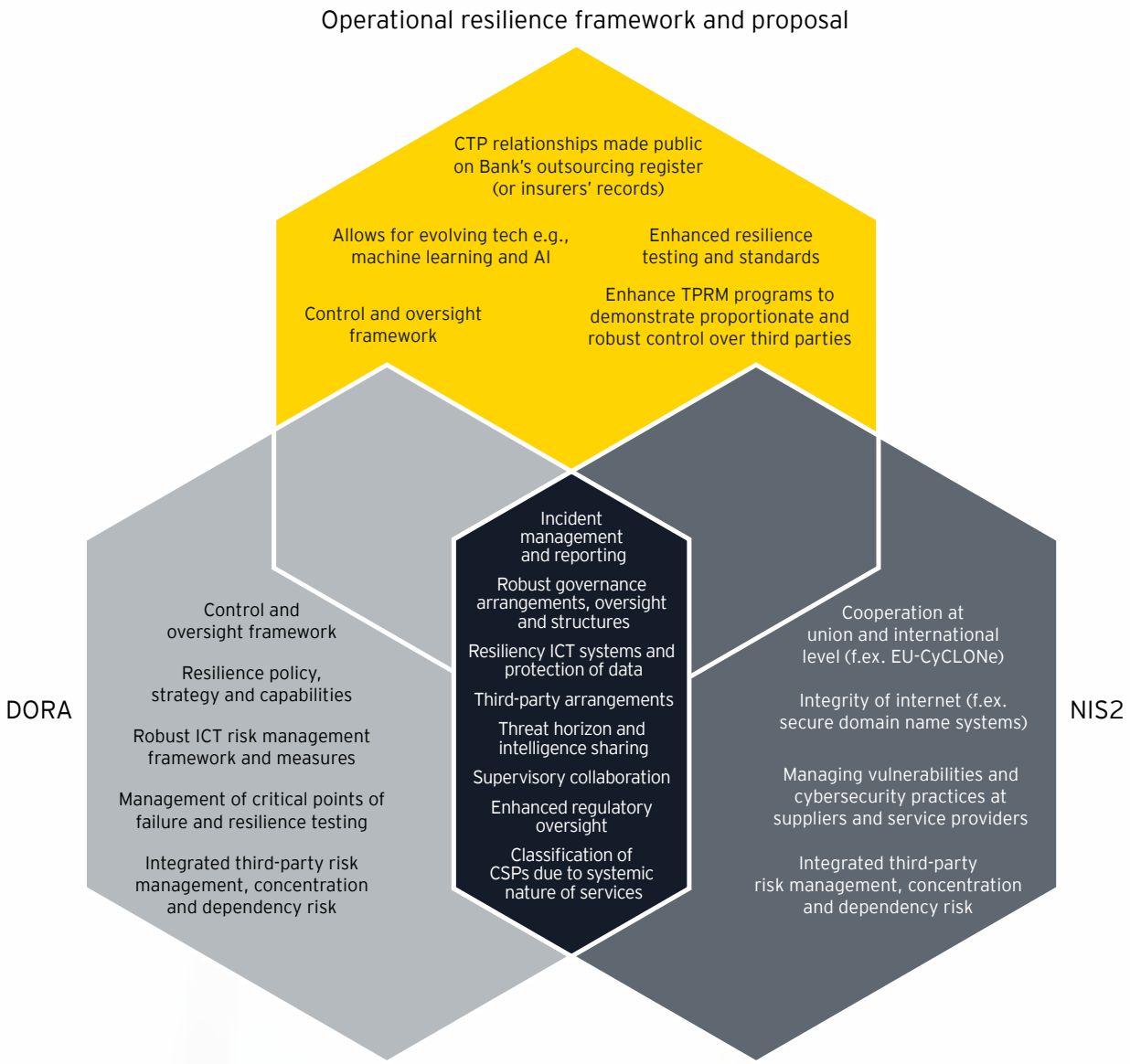
Key points to note:

- The FSM Bill provides that HM Treasury (HMT) may designate[6] a person who provides services to one or more authorized persons, relevant service providers[7] or FMI entities as a "critical third party" (CTP).
- Certain ICT third-party service providers are likely to be considered for designation as CTPs due to firms' and FMIs' increasing reliance on their services.
- If a third party is then designated as a CTP, the regulators will be able to exercise a range of powers with respect to the material services the CTP provides to the financial sector.
- Third-party providers of non-ICT services, e.g., claims management services to insurers or cash distribution, could also be considered for CTPs designation if deemed to meet the proposed statutory designation criteria.

