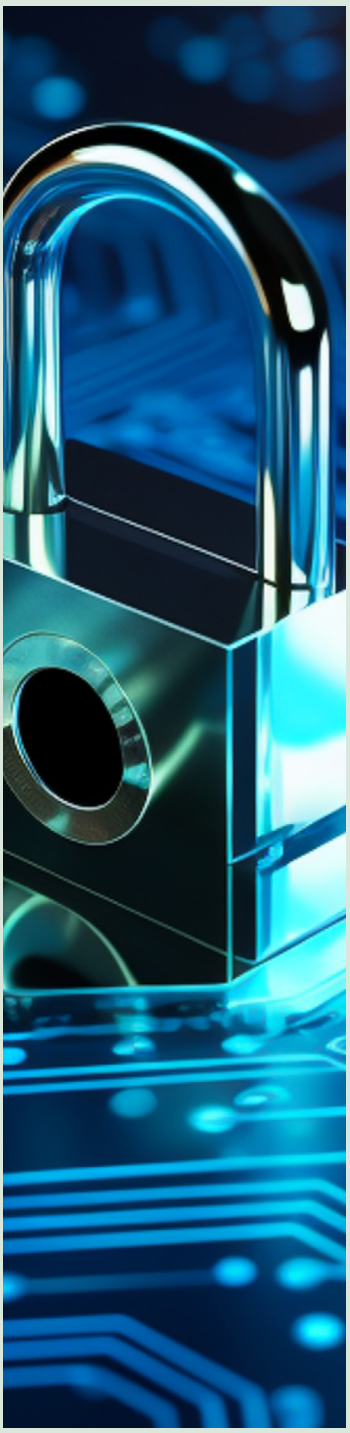
WHITE PAPER



STRENGTHENING CYBER RESILIENCE WITH DORA & INFOSYS' 3R STRATEGY TOWARDS COMPREHENSIVE ADOPTION

Abstract

This whitepaper examines the Digital Operational Resilience Act (DORA), that came into effect in Jan 2025 and is applicable to the EU. It provides a detailed overview of the act, its applicability to financial institutions, ICT, and third-party providers. The whitepaper highlights the importance of cyber resilience for enterprises, current implementation challenges, Infosys' recommended best practices, thought leadership, recommendations and accelerators.

Infosys®
Navigate your next

Insights

The following areas are thoroughly examined further to enhance readers' understanding of DORA's significance and to outline the subsequent steps

- **Why should we focus on DORA? What is the current situation?**
- **What are the challenges faced by enterprises in building resilience?**
- **How can Infosys solve? Our framework to help enterprises become more resilient**
- **Our key learnings and best practices**
- **Our views and opinions & a peek into the future**

DORA – what does it mean and its impact?

The Digital Operational Resilience Act (DORA), that came into effect in Jan 2025, aims to establish a uniform regulatory framework across the European Union (EU). It applies to ICT (Information and Communication Technology) providers, financial enterprises, and third-party service providers. Given the rise in cyber threats, system outages and third-party ICT failures, digital resilience is more critical than ever. To safeguard against disruptions and uncertainties, organizations must not only implement DORA but also adopt a holistic approach to operational resilience.

Why should we focus on DORA?

World Economic Forum (WEF) identifies with the significance of cyber resilience in today's digital world. Based on the insights, cyber resilience is crucial as digital systems and services are fundamental to the economy and society. Major cyber incidents can significantly disrupt operations, finances and reputation. Ensuring cyber resilience allows organizations to mitigate these impacts, maintain essential services, protect stakeholder confidence and preserve strategic value. It also draws the attention of leaders to implement proactive strategies and continuous investment to ensure long-term growth and stability.

With its current effect in Jan 2025, enterprises continue to face challenges either in implementing or enhancing their digital operational resilience towards achieving compliance. Various analysts have provided their insights, highlighting the significant effort required for successful compliance. As per FS-ISAC (**Financial Services Information Sharing and Analysis Center**) applying DORA faces challenges such as tight compliance deadlines, securing management buy-in and coordinating multiple teams. Additionally, international applicability and stringent third-party management requirements add to the complexity.

