Multi-sector digital *operational resilience*

Applying lessons learned by the financial sector

Capgemini

Achieving digital operational resilience is challenging due to the balance needed between external, internal, and strategic challenges in an increasingly digital environment. Organizations are navigating the possibilities of digital transformation, which promises growth, innovation, and efficiency. Simultaneously, companies face increased exposure to cyber threats, geopolitical tension, and third-party supply chain disruption.

Establishing digital operational resilience requires an integrated solution across people, processes, and technology to help identify threats, prevent attacks, and resume operations smoothly and quickly if interrupted.

The pressure on organizations to ensure cybersecurity and digital operational resilience originates from regulations in multiple global jurisdictions, increasing digitization of business processes with complex interdependencies, and greater reliance on third-party providers for key systems.

Operations are at risk from physical damage, cyber-attacks, IT system outages, and third-party supplier failures. Natural hazards, war, political protests, and employment disputes are also potentially disruptive. The past two decades of legislation and regulation since Sarbanes-Oxley in 2002 indicate that operational risk resilience regulations globally are likely to grow in scope and detail.

Financial services – the first in line

The centrality of banking and financial services to economies makes the sector a recurring high priority for policymakers, political representatives, and regulators. The United States started the most recent drive for improved operational resilience in financial services in 2020 when the Federal Reserve published SR 20-24, its operations sound practices for the largest and most complex domestic banks and financial services companies. The EU followed with the Digital Operational Resilience Act (DORA).1 Since 2020, banks and other financial services providers connected with the EU have been completing transformation programs to comply with the act, a key part of the EU's Cybersecurity Strategy for the Digital Decade.

The UK added its own initiative in March 2022 when the financial regulator, the Prudential Regulation Authority (PRA), issued a supervisory statement on operational resilience, setting high standards for board accountability, regular basic testing (with annual as a minimum), and third-party contractual provisions for testing, contingency, and terminating relationships. These regulations have set a high standard for financial sector IT practices. Financial institutions are now mandated to have action and communications plans and disaster recovery strategies, including backups and data recovery.

The US National Institute of Standards and Technology (NIST) describes operational resilience as "the ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions. For the financial sector specifically, the Bank of England defines operational resilience as the ability of firms and the financial sector to absorb and adapt to shocks and disruptions rather than contribute to them.

Historically, operational resilience has mainly focused on market events, with financial and strategic resilience getting particular attention following the 2007-2009 global financial crisis. With increasing digital reliance, digital operational risk has evolved from being primarily internal to a risk that could affect many stakeholders: consumers, clients, employees, shareholders, and regulators. This shift has caused regulators to widen their focus to introduce minimum requirements and comparable standards beyond financial services companies to other industries and sectors.

Recently, many organizations in or connected with the European Union have had to prepare intensively for a raft of cybersecurity regulations, including: the Network and Information Security Directive 2 (NIS2, 2022), the Cyber Resilience Act (CRA, 2024), and for financial services, DORA (2023).4 NIS2 updated rules for a common level of cybersecurity across the EU, broadening the scope of the 2016 NIS directive to include more sectors, including specific reference to supply chain security. The CRA introduces EU-wide cybersecurity requirements for hardware and software products to avoid overlapping requirements.

These acts followed the 2019 European Cybersecurity Act, which strengthened the EU Agency for cybersecurity (ENISA) and introduced a certification framework for ICT products and services. Each piece of legislation required the evaluation of ICT relationships on the basis that third parties can be a prevalent source of operational failures.

1. Capgemini, *Navigating DORA*, November 2023
2. NIST, *Glossary, operational resilience*, accessed October 8, 2024
3. Bank of England, *Operational resilience of the financial sector*, accessed October 23, 2024
4. European Parliament, *Fighting cybercrime: new EU cybersecurity laws explained*, accessed March 19, 2024
5. European Council, *Cyber resilience act*, October 10, 2024

Frameworks for success

As operational resilience has moved up the agenda, the number of frameworks available to enterprises to manage it has expanded. NIST published its framework for cyber-physical resilience in 2024, while the American Productivity & Quality Center (APQC), World Economic Forum (WEF), and ISO 207001 also offer their own relevant to information and cybersecurity operational resilience.