[6] Designation is allocated if a failure in, or disruption to, the provision of those services could threaten the stability of, or confidence in, the UK financial system

[7] Examples of relevant service providers include electronic money institutions, authorised payment institutions, payment institutions or regulated account information services providers

Differences and similarities between DORA/NIS2/UK operational resilience framework



UK – Operational Resilience Framework	▸ Focuses on UK firms and financial market entities (FMIs) ▸ Focuses on important business services (IBS) provided to end users that impact regulators' objectives and sets the impact tolerance level for each IBS ▸ Outlines the expectation for outsourcing and third-party risk management ▸ The FSM Bill provides statutory powers to FCA, PRA/BoE to regulate third parties designated as critical in connection with the provision of services to financial services firms and FMIs
UK – Critical Third-Parties Act	▸ Focuses on how regulators will use statutory powers over Critical Third Parties (CTPs) and the potential measures that will be applied ▸ Outlines minimum resilience standards for CTPs and resilience testing of CTPs (including identification and review by HMT) ▸ Scope includes cloud-service providers and non-digital providers ▸ Includes enhanced oversight of CTPs by firms and regulators
DORA	▸ Focuses on organizations in the financial industry ▸ Focused on ICT governance, risk, resilience and ICT outsourcing ▸ Prescriptive on procedures, controls ▸ Enhanced testing and focuses on stress testing continuity and security ▸ Focuses on concentration risk and incident reporting/communications ▸ DORA builds on the NIS directive and addresses possible overlaps via a lex specialis exemption
NIS2	▸ Focuses on national level, EU level and international level and applies to more variety of industries ▸ Baseline for cybersecurity risk management and reporting obligations and focuses on network security and information security of essential and important services ▸ Focuses on many authoritive entities such as the CISRT, ENISA and the commission ▸ Focuses on aligning policies, authorative process of cyber security on a national level

FINMA circular "operational risks and resilience"

Switzerland

The updated FINMA Circular "Operational Risks and Resilience – Banks" introduces a new chapter on Operational Risk and Resilience for banks. Generally, in line with the BCBS principles on operational resilience, the goal of the new requirements is to improve the resilience of the Swiss financial market by strengthening the resilience of individual banks. The new requirements center around "critical functions" that need to be identified and adequately managed.

Key points to note:

- The requirements will enter into force on January 1, 2024 with a subsequent transition period for implementation.
- Currently, no similar requirements are in place or planned for insurance companies. Given FINMA practice, similar requirements are expected in the next five years.
- Key requirements follow the design of the BCBS principles for Operational Resilience.
- The Circular distinguishes between "large" (FINMA category 1–3) and "small" (category 4–5) banks, with several margins not applicable for "small" banks. This is in line with general FINMA practice.
- The adjustments to the qualitative requirements are principle based and technology neutral. Proportionality is adequately considered.

Timeline

	2022	2023	2024	2025 onwards
DORA/NIS2	**Q4** – Vote in general European Parliament plenary.	**Q1** – Publication into the Official Journal (OJ) and subsequent entry into force.[9]	ESAs to submit draft RTS to the Commission.[10]	Compliance with DORA takes effect and penetration testing should start. ESAs and the European Central Bank to submit draft RTS to the Commission.[11] Members states should have adopted and published NIS2 into national law.[12]
FINMA			**Q1** – Entry into force on January 1, 2024. Basic concepts need to have been defined. An inventory of critical services including impact tolerances and related critical processes and resources needs to be compiled.	**January 1, 2025** – First testing of impact tolerances in severe but plausible disruption scenarios need to be performed. **January 1, 2026** – Full framework implemented in business as usual mode.
Operational resilience framework*[8]	**December 23, 2022** – Discussion Paper DP22/3/ DP3/22 closes for comments.	**H1** – the FSM Bill is expected to receive royal assent. **Q3** – PRA/FCA and the bank discussion paper on "Incident and Outsourcing and Third-party Reporting" by firms is expected to be published. **H2** – the new CTP regime could commence **2023** – regulators anticipate consulting on the proposed measures once the FSM Bill receives Royal Assent.		

[8] Note: HMT will commence the CTP provisions, at a time of its choosing, by secondary legislation.

[9] Member states have 24 months to implement DORA into national law. A similar timeline is expected for NIS2 but Member States will have more discretion in the implementation of the rules as it is a Directive and not a fully harmonized regulation like DORA.

[10] ESA were mandated to submit draft RTS to the European Commission 12 months after DORA's entry into force.

[11] ESA and European Central Bank were mandated by the Commission to submit draft RTS 18 months after DORA's entry into force.

[12] Member states are expected to apply NIS2 21 months after entry into force.

How to get prepared – key questions

It is important that firms start working on their operational resilience journey early. Below we have provided key areas/questions that firms should consider when improving and aligning their operational resilience plans to either DORA, NIS2, FINMA and/or the UK Operational Resilience Framework.