June 24th, 2022

Adoption of DORA

EU institutions adopted DORA as it was approved

January 16th, 2023

DORA officially enters into Force

Marks the adoption of the DORA as an official EU Regulation

January 17th, 2025

DORA implementation period ends

DORA will be entirely binding and applicable for all member stat

DORA is first game-changing legislative regulation in the European financial ecosystem that helps FIs to grapple with digital revolution

What is the current situation?

Enterprises are at varied levels of implementations, while large enterprises with a robust infrastructure are ahead in making progress, smaller or mid-size enterprises may still have challenges due to limited resources or budget.

For instance, ING, a leading European bank, proactively began understanding the DORA requirements as early adopters in 2024. The initial steps involved conducting an impact assessment and gap analysis of existing practices against the new DORA requirements. Subsequently, they identified the relevant applications and infrastructure. Following this, critical business applications were identified and the implementation process towards regulatory compliance is currently underway.

Overall, though there is considerable focus across with few ahead as early adopters, many enterprises are still navigating through challenges in fully implementing DORA and enhancing their digital operational resilience.

What are the challenges faced by enterprises in building Resilience?

Building resilience helps protect the entire ecosystem of enterprises and customers. However, enterprises face various challenges due to requirements in investment in building, maintaining the right infrastructure, comprehensive risk management, backup and recovery plans. Failure in compliance with regulatory requirements can also impose heavy fines.

Few key challenges include:

Legacy Landscape:

Organizations face challenges in building resilience and keeping pace for legacy environments. Constraints in existing infrastructure can hamper the implementation of resilience measures.

Cybersecurity Risks:

Any compromise in cybersecurity can lead to significant financial losses and revenue impacts.

Investment and Upgrades:

Continuous investments and upgrades are essential to sustain and enhance cybersecurity measures both from resources & technology perspective.

Response and Recovery Strategies:

Enterprises may lack versatile strategies for response and recovery due to inadequate planning, uncertainties, insufficient risk management and budget constraints.

Choosing the Right Partners:

Selecting appropriate partners for technology and service provision can become complex.

Organizational Culture Changes:

Shifting the organizational culture to prioritize resilience and adaptability can also be challenging but is necessary for long-term success.

How can we resolve?

While DORA is the most important regulatory initiative for the financial institutions of the EU region, a holistic approach, identification of early risks, and comprehensive strategy will help the enterprises towards early adoption.

Enterprises need to look at their risk posture, model their responses and plan for robust recovery strategies in an integrated approach towards operational resilience. Infosys recommends a **3R approach - Risk assessment, Response, Recovery** towards building effective and efficient resilience

Infosys recommends a 3R approach - Risk assessment, Response, Recovery towards building effective and efficient resilience

Is Risk assessment your shield against uncertainty?

Any potential risk not identified early in life cycle or managed can lead to major business disruptions, attracting loss of reputation, financial implication including penalties.

An end-to-end assessment would be the right starting point to understand the gap between As-Is and expected state, create the roadmap to address the gaps, implement the right strategies & mitigate any potential risk.

