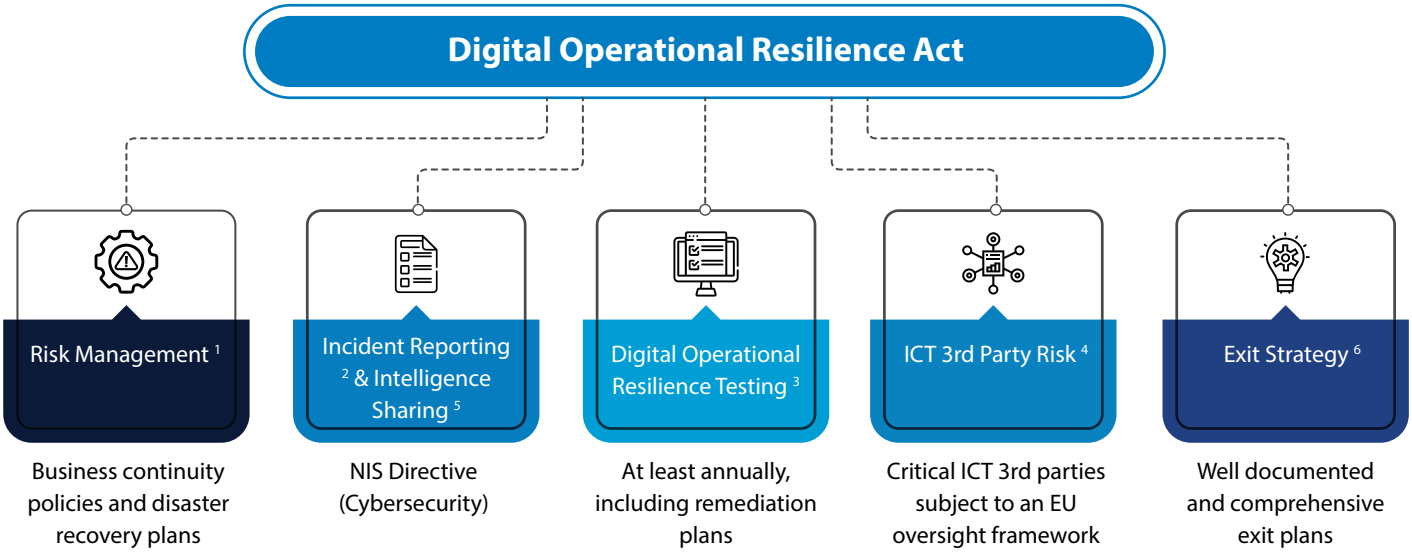
DIGITAL OPERATIONAL RESILIENCE

DORA – New European Regulatory Requirements

The Digital Operational Resilience Act (DORA) is a European Central Bank regulatory compliance requirement that came into force on the 16th January 2023 with adherence mandated by 17th January 2025. The objective of DORA is to strengthen the operational resilience within all financial markets. In the event of severe operational disruption, financial entities must ensure that they can provide continued operational resilience. In order to comply, a financial entity must demonstrate their ability to build, assure, and review their operational integrity and resilience for their ICT related capabilities including those provided by a 3rd party.

Any financial entity that fails to comply may be subject to a fine of 1% of their prior year average daily turnover.

Main Pillars of DORA



Source: DORA Proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1

1 Chapter II- Art 5-14 2 Chapter III- Art 15-20 3 Chapter IV- Art 21-24 4 Chapter V- Art 25-39 5 Chapter VI- Art 25-39 6 Chapter VI- Art 25-39

What do financial institutions normally do as part of operational resilience?

