cognizant®

Cognizant service offering

Digital Operational Resilience Act (DORA)

Introduction

In today's rapidly evolving business landscape, partners face numerous challenges that can hinder their ability to deliver top-tier solutions. At Cognizant, we understand the importance of these obstacles and are dedicated to addressing them head-on. This fact sheet highlights the critical aspects of various DORA challenges, including regulatory disparities, technological hurdles, and the complexities of third-party management. By understanding and proactively tackling these issues, we help ensure operational efficiency and robust data protection. Our goal is to provide a clear, comprehensive overview of these challenges and offer actionable insights for effective mitigation, empowering your business to thrive.

As an outsourcing partner we are affected by DORA and therefore know exactly how to address our clients' challenges

Key client challenges

Cross-Jurisdiction

- Differences in regulatory requirements timings
- Insufficient oversight/authority access to critical technology and infrastructure
- Maturity differences in technology, risk management & controls

Excessive ICT risks

- Fragmented and sometimes incompatible tools, technology supporting complex business processes
- Insufficient testing capability and/or tooling
- Reliance on manual processes e.g. incident management
- Concentrations risk related to ICT assets

Third party

- Mid cycle changes to contractual terms
- Providers do not yet have the required resilience and reporting capability
- Group/ entity concentration risks
- Market concentration risks

Data Security

- Inadequate data governance
- Alignment with disparate global data privacy and security requirements

Culture

- Shifting mindsets from individual disciplines to whole op model
- (Re)definition of roles and responsibilities across business services

Comms

- Resilience strategies accounting for social media-related customer flight

Financial regulators across the globe are now setting out new operational resilience requirements

All leading financial services regulators have recently issued guidelines and regulations for FS firms. Regulators expect banks and FS firms to have a strong enterprise-wide operational resilience to adapt to elevated threats. Technology-led business transformation, interconnected financial systems and high-profile instances of disruption have led to sharper focus on identifying and understanding what is material for resilience; setting standards of resilience; and testing against them.

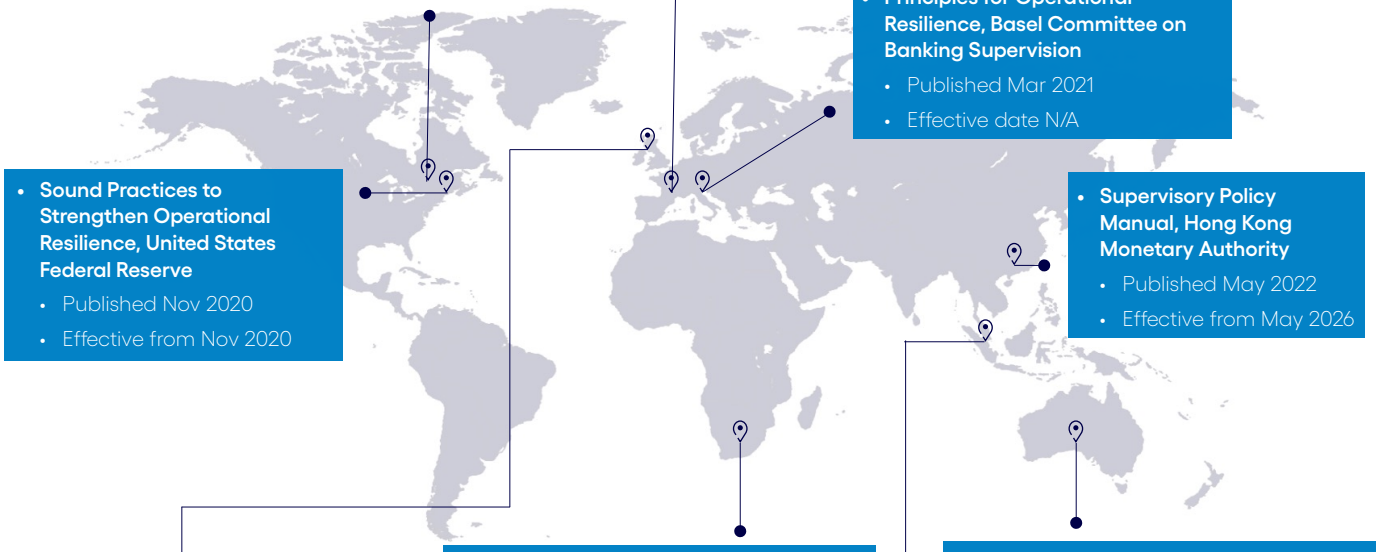
- **Operational Risk and Resilience Guidance, Financial Services Regulatory Authority of Ontario (FSRA)**
  - Published Jan 2023
  - Effective from Mar 2024
- **Operational Risk and Resilience Guidance, Financial Services Regulatory Authority of Ontario (FSRA)**
  - Published Jan 2023
  - Effective from Mar 2024