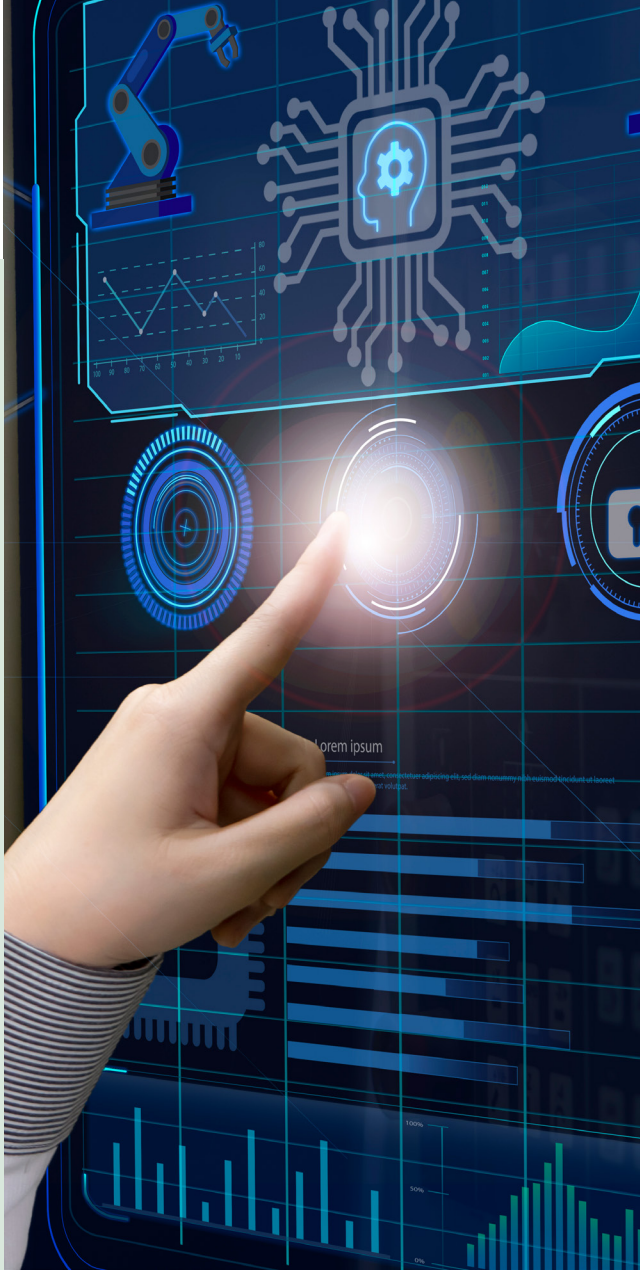
A well-rounded strategy should include periodic assessments with frequencies of the assessments well defined, governance and metrics defined for measuring success.

Key pillars of strategic Assessment solution across various dimensions of DORA

ICT Risk Management	ICT-related incident management, classification and reporting	Digital operational resilience testing	Managing of ICT third-party risk	Information-sharing arrangement
• Information security policy • ICT risk management framework • Data Loss Prevention (DLP) policy • ICT business continuity policy	• Incident management process • Early warning indicators • Communication Plan • Notification Mechanisms	• Risk-based testing approach • Threat-led penetration testing • Third-party penetration test report. • Contracts with external testers	• Contractual arranagements • Third Party Risk Management Policy • Skill and knowledge • Subcontractor Risks assessments • Exit strategies	• Other financial entities information sharing & strategies • Protection of personal data • Defined condition of participations • Notification of competent authorities

Is your response framework ready for any challenge?

For ensuring effective Response procedures towards building resiliency, looking at all key areas is crucial implementation.



Training and Awareness:

- Enterprises need to ensure the ICT providers are aware & trained both towards understanding the regulations and response mechanisms
- Leadership buy-in and alignment towards overall strategies is key to success
- Identifying the right stakeholders, specific role-based training programs, staying updated with regulatory changes, are essential components for building organizational resilience

Governance and Practices:

- Developing a robust governance mechanism towards implementation of Gaps identified from Risk assessment
- Conducting assessments with a defined scope and frequency, customized to align with the organization's size and risk posture

Technology:

- Identification on inventories and building required infrastructure
- Real time monitoring & analysis with SIEM
- Looking for an integrated platform like SOAR leveraging the automation & improve response efficiency

Why robust resilience is critical aspects for DORA compliance?

Resilience: Even in a well thought risk implementation model, an Incident can arise due to evolving threats and complexities. Continuous service and operations are crucial with swift and accurate recovery model.

A well-rounded strategy implementation should integrate key aspects of data governance, security measures, and robust defenses against cyber vulnerabilities.

