TECH
mahindra

Whitepaper

Digital Operational Resilience ACT:

A TechM roadmap

Abstract

Digital Operational Resilience Act (DORA) is now a reality, and it is mandated for implementation for financial institutions in the European Union (EU) with effect from January 17th, 2025. The financial sector in EU has always been governed by a single rule book and this regulation aims at building single rule book on achieving digital operational resilience. This white paper outlines the scope of DORA for financial services firms and how to build a digital operational resilience framework and how to comply to this regulation.

Decision makers from the financial services industry, through this whitepaper, deep dive into the nuances of DORA regulation along with the benefits from the practitioner's view.

Key Takeaways

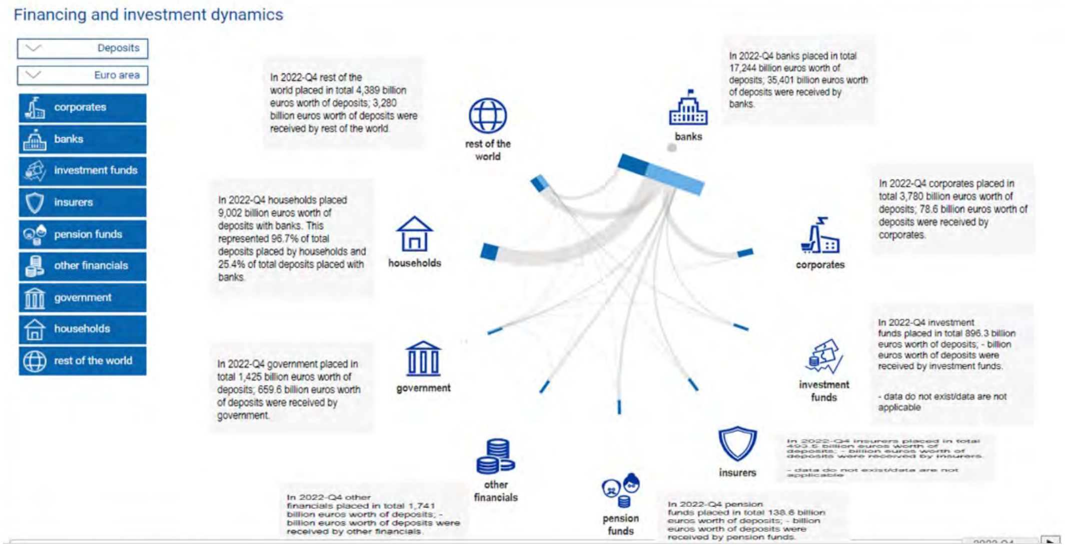
- Need for DORA and components of compliance
- TechM's 5-Step framework
- Steps to achieve DORA compliance
- Tech Mahindra's credentials in cybersecurity - governance, risk management and compliance

Introduction

According to Europa.eu, EU has 22000 financial entities spread across 27 member countries and constitutes to 14% of the world trade.1

Banks are key pillars of economic support for all the institutions that support the economic growth in the region. The real economy requires the financial system to perform a range of key economic functions reliably. These include financial activities like payment services, securities trading, securities settlement services and deposit taking, among many. These processes have become increasingly digitalised, creating new and important interdependencies.

Data points enclosed from Euro Area statistics highlight the interconnectedness:



In 2022-Q4 rest of the world placed in total 4,389 billion euros worth of deposits; 3,280 billion euros worth of deposits were received by rest of the world.

In 2022-Q4 banks placed in total 17,244 billion euros worth of deposits; 35,401 billion euros worth of deposits were received by banks.

In 2022-Q4 households placed 9,002 billion euros worth of deposits with banks. This represented 96.7% of total deposits placed by households and 25.4% of total deposits placed with banks.

In 2022-Q4 corporates placed in total 3,780 billion euros worth of deposits; 78.6 billion euros worth of deposits were received by corporates.

In 2022-Q4 government placed in total 1,425 billion euros worth of deposits; 659.6 billion euros worth of deposits were received by government.

In 2022-Q4 investment funds placed in total 896.3 billion euros worth of deposits; - billion euros worth of deposits were received by investment funds.