- **DORA (Digital Operational Resilience Act), European Commission**
  - Published Nov 2022
  - Effective from Jan 2025

- **Principles for Operational Resilience, Basel Committee on Banking Supervision**
  - Published Mar 2021
  - Effective date N/A

- **Sound Practices to Strengthen Operational Resilience, United States Federal Reserve**
  - Published Nov 2020
  - Effective from Nov 2020

- **Supervisory Policy Manual, Hong Kong Monetary Authority**
  - Published May 2022
  - Effective from May 2026



- **Directive on operational resilience D4/2023, South African Reserve Bank**
  - Published Jun 2023
  - Effective from Dec 2024

- Prudential Standard CPS 230 Operational Risk Management **(CPS 230), Australian Prudential Regulation Authority (APRA)**
  - Published Jul 2023
  - Effective from Jul 2025

- **PS 21/3 Building Operational Resilience, Financial Conduct Authority**
  - Published Mar 2021
  - Effective from Jan 2025
- **PS 6/21 Operational resilience: Impact tolerances for important business services, Prudential Regulation Authority**
  - Published Mar 2021
  - Effective from Mar 2021

- **Financial Services and Markets Act 2022, Monetary Authority of Singapore (MAS)**
  - Published Apr 2022
  - Effective from Mar 2024
- Information Paper **– Risk Management and Operational Resilience in a Remote Working Environment, MAS & The Association of Banks in Singapore (ABS)**
  - Published Mar 2021

Five pillars are constituting the DORA regulation

The five pillars provide DORA with a systematic approach, laying down a path to ensure that the financial infrastructure remains steady, adaptable, and resilient against ICT challenges.

ICT Risk Management (Art. 5 to 16)

ICT risk mgmt. framework centered on specific functions:

- Identification
- Protection and prevention
- Detection
- Response and recovery
- Backup, restoration and recovery
- ICT security training
- Crisis communication plans
- Use adequate systems, protocols and tools
- Conduct regular audits of the ICT risk mgmt framework

Incident management (Articles 17 to 23)

- Define and implement processes for managing and reporting ICT-related incidents
- Classify incidents and cyber threats by impact, including affected clients, transactions, and duration
- Establish procedures for monitoring, handling, and preventing repeat incidents
- Promptly inform clients about major incidents and cyber threats

Digital operational resilience testing (Art. 24 to 27)

Testing program to incl.:

- Vulnerability assessments and scans
- Open-source analysis
- Network sec. assmt.
- Gap analysis
- Physical sec. Review
- Scanning software
- Source code review
- Scenario based tests
- Compatibility tests
- Performance tests
- E2E and pen tests

Threat level penetration testing – at least critical functions and services

Includes critical live prod

ICT 3rd-party risk management (Art. 28 to 44)

- Assess & integrate 3rd-Party ICT risks into core risk strategy
- Consider criticality of services and potential impacts on their continuity & availability
- Guidelines for pre-contract assessment, contract contents, termination, stressed exit
- Audit rights and key contractual clauses
- Elevated obligations on outsourcing

Information-sharing arrangement (Art. 45)

Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools", with aim of:

- Enhancing OpRes of financial entities
- Raising awareness
- Taking place within trusted communities
- Protect sensitive nature of information shared

Firms need to strategize and budget for DORA compliance

Technology upgrades

Invest in advanced cybersecurity and resilient IT infrastructure to meet DORA's stringent standards. This includes hardware, software, and network improvements.