Data Managment

- Data compression
- Data Migration
- Data Governance

Data Protection

- Backup data
- Recover Data
- Disaster Recovery
- Archiving

Cyber Resilience

- Ransomware protection
- Anomaly detection

Infosys recommends the industry proven S3 4D framework for DORA regulation

Diagnose

As-is state assessments can help FIs along the entire journey towards DORA compliance by assessing the current readiness and proposing measures to meet the regulatory requirements

Design

Understand the current state and design the target state to achieve DORA compliance as per the regulatory requirements

Deliver

DORA framework will be delivered as per the client requirement. Support clients in the organizational and technical implementation of DORA

Defend

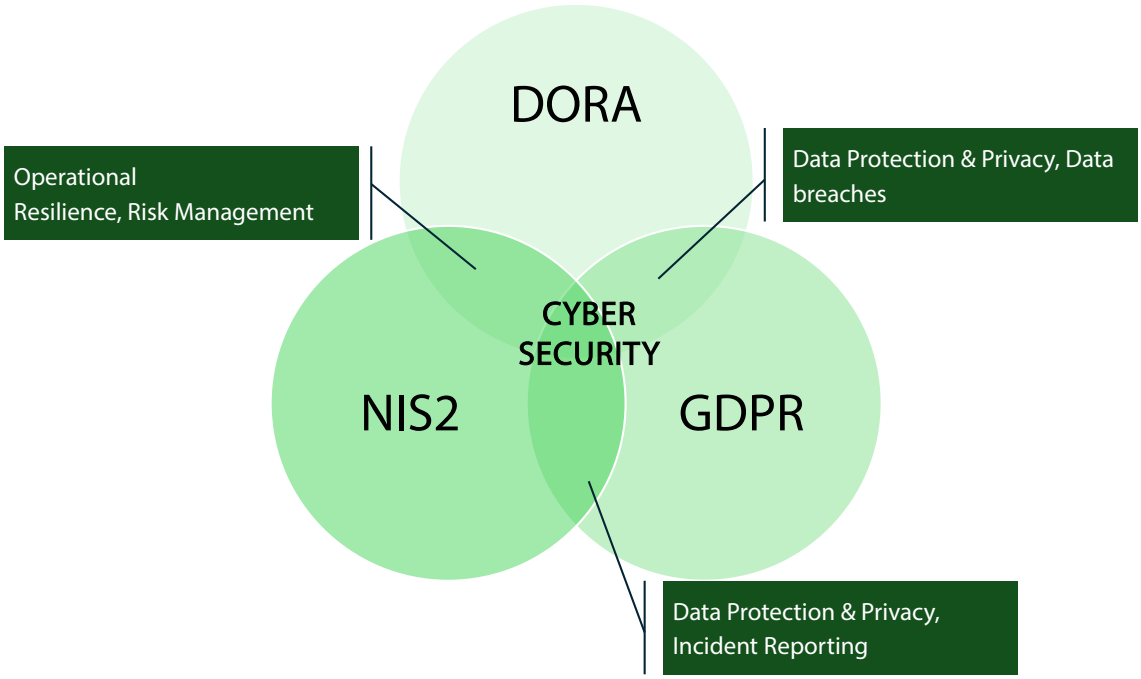
Compliance operational framework will be implemented post-delivery which will in turn proactively guard the FIs against future cyber threats.

Recommendations

What are our learnings /best practices?

Leveraging an overarching strategy towards regulations and directives

Though DORA is recently introduced for financial sectors in the EU region, the organizations would be complying with other regulations already like GDPR, NIS2 which fall under broader scope of cyber security. Hence organizations need to look at commonalities between these as per regulations already implemented.



In addition, implementing standards like ISO27001 can help in achieving the compliance across these regulations. ISO is a comprehensive framework for implementing and improving the Information Security Management System.

Choose the right collaboration partner

Choosing right partners to implement DORA would help the enterprise to focus on core business while leveraging the knowledge and expertise from the partnership.

Partners will help to have an independent, yet comprehensive outlook integrating various aspects. This helps to scale, optimize and operate at optimal cost.

Leveraging AI for effective implementation

AI-based solutions can support monitoring, threat detection, early predictions, analysis, deriving insights, auto resolution. This further would enterprises strengthen their security measures and protection.

Why is cyber resilience increasingly crucial for futureproofing and mitigating technological disruptions?

Emerging technologies such as AI, quantum computing, IoT, and blockchain etc. present significant opportunities as well as challenges for cyber resilience. Quantum computing threatens current encryption methods, AI enhances threat detection but introduces risks like adversarial attacks, IoT expands the attack surface and blockchain offers secure transactions but requires robust security measures.