- data do not exist/data are not applicable

In 2022-Q4 insurers placed in total 493.5 billion euros worth of deposits; - billion euros worth of deposits were received by insurers.

- data do not exist/data are not applicable

In 2022-Q4 other financials placed in total 1,741 billion euros worth of deposits; - billion euros worth of deposits were received by other financials.

In 2022-Q4 pension funds placed in total 138.6 billion euros worth of deposits; - billion euros worth of deposits were received by pension funds.

Source : Euro area statistics (euro-area-statistics.org)

Figure 1: High interconnectedness on "financing and investment dynamics" activities between institutions and financial service sector[2]

Greater interconnectedness means higher the chances of a systematic risk that can pass from one institution to the other.

Regulators in the past have strengthened the financial system by physical resilience strategies by conducting stress tests to check the financial strength of the financial services firms and aided them by key actions like liquidity infusion, capital funding and more. Now the global financial system has become digital, and the regulators have been adopting digital resilience strategies to thwart threats from cyber actors.

Need for DORA

The EU financial sector is regulated by a single rulebook and governed by a European system of financial supervision. Exceptions to this have been digital operational resilience and ICT security. As digital operational resilience strategy is vital for financial stability that can eliminate systematic risks. DORA regulation should be seen from that direction. DORA regulation is mandated to all financial institutions operating in the EU region. DORA framework proposes key approaches in addressing ICT risk arising from cyber incidents. The outcome is to enable financial services firms to withstand operational outages to always preserve the integrity of the financial markets.

DORA Compliance

DORA regulation will be effective and be binding on financial entities in the EU region effective from 17 January 2025.

The components of DORA compliance have been called out in Articles 1 to Article 64. The key areas for building operational resilience have been highlighted in the chapters below:

Chapter 1 – General provisions

Chapter 2 – ICT risk management

Chapter 3 – ICT -related incident management, classification and reporting

Chapter 4 -Digital Operational resilience testing

Chapter 5 -Managing of ICT third party risk

Chapter 6 -Information sharing arrangements

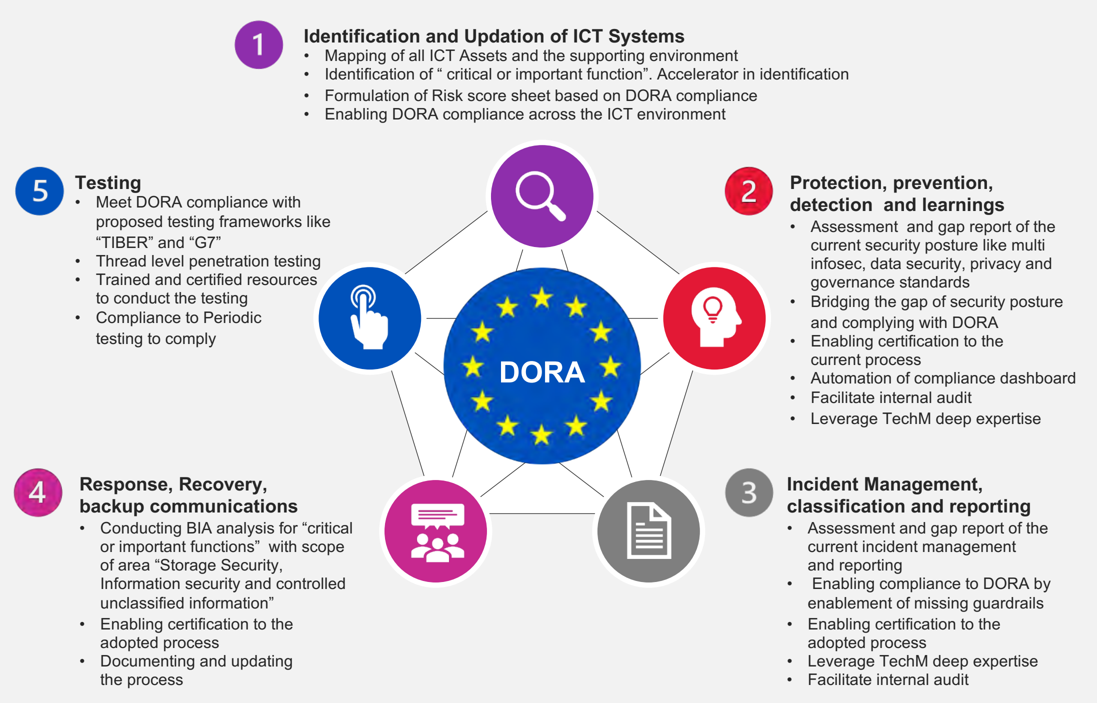
Chapter 7 -Competent authorities

Chapter 8 – Delegated acts

Chapter 9 – Transitional and final provisions

TechM Framework to Accelerate DORA Compliance

TechM has developed an analytical approach in complying with DORA. The framework has been built based on deep insights from the business domain team and the security practice team. The framework has been sharpened by inputs from our interactions with clients, partners, and analysts.



1 **Identification and Updation of ICT Systems**

- Mapping of all ICT Assets and the supporting environment
- Identification of " critical or important function". Accelerator in identification
- Formulation of Risk score sheet based on DORA compliance
- Enabling DORA compliance across the ICT environment

2 **Protection, prevention, detection and learnings**

- Assessment and gap report of the current security posture like multi infosec, data security, privacy and governance standards
- Bridging the gap of security posture and complying with DORA
- Enabling certification to the current process
- Automation of compliance dashboard
- Facilitate internal audit
- Leverage TechM deep expertise

3 **Incident Management, classification and reporting**

- Assessment and gap report of the current incident management and reporting
- Enabling compliance to DORA by enablement of missing guardrails
- Enabling certification to the adopted process
- Leverage TechM deep expertise
- Facilitate internal audit

4 **Response, Recovery, backup communications**

- Conducting BIA analysis for "critical or important functions" with scope of area "Storage Security, Information security and controlled unclassified information"
- Enabling certification to the adopted process
- Documenting and updating the process

5 **Testing**

- Meet DORA compliance with proposed testing frameworks like "TIBER" and "G7"
- Thread level penetration testing
- Trained and certified resources to conduct the testing
- Compliance to Periodic testing to comply

Figure 2: The five-step framework will accelerate DORA compliance

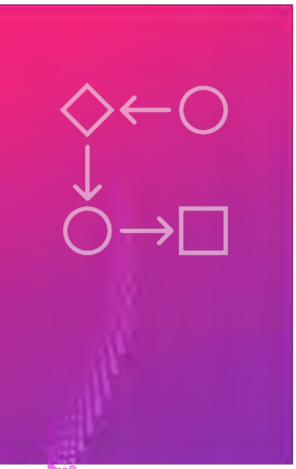
Steps to Achieve DORA compliance: TechM approach

1. Identification and enhancement of the ICT systems for critical or important functions

DORA recognizes that all ICT assets are not equally important as all of them do not support critical or important functions. The foundational steps have been elaborated in articles 7, 8 and 29.

TechM approach has ingrained the objectives spelt out by the above articles and basis which the below analytical approach has been proposed.

- Identification of all business functions and mapping them to the ICT assets. Tech M has multiple approaches that can be customized to suit the client's maturity. For example: Leveraging single source of truth tools, internal accelerators, manual mapping exercise.



- Identifying the critical or important business functions and mapping them to the associated ICT assets. Tech M has built a full list of functions that are classified as critical or important. Our home-grown list of critical or important functions has been developed based on readings from various regulatory bodies like ESRB. These critical or important functions are classified for business continuity planning.
- Risk scoring of the Critical ICT assets. TechM has a developed an internal framework which aptly classifies the risk bucket of the ICT asset. Each of the ICT assets are qualified as low risk, medium risk, and high risk.
- Remediation framework of TechM will help financial services with a road map built on strategy for "risk reduction" on the ICT asset. The framework would highlight the ICT assets where no vendor lock in is accepted, which means these ICT assets need to be built in open architecture. TechM has strong capabilities in building open architecture ICT environments.