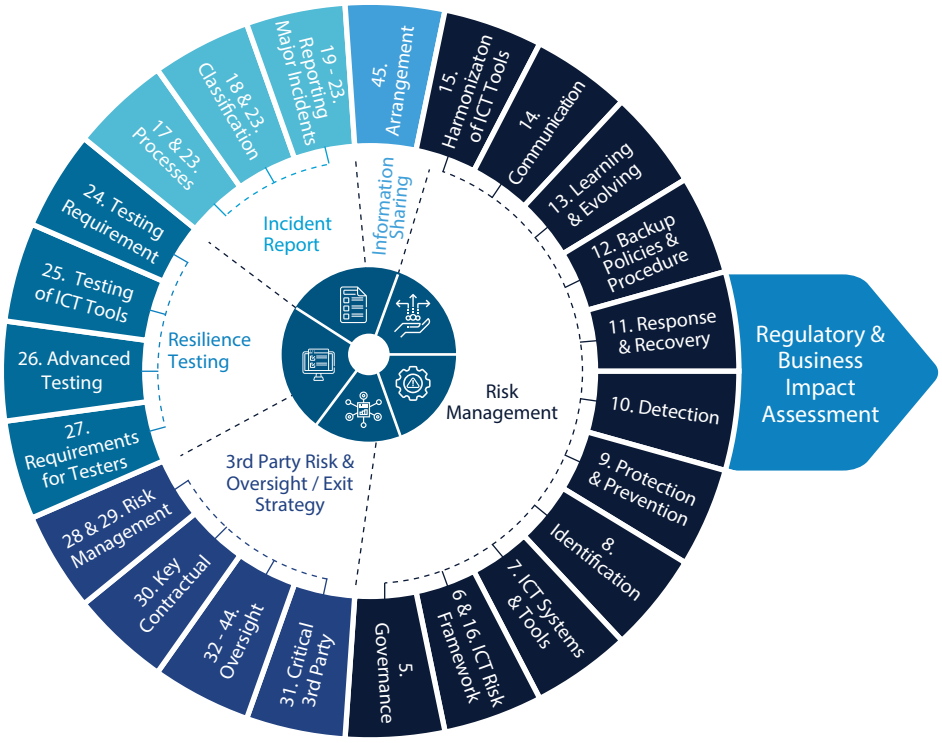
- Performance testing
- Disaster recovery testing
- Regression testing
- Internal risk management
- Scanning software solutions

Ops resilience existing framework vs **DORA expectations**

What is additionally required as part of DORA?

- Identification of **Critical Business Services** (Article 5)
- End-to-end **Service Chain Mapping** for customer journeys (Article 8)
- **Vulnerability Assessments** (Article 25)
- Assessments at least every year (Article 6)
- **Scenario-based testing** (Article 25)
- **Cyber threat information sharing as per regulatory guidelines** (Article 45)
- **Threat-led Penetration Testing** (Article 26)
- **Impact tolerance for** critical business services (Article 6)
- **ICT exit strategy** (Article 28)

An impact assessment framework to identify the non-compliance areas as a starting point for the DORA Program



Infosys' Impact Assessment Framework

Full Compliance
Articles requiring evidence gathering to show compliance

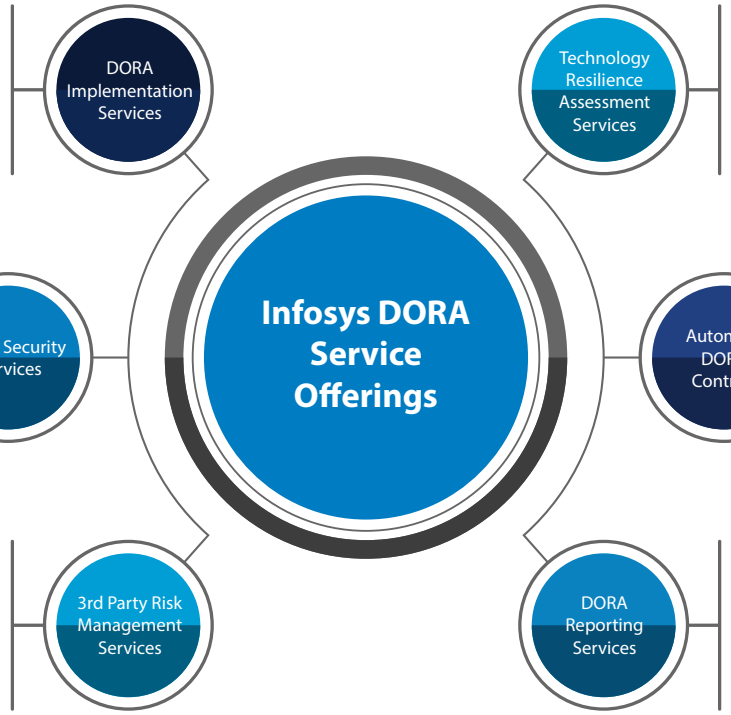
Non-compliance
Articles requiring new capabilities or controls to be implemented

Future Review
Further detail required via Regulatory Technical Standards

Partial Compliance
A hybrid approach of evidence gathering with an increase in BAU workload

Infosys' suite of implementation services for DORA - post identification of gaps, Infosys offers a suite of implementation services for DORA

- Implementation and execution-focused advisory services
- Expertise and capability combining people and frameworks
- Mitigate risks through implementation of improvements based on DORA assessment/audit



Infosys point solution for DORA

Infosys SRE Platform

- Predefined and customizable assessment templates for Failure Mode Effect Analysis, No Single Point of Failure Analysis, and Chaos Engineering
- Questionnaire assessment
- Identifying vulnerability and recommendation

Infosys Continuous Compliance Monitoring (CCM) System

- The Infosys CCM Solution enables financial organizations to improve their risk and compliance posture by automating the internal control monitoring and testing environment and lowering the cost for manual testing

For more information, contact askus@infosys.com

Infosys®
Navigate your next