DORA formalized ICT frameworks for banks, insurance companies, investment firms, and other financial service providers (FSPs). They had to examine the resilience of their ICT infrastructure through a risk management lens in a way that had not happened before. They have applied frameworks to ensure comprehensive, thorough transformation. The approaches used to define the levels of criticality of their digital assets, i.e., identifying critical domains and related residual risk, are applicable in other sectors to assess risks and implement controls.

With DORA financial services companies as case studies, an operational resilience risk management framework has proven essential for comprehensive transformation. It gives a view of all activities, functions, and components that will be affected by design or remediation, including critical processes and supporting digital assets. Its ultimate purpose is to confirm that business execution is carried out with business and IT resilience in mind and that continuous improvement is built into the lifecycle. It highlights critical business services, where company board oversight is required, and any policy deficits. Defining these and related protective security measures is crucial for maintaining security and supporting the requirement for a board of directors' attestation of control of digital operational resilience.

[6] NIST, *Operational Resilience Framework*, September 2024
[7] WEF, *Risk Proof: A Framework for Building Organizational Resilience in an Uncertain Future* July 2022

Shared responsibility for resilience

It is important to identify dependencies and security responsibilities across IT/OT infrastructure or supply chains, especially for ICT vendors linked to critical assets, including cloud services. This ensures that all parties involved are aligned. Additionally, incident reporting is now mandatory, requiring organizations to respond swiftly to disruptions while collaborating with peers and regulators. These more sophisticated demands emphasize how digital operational resilience needs to be proactive, standardized, and integrated so that organizations can quickly adapt to and withstand the latest threats.

When IT architecture was entirely on-premises, this was an organization's own responsibility, but with cloud-based infrastructure, some of this responsibility transfers to the cloud service provider (CSP). The shared responsibility model specifies how responsibility for infrastructure, compute, and applications is divided between an organization, its CSP, and third parties.

The cost of disruption and fines for operational failures

The impact of an operational resilience event goes beyond the immediate fallout. An affected critical system, or an entire organization, could be out of commission with potentially disastrous consequences for commercial viability.

Along with the threat to commercial activity and interruption of services, regulatory fines focus the minds of compliance, legal, and company boards. Under DORA, for example, offending organizations may be subject to a periodic penalty payment of 1 percent of average daily global turnover (based on the preceding year) for up to six months until compliance has been achieved.

In 2023 the US Securities and Exchange Commission (SEC) marked developments in cybersecurity and risks by issuing its set of rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. The rules require registrants to disclose material cybersecurity incidents they experience within four business days and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance.

When news of operational failures due to improper business or market practices becomes public knowledge, share prices decline on average nearly 2.9 percent over 120 days versus peers, or 2.8 percent below peers 60 days after disclosure. A company's reputation may be permanently damaged in the eyes of customers, the market, investors, and regulators.

8. McKinsey, *Response and resilience in operational risk events*, March 30, 2023
9. SEC, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, July 26, 2023

Attention to the right detail – lessons from Sarbanes-Oxley

In complying with Sarbanes-Oxley Act (SOX) Section 404 – the requirement to assess a company's internal controls over financial reporting – regulators and corporate officers have learned to focus on governance, materiality, and risk-based assessment. Within this scope come critical processes and underlying digital assets.

The following milestones are key to determining where to focus:

- A complete overview of business processes and digital assets
- Definition of critical processes and assets
- Assessment of third parties involved
- Oversight of control over those critical assets
- Establishing governance and reporting frameworks

The ideal end state for an operational resilience transformation project is for a company to create the above, which then becomes a foundation for future compliance programs. Once this is set, a modular continuous compliance system drastically reduces the resources necessary to update policies, produce reports for audits, and provide a view on third-party compliance. A fully automated system enables a company to quickly view its compliance status via dashboards and make data available to auditors with relevant evidence.