Mapping and identification of critical functions

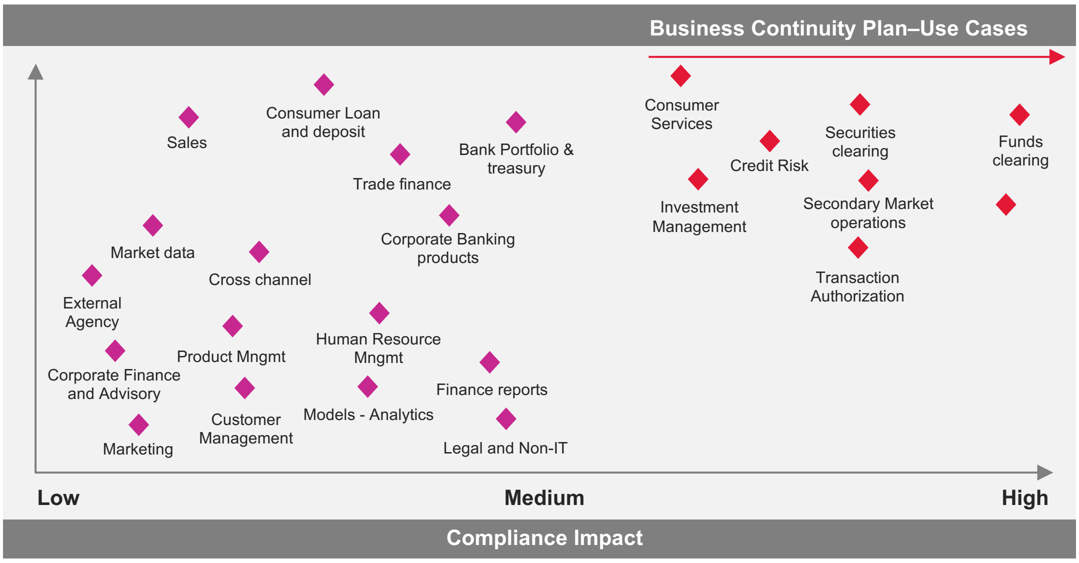


Figure 3: Classified -critical or important function - BCP Planning

ICT Risk Profile Approach

Classification – ICT service provider	Risk rating – based on control	Reasons
Intra-group service provider	Low 🟢	ICT service provider is part of the financial services group
ICT third-party service provider within the EU region	Medium 🟡	ICT services are offered from the service provider registered in the EU region and are subject to EU regulation
ICT third-party service provider established in a third country	High 🔴	ICT services are offered from third country

2. **Protection, prevention detection and learning:**

DORA does not spell out what are the protection, prevention, detection and learning approaches to be adopted. There is no new approach proposed by DORA. The scope or the intent of DORA is covered in articles 5,6,9, 10, 13 and 16. The understanding from the above articles is that financial services firms must demonstrate that they are complying with the best of industry standards under this approach.

TechM has proposed a three-step approach:

- Assessment of current security posture with the industry security practices covering
  - **a. Infosec certification**
  - **b. Privacy information management**
  - **c. Business continuity management**

Infosec – security standards, regulations and controls	**Privacy information management**	**Buiness continuity management**
ISO/IEC 20000 1:20 18	GDPR	ISO 2230 1:20 12
ISO/IEC 2700 1:20 13	ISO/IEC 2770 1:20 19	
ISO/IEC 270 17:20 15		
ISO/IEC 270 18		
SOC 2 Type 2		
NIST SP 800 - 53		
NIST Cyber security Framework		
PCI D88		

- We enable clients in building compliance to the above security standards. TechM has a credible history in handholding its clients and complying with the industry certifications
- Automation of dashboard to the senior management. TechM can build a live dashboard on real time environment which will show the compliance posture and enable action on the missing compliance areas.