Governance	▸ Are changes required to your company's governance structure to manage and perform oversight on resilience? ▸ Have resilience roles and responsibilities been considered and allocated throughout 3 Lines Of Defence? ▸ Have reporting lines been established to enable informed decision making of Board of Directors and executive management?
ICT risk management framework	▸ Have the company's existing registers of ICT information been reviewed to ensure its appropriateness? ▸ Does your company leverage opportunities to align to operational resilience business services? Has a mapping exercise been undertaken to integrate views of criticality and/or importance? ▸ Does your company apply "extreme scenarios" to identify risks linked to disruptions? And have the necessary measures been implemented to remain resilient?
ICT-related incident reporting	▸ Has a communication strategy for all stakeholders (i.e., internal, vendors, customers, third parties and authorities) been developed? ▸ Have business continuity plans been mapped to relevant critical functions and underlying processes and resources? ▸ Have key controls been defined, documented and mapped to critical functions?
Digital operational resilience testing	▸ Has the breadth, depth and frequency of testing for critical ICT systems been tested? ▸ If your company is an outsource service provider, have you reviewed your exposure to wider operational resilience requirements across your client base? ▸ Has an inventory of "critical functions" been compiled and maintained, including regular reporting? And has the board of directors approved it? ▸ Does the inventory include underlying processes, activities and resources (information and communication technology (ICT), data, facilities, people and third parties) for critical functions?
ICT party-risk management	▸ If you are an ICT provider, has a review on your compliance against operational resilience requirements been undertaken? Has it been documented that your frameworks are "comprehensive, sound and effective" to manage ICT risks? ▸ Has your procurement and third-party strategies been refreshed to consider concentration risk and resilience as part of the upfront and on-going third-party engagement? ▸ If a third party, do your operational resilience programs mirror the firms you are engaged to and have you provided them with some level of assurance?
Information sharing	▸ Do you participate in collaborative forums to share information relating to cyber threats and threat intelligence with other financial institutions? ▸ Has a process been implemented to ensure a secure transfer of information between financial institutions? ▸ Do you keep track of national divergences regarding the implementation of NIS2? ▸ If your organization operates in other major jurisdictions such as the UK, has a review been undertaken to identify alignment and possible divergences?

How can EY help?

EY teams regularly monitor regulatory developments, including in UK, EU, and Switzerland, especially regarding DORA, NIS2 Directive and the UK Operational Resilience Framework.

There may be some changes in the final versions of the proposed UK and European regulations. The current drafts provide ample context and indication for firms to begin preparing for implementation before the final publication.

Now is a good time for organizations to prepare. EY teams have performed several projects in this area and can help organizations with pragmatic and cost-effective options in this space, including:

- Delivering a global roll out to facilitate regulatory alignment and compliance
- Embedding resilience into firms' organization
- Reviewing their critical processes, services and assets
- Performing a gap analysis against the currently proposed drafts
- Sharing regulatory insights
- Sharing industry insights on existing and emerging best practices in relation to critical infrastructure arrangements

Contacts

EU

Borja Bosch
Manager, Operational Resilience
Ernst & Young Consulting CVBA/SCRL
borja.bosch@be.ey.com

Alan Marcelis
Manager, Operational Resilience
Ernst & Young Consulting CVBA/SCRL
alan.marcelis@be.ey.com

Switzerland

Tom Schmidt
EMEIA Financial Services Cybersecurity Competency Leader and EY Switzerland Cybersecurity Leader
Ernst & Young AG
tom.schmidt@ch.ey.com

Christian Schnewlin
Senior Manager, Business Consulting
Ernst & Young AG
christian.schnewlin@ch.ey.com

UK

Kanika Seth
EMEIA Financial Services Consulting Cybersecurity Leader
Ernst & Young LLP
kseth@uk.ey.com

Jack Armstrong
Partner, Operational Resilience, Financial Services Consulting
Ernst & Young LLP
jack.armstrong@uk.ey.com

Authors

Danielle Grennan
Senior Manager, EMEIA Financial Services Regulatory and Public Policy
Ernst & Young LLP
dgrennan@uk.ey.com

Nina Emordi
Senior Manager, EMEIA Financial Services Regulatory and Public Policy
Ernst & Young LLP
nina.emordi@uk.ey.com

Jane Hayward Green
Senior Manager, UK Government, Financial Services
Ernst & Young LLP
jgreen4@uk.ey.com

Pranathi Praveen
Senior Manager, Operational Resilience, Financial Services Consulting
Ernst & Young LLP
pranathi.praveen@uk.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 010615-22Gbl
ED None

UKC-026970.indd (UK) 01/23.
Artwork by Creative UK.

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com