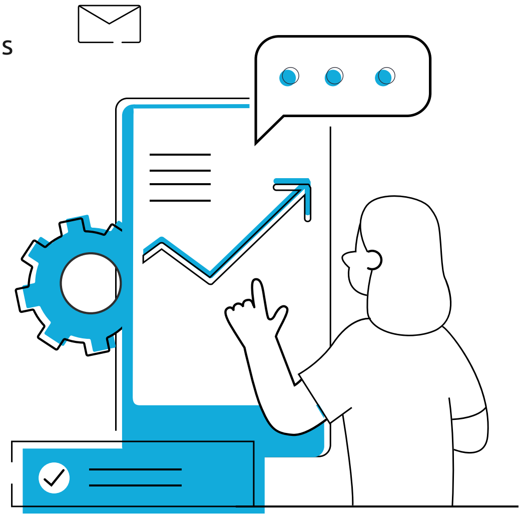
Paper compliance alone is not enough – automation is key

The financial sector's campaign to reach digital operational resilience insight and compliance revealed differences between companies that dug deep into their systems and practices to properly test for vulnerabilities and companies that were complying with policies and governance, but would only achieve "compliance on paper," i.e., minimum compliance, by the deadline.

While the numerous regulations across different jurisdictions may be very similar, it is where they differ that can cause non-compliance breaches or operational failure for businesses with a global network or extensive supply chain. While policies and governance are strategically important, only technology fully integrated with automation will lead to an operationally resilient organization. This starts with designing disaster recovery and crisis management plans with vulnerability scans, network assessments, and penetration assessments.

Organizations must be crisis-tested to achieve control of every critical system. Other sectors can learn from the example of the financial services sector's operational resilience tests conducted by impartial, external parties to probe threat-detection capabilities and find vulnerabilities.

Realistic testing means thoroughly testing whole systems offline under simulated crisis conditions. When that system is a trading or payment platform used by thousands of employees or customers, it is a significant operational commitment and commercial cost. Considering the alternative. This is essential for operational resilience planning, when one considers the alternative.



Case Study

Resilience transformation for a global bank's retail banking division

A three-month transformation program designed to:

- Ensure total clarity of third-party supplier risks
- Test all threat scenarios
- Guarantee readiness for business continuity and disaster recovery planning

The project team found thematic gaps across multiple business lines.

Fundamentally, the bank needed a clearer decision-making process and an action plan for remediations in time for Q4 2024 executive board attestation ahead of the DORA 2025 deadline.

During the project, we identified a risk at a third-party supplier, a printing firm, which was exposed to external threats. This had not appeared in previous mapping of critical business services and dependencies.

Challenges identified

- Siloed approaches were leading to inconsistencies
- Unclear rationale in defining business services
- Incomplete testing of various risk events
- Continuity plans were not stress-tested and lacked specificity

Threats prioritized

An initial review identified three key service outage threats:

- Financial market infrastructure (FMI) disruption
- Cyber events impacting customer-facing applications
- Risk of public cloud loss

Phase One:
Designing an end-to-end resilience and remediation program for the retail banking division.

Phase Two:
Establishing a group-wide communications stream.

Retail business end-to-end work stream-

- Decision governance: scoped and applied regulatory guidance for a consistent decision-tree structure
- Set a clear rationale for business service definition
- Workshopped existing processes via defined scenarios for priority threats
- Completed remediation design and planning across ICT recovery, contingent processes (payments, communications, funding), supplier contingencies and assurance, FMI, and enhanced scenario testing strategy

Group communications workstream

- Analysis and definition of a new communications strategy across key threat scenarios to be applied to content, method, format, and timing approach to fit any system outage circumstances

Delivering continuous compliance for operational resilience

What begins as technological development in the financial sector often spreads to others, particularly national infrastructure, manufacturing, life sciences, energy and utilities, and the food industry. As these sectors' digitalization has increased in the form of the Internet of Things, operational technology, and the application of artificial intelligence, their threat profiles and attack surfaces have grown too.

The evolution of digital operations means practices for operational resilience must continuously renew to face technological advances, digital transformation, geopolitical events, and criminal innovation.

Capgemini can sustainably support clients with their digital operational resilience transformation to reach a state of continuous compliance supported by automation.

Experts to contact

Marieke van de Putte
Global Portfolio Lead,
Continuous Compliance and
Operational Resilience
marieke.vande.putte@capgemini.com

Desre Sheen
Global Invent Lead,
Operational Resilience
desre.sheen@capgemini.com

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided every day by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of nearly 350,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering, and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the future you want | www.capgemini.com

GIS_072025_SB

For more details contact:

cybersecurity.in@capgemini.com

Capgemini

Copyright © 2025 Capgemini. All rights reserved.