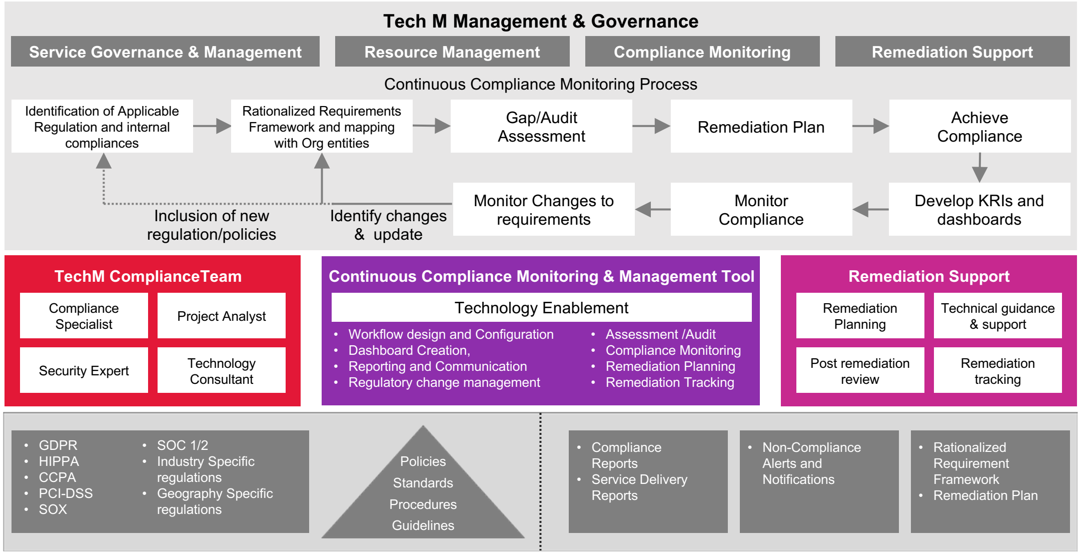

Tech M Management & Governance
Service Governance & Management
Resource Management
Compliance Monitoring
Remediation Support
Continuous Compliance Monitoring Process
Identification of Applicable Regulation and internal compliances
Rationalized Requirements Framework and mapping with Org entities
Gap/Audit Assessment
Remediation Plan
Achieve Compliance
Develop KRIs and dashboards
Monitor Compliance
Monitor Changes to requirements
Identify changes & update
Inclusion of new regulation/policies
TechM ComplianceTeam
Compliance Specialist
Project Analyst
Security Expert
Technology Consultant
Continuous Compliance Monitoring & Management Tool
Technology Enablement
Workflow design and Configuration
Dashboard Creation,
Reporting and Communication
Regulatory change management
Assessment /Audit
Compliance Monitoring
Remediation Planning
Remediation Tracking
Remediation Support
Remediation Planning
Technical guidance & support
Post remediation review
Remediation tracking
GDPR
HIPPA
CCPA
PCI-DSS
SOX
SOC 1/2
Industry Specific regulations
Geography Specific regulations
Policies
Standards
Procedures
Guidelines
Compliance Reports
Service Delivery Reports
Non-Compliance Alerts and Notifications
Rationalized Requirement Framework
Remediation Plan

Figure 4: Tech Mahindra's compliance management framework

3. Incident management, classification and reporting:

DORA does not spell out what are the incident management, classification, and reporting approaches to be followed at the organization level. Credit institutions classified under Article 6(4) should submit a report to the competent authority. The scope of the intent of DORA is covered well in articles 17,18,19 and 23.

TechM has proposed a four-step approach:

- Assessment of current security posture with the mandated industry security practices like covering Infosec certification, privacy information management, and business continuity management for incident management, classification, and reporting as mandated by the security industry.
- Enabling compliances against the identified missing gaps.
- Tech M has developed a next gen SIEM/SOC platform with a repository of more than 1000 patterns in identification of an incident. This can be leveraged by the client.
- Automation of dashboard to the senior management.