Training and Awareness

Develop comprehensive training modules and awareness campaigns to educate employees about DORA requirements, ensuring successful implementation and daily adherence.

Policy and procedure revision

Undertake a thorough review and update of internal policies and procedures to ensure full compliance with DORA mandates, covering data protection, incident reporting, and business continuity.

External consultancy needs

Engage with external consultants who specialize in DORA compliance for their expertise in seamless integration and strategic implementation across the organization.

Legal advisory and compliance audits

Allocate resources for legal counsel to ensure DORA's regulations are meticulously adhered to, and budget for comprehensive internal and external audits to validate and maintain compliance standards, encompassing the full audit lifecycle from preparation to follow-up.

Notes: Expected compliance efforts in perspective to FS players in the ecosystem

Operational resilience requirements will significantly impact firms – across many dimensions

Through our work on **operational resilience** for our clients we are seeing several common themes and challenges. We highlight the main ones below.

Excessive ICT risks

- Over-**reliance on manual processes** in the delivery of critical business services.
- Generating resilient practices across **fragmented and sometimes incompatible tools and technology.**
- Addressing **concentrations risk related to ICT assets** used across multiple entities and critical business lines.
- **Insufficient testing capability and/or tooling** to detect resilience vulnerabilities.

Third party risk management

- Amending **contractual terms** in the middle of a contractual period without impacting service provisions.
- Historically, third party service **providers do not have the required resilience capability** to collect/ monitor/ review data and respond to it/ report on it to current expectations [and in the case of DORA, to submit to direct FS regulatory oversight].
- **Group/entity concentration risks** where many legal entities and/ or business lines relying upon single/ few third-party critical services providers.
- **Market concentration risks** where actors in the FS market use the same one/two service providers for some activities (e.g. cyber security threat forensic response), and monitoring and mitigating the impacts of this

Group operations limitations

- Details of **regulatory requirements and their timings differ per jurisdiction.**
- **Insufficient oversight/ authority/ access to critical technology and infrastructure** across authorised/ accountable role holders.
- Establishing a proportionate **maturity baseline across entities in technology, risk management & controls, and data governance.**

Data privacy and security

- Overcoming **inadequate data governance** practices and infrastructure vulnerabilities.
- Implementing Operational Resilience expectations **while retaining alignment with disparate global data privacy and security requirements.**

Culture shift

- Shifting mindsets from addressing operational resilience in **individual disciplines like Business Continuity Planning, Third Party Risk Management, to embedding Operational Resilience end-to-end**, across the operating model, from the leadership down to staff.
- Clearly distinguishing between accountability and responsibility so that those setting the standards and those implementing the technology are clear on their roles e.g. an example we see is between information security and development engineering teams.

Customer journeys and communications

- **Undocumented/ unmapped customer journeys** and relying on corporate memory to undertake resilience related activities.
- Improving operational resilience event communications to external stakeholders, particularly to account for **social media management and impacts to customer flight.**

Authors

Habiba Rye
Associate Director,
Governance Risk & Compliance

Shardorn Wong-A-Ton
Strategic Technology
Integration Director

Philipp Meyer
Sr. Consultant

cognizant®

Cognizant (Nasdaq-100: CTSH) engineers modern businesses. We help our clients modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. Together, we're improving everyday life. See how at **www.cognizant.com** or **@cognizant**.

World Headquarters
300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters
280 Bishopsgate
London
EC2M 4RB
England
Tel: +44 (01) 020 7297 7600

India Operations Headquarters
5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai 600 096
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

APAC Headquarters
1 Fusionopolis Link,
Level 5 NEXUS@One-North,
North Tower
Singapore 138542
Phone: +65 6812 4000

WF 2742507