To address the ever increases challenges, analysts at the World Economic Forum emphasize the importance of adopting a proactive and collaborative approach that integrates security, resilience, and sustainability. Utilizing data-driven insights and incorporating resilience by design principles are essential strategies. This proactive approach will help organizations improve their cyber resilience and safeguard their digital assets.

The "**resilience by design**" approach recommended focuses on building systems that are inherently robust, adaptable, and capable of withstanding and recovering from cyber threats. This involves integrating resilience principles into the design and development stages of technology, ensuring that security and resilience are foundational aspects rather than afterthoughts. The goal is to create systems that can maintain essential functions and quickly recover from disruptions, thereby enhancing overall cyber resilience.

The Digital Operational Resilience Act (DORA) provides a comprehensive framework for ICT risk management, incident reporting, and third-party risk management, addressing the challenges posed by emerging technologies. As these technologies continuously evolve, the adoption of DORA will ensure that financial institutions are better equipped to handle these challenges, making it an indispensable framework for operational resilience.

Infosys CyberNext Platform - Your one stop solution

Infosys provides the right solution to DORA implementation integrating the 3Rs strategy augmented by the CyberNext platform. The platform enables you to collaborate, optimize your security stack, and get the right recovery solution for Enterprise customers, thus offering a robust framework as well as platform towards resiliency.

References

1. Exploring DORA | ING
2. DORA Act
3. Digital Operational Resilience Act (DORA) - EIOPA
4. Digital finance: Council adopts Digital Operational Resilience Act - Consilium
5. FSISAC_DORA-ImplementationGuidance
6. WEF_Unpacking_Cyber_Resilience_2024.pdf
7. WEF_Navigating_Cyber_Resilience_in_the_Age_of_Emerging_Technologies_2024.pdf
8. DORA The Romania Journal
9. DORA – Digital Operational Resilience Act | Italy | Global law firm | Norton Rose Fulbright
10. Study: financial services organizations show progress in implementing the new EU regulation on digital operational resilience - The Romania Journal
11. Managing Digital Operational Resilience Act (DORA) Compliance | Informatica
12. DORA Compliance with Vectra AI
13. Cyber-security regulation - Wikipedia
14. Digital Operational Resilience Act (DORA) - ISC2 Community

Glossary

DORA	Digital Operational Resilience Act
ICT	Information and Communication Technology
NIS2	Network and Information Security directive
ISO	International Organization for Standardization
SOAR	Security Orchestration, Automation and Response
SIEM	Security Information and Event Management

About the Author

Saratha Narasimhan

Principal Consultant

Saratha has 17 years of IT experience, specializing in consulting and driving delivery excellence. As a solution architect with the Infosys' Data Privacy & Protection team, she specializes in implementing compliance standards and policies. Her expertise includes implementing regulatory requirements and industry best practices across various domains.

About the Co-authors

Lochan Brid

Senior Consultant

Lochan has 18+ years of experience in Consulting and Presales for cybersecurity services. She has been part of Infosys' Data Protection CoE team and has been focusing on building Security for AI solutions. She is certified in **Generative AI Fundamentals** - Databricks, **AI Governance** - OneTrust & Securiti.ai, **AZ-900** - Microsoft Azure Fundamentals, **SC-900**a - Microsoft Security, Compliance, and Identity Fundamentals

Aditya Yerramilli

Principal Consultant

Aditya has 20+ of IT experience in Governance Risk and Compliance having worked in ensuring Compliance, Risk Assessments, Audits related to IS0-27001, ISO-27701, ISO-42001 AI Lead Implementor, GDPR, CCPA, PDPL, DPDPA 2023. He has been part of projects involving Data Protection & Privacy Architecture work, Protection and Privacy Proposals & Solutioning, Data Protection Officer Advisory, AI Compliance & Governance Advisory & Consulting. He has expertise in driving strategy for Organizations to improve on their overall security, Data Protection, Data Privacy, AI Security posture. He is certified in **CIPP/E - IAPP, AI Governance - Securiti.ai.**

For more information, contact askus@infosys.com

Infosys®
Navigate your next