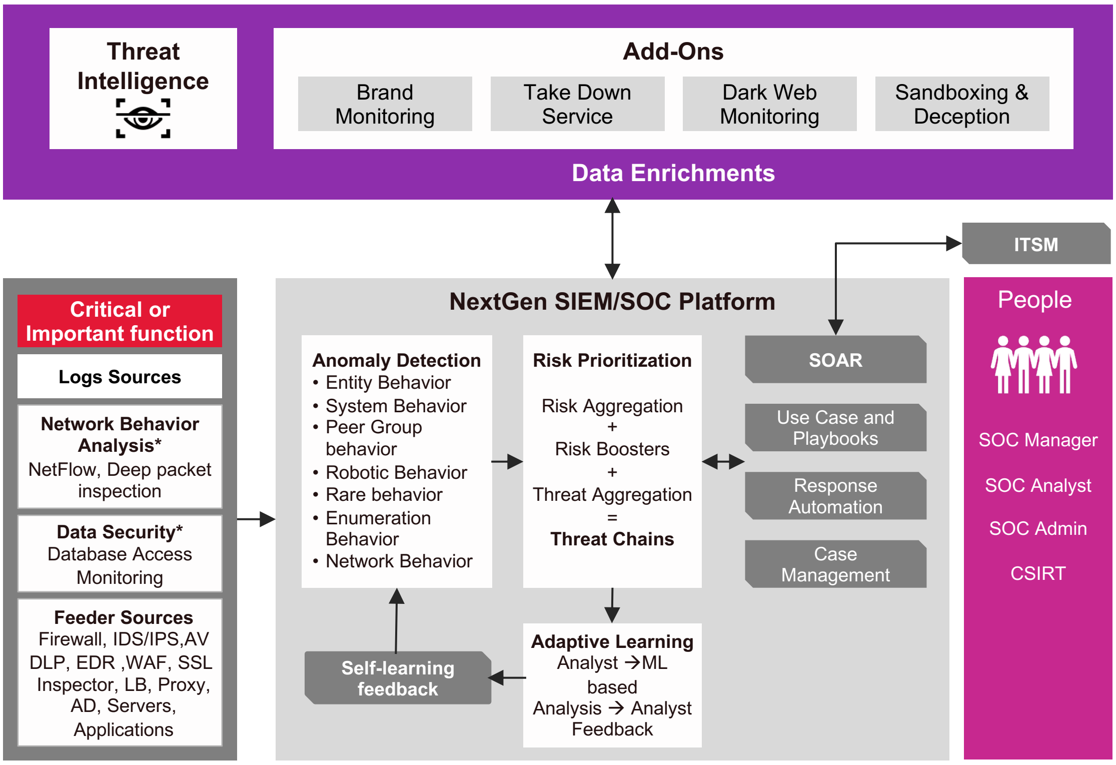


Figure 5:Prevention, detection, and learning architecture

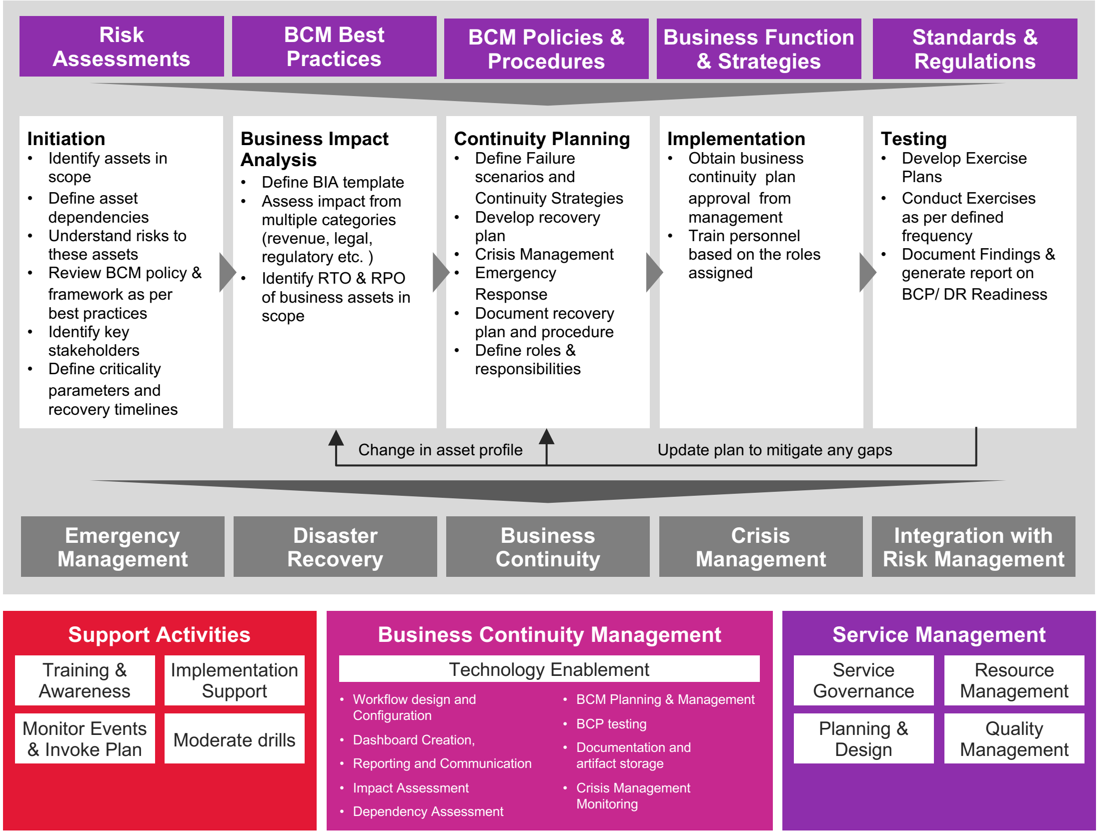
4. **Response, recovery, back up and communication:**

DORA clearly calls that Business continuity plans are to be enabled for all ICT assets that support critical or important business functions. The objective is to ensure the continuity of the financial services that are identified as critical or important functions. The suggested approach has been covered in Articles 11, 12 and 14.

TechM has proposed a three-step approach, which would enable the financial services firms to put a BCP strategy. The industry standard certification to be adhered is ISO 22301:2012.

TechM proposes three steps:

- Business continuity plan would be enforced on all ICT assets that are identified to support all critical or important functions which were identified in Step 1.
- Validate compliance to ISO 22301 :2012 and validate if compliance is in place. If compliance is not in place building the compliance standards
- Prepare a document which would be a register with detailed workflows, roles and responsibilities and actions to restore.



Risk Assessments | BCM Best Practices | BCM Policies & Procedures | Business Function & Strategies | Standards & Regulations

Initiation
- Identify assets in scope
- Define asset dependencies
- Understand risks to these assets
- Review BCM policy & framework as per best practices
- Identify key stakeholders
- Define criticality parameters and recovery timelines

Business Impact Analysis
- Define BIA template
- Assess impact from multiple categories (revenue, legal, regulatory etc.)
- Identify RTO & RPO of business assets in scope

Continuity Planning
- Define Failure scenarios and Continuity Strategies
- Develop recovery plan
- Crisis Management
- Emergency Response
- Document recovery plan and procedure
- Define roles & responsibilities

Implementation
- Obtain business continuity plan approval from management
- Train personnel based on the roles assigned

Testing
- Develop Exercise Plans
- Conduct Exercises as per defined frequency
- Document Findings & generate report on BCP/ DR Readiness

Change in asset profile

Update plan to mitigate any gaps

Emergency Management | Disaster Recovery | Business Continuity | Crisis Management | Integration with Risk Management

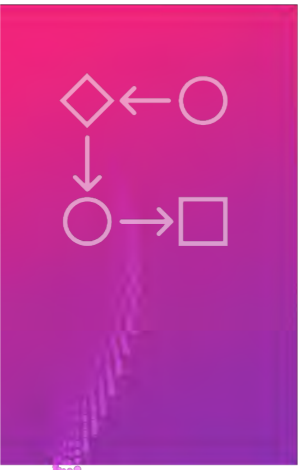
Support Activities
- Training & Awareness
- Implementation Support
- Monitor Events & Invoke Plan
- Moderate drills

Business Continuity Management

Technology Enablement
- Workflow design and Configuration
- Dashboard Creation,
- Reporting and Communication
- Impact Assessment
- Dependency Assessment
- BCM Planning & Management
- BCP testing
- Documentation and artifact storage
- Crisis Management Monitoring

Service Management
- Service Governance
- Resource Management
- Planning & Design
- Quality Management

Figure 6: Business continuity management framework



5. Security Testing :

DORA regulation on testing is to ensure financial services firms have a sound and comprehensive risk management framework. The scope has been detailed in articles 24, 15, 26 and 27.

TechM proposes two steps:

- Handholding the client and conducting advanced penetration testing on TIBER-EU framework and identify the gaps. Run comprehensive ICT testing against a defined catalogue covering application penetration testing, infrastructure penetration testing, DevSecOps, security awareness programs and cloud security.
- Building an enhanced resilience approach based on the learnings from failed scenarios.

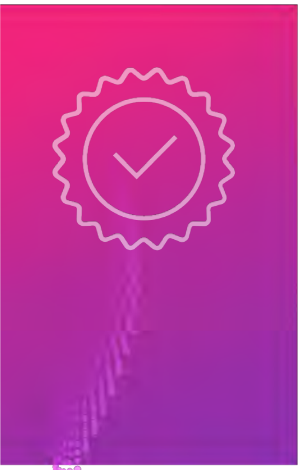
Application Penetration Testing	Infrastructure Penetration Testing	DevSecOps	Security Awareness programs	Cloud Security
Greybox and Blackbox • Web application • Mobile application • Thick client • API • Secure source code reviews • Application architecture reviews • Threat modeling	• Exploitative network pentest ➢ External network ➢ Internal network • Wireless pentest • Secure network • Architecture reviews • Firewall rule base audit • Configuration reviews	DevSecOps implementation • Threat modeling • Secure SDLC • Security tools integration in CI/CD pipeline • Secure source code reviews • Open-source secure code reviews	• Social engineering • Security awareness training sessions • Help conduct CTF’s	• External network pentest • Cloud configuration reviews

Our Differentiated Service Offerings

Vulnerability management with ServiceNow Secops and Balbix	Red Team and CARTA	Application security with Armorcode	Fast Track to Appsec - MSSP	Strategic Cyber Insights

Figure 7: Security testing services catalogue

As the deadline for compliance with DORA is on 17 Jan 2025, financial services firms in the EU region will have to start preparing their approach in complying to DORA before the deadline. At this critical juncture financial services firms can rely on the expertise of Tech Mahindra in complying with the DORA framework. TechM has strong credentials in the cyber security space with built-in frameworks, IPs, and consulting.



Tech Mahindra: Credentials in Cyber security - Governance, Risk Management, and Compliance

We offer GRC services, that leverage accredited consulting skills and real-time AI-powered dashboard for delivering end-to-end risk and compliance. Tech Mahindra is one of the earliest Indian system integrators to have built a DORA compliance framework for financial services firms in EU region.

Tech Mahindra has been successfully delivering cyber security services to Fortune 1000 clients globally for more than two decades.

Our service offerings

Service Offerings	Capability
Advanced threat management – SIEM / SOC	✓
Application security – VA/PT, DevSecOps and others	✓
Cloud security	✓
Cyber advisory – strategy assessment and awareness	✓
Cyber risk and analytics	✓
Data security and privacy	✓
Third party risk managment	✓
Network security	✓
Industry leading partnerships to strengthen the offerings	✓

About the Authors

Lakshmi Kanth

Principal Consultant, Banking and Financial Services

Lakshmi Kanth has more than two decades of experience in banking and financial services domain. He is a certified privacy specialist from DSCI. He is passionate about creating purposeful and innovative solutions for the BFSI vertical— wherein solutions like RITA, CTEE, and data residency-as-a-service stood out at the time of launch. His deep domain skills and ability to map an outcome are his strengths.

Gopal Parasnis

Head of Digital Transformation, Banking & Financial Services

Gopal Parasnis heads digital transformation for the BFSI vertical at Tech Mahindra. Gopal has around 25 years of experience in the IT industry and has been part of several large-scale digital transformation initiatives across the banking and financial services clients. He has led and advised on several mainframe modernization journeys. He has a deep understanding of the latest industry and technology trends in the space.

Abbreviations

IDS - Intrusion detection system
IPS - intrusion prevention system
AV - Antivirus
DLP - Data Loss prevention
EDR - Endpoint detection and response
Waf - Web Application Firewall

SSL - Secure socket layer
LBP - Location based privacy
AD - Active directory
SOAR - Security orchestration, automation, and response
SOC - Security operations center
CSIRT - Computer security incident response team

References

1. Facts and figures, EU economy | European Union. (n.d.). European Union. https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/economy_en
2. Euro area statistics. (n.d.). https://www.euro-area-statistics.org/financing-and-investment-dynamics?cr=eur&lg=en

TECH mahindra

2023 Brand Finance® Awards
TOP 10 STRONGEST IT SERVICES BRAND

2023 Brand Finance® Awards
FASTEST-GROWING IT SERVICES BRAND IN BRAND VALUE RANK