

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

Guideline to Implement the DORA Regulations

USE CASES

CONTACT

PDF

## Application of DORA

103

days

08

hours

13

minutes

39

seconds

## Implementation Strategies of the Five Pillars of DORA Regulations

Governance and Risk Management

Operational Resilience Testing

Incident Management and Recovery

ICT Third-Party Risk

Information Sharing

## Digital Operational Resilience Act (DORA) Objectives

The **Digital Operational Resilience Act (DORA)** is a pivotal regulation by the European Commission aimed at bolstering the digital operational resilience of the financial sector. Enacted to address the evolving digital risks and ensure financial institutions can effectively withstand, respond to, and recover from ICT-related disruptions, DORA introduces a comprehensive regulatory framework. Its main objectives include improving ICT risk management, enhancing cybersecurity measures, establishing robust governance and oversight, and

promoting effective incident reporting and business continuity planning among financial entities operating within the EU.

**DORA  
REGULATIONS**

**GOVERNANCE  
AND RISK  
MANAGEMENT**

**OPERATIONAL  
RESILIENCE  
TESTING**

**INCIDENT  
MANAGEMENT  
AND  
RECOVERY**

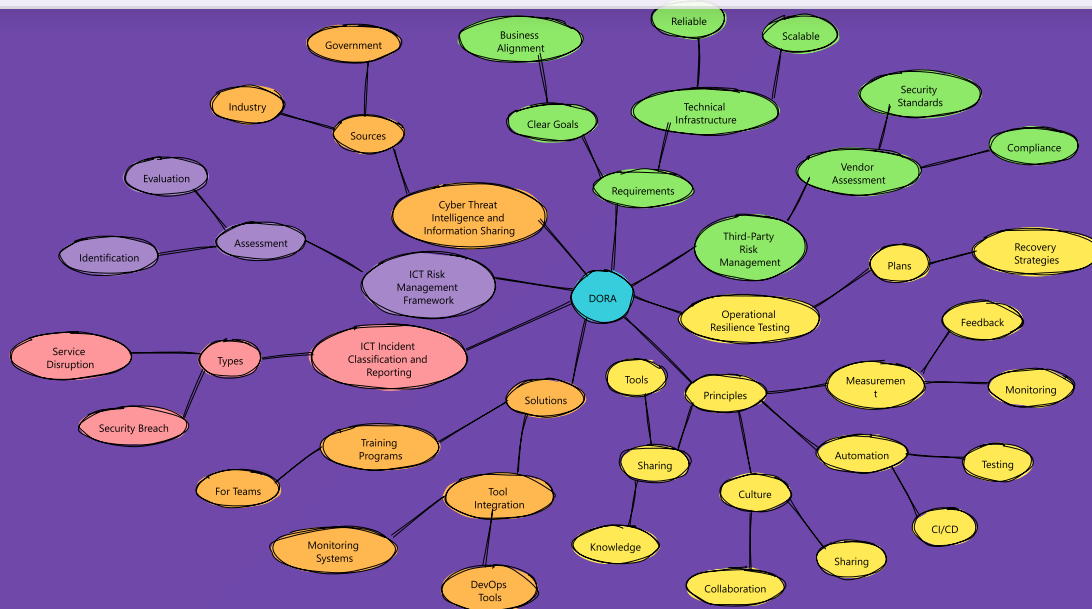
**ICT  
THIRD-  
PARTY  
RISK**

**INFORMATION  
SHARING**

**USE CASES**

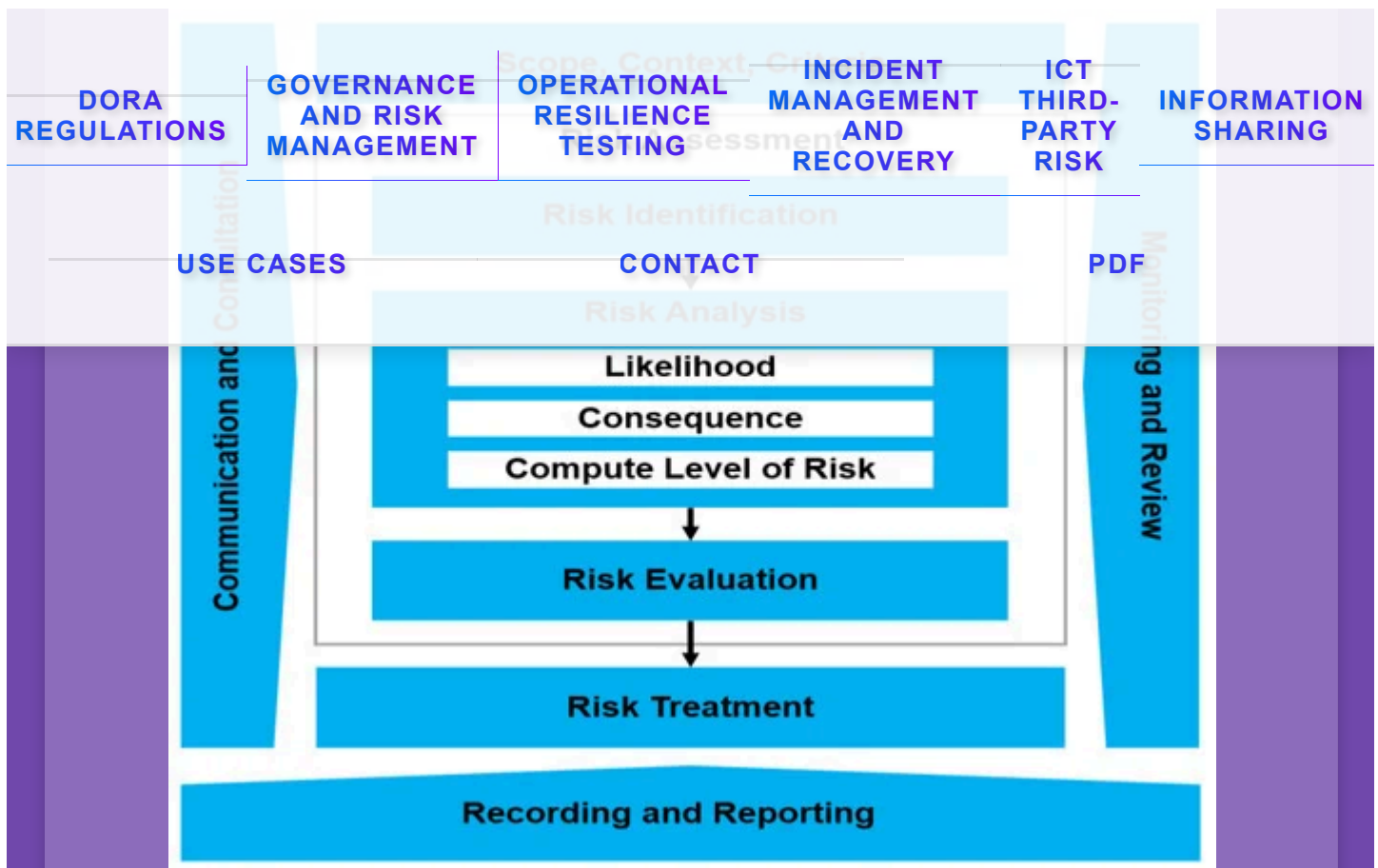
**CONTACT**

**PDF**



## First Pillar : Governance and Risk Management

### ICT Risk Management Frameworks under DORA



In the context of the Digital Operational Resilience Act (DORA), financial institutions are encouraged to adopt comprehensive ICT Risk Management practices. While DORA provides a regulatory framework for digital operational resilience, institutions may refer to various established standards to enhance their ICT risk management capabilities:

- **ISO/IEC 27001:** International standard for information security management systems (ISMS), offering a systematic approach to managing sensitive company information.
- **NIST Cybersecurity Framework:** Provides a policy framework of computer security guidance for how private sector organizations in the US can assess and improve their ability to prevent, detect, and respond to cyber attacks.
- **COBIT:** A comprehensive framework for IT governance and management, facilitating the optimization of technology resources for businesses.
- **ITIL:** A set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the business.
- **CIS Controls:** A prioritized set of actions for cyber defense that provides specific and actionable ways to stop today's most pervasive and dangerous attacks.
- **PCI DSS:** A security standard for organizations that handle branded credit cards from the major card schemes.
- **GDPR:** Although primarily focused on data protection, GDPR imposes significant security obligations on data controllers and processors.
- **EBA Guidelines on ICT and Security Risk Management:** Guidelines provided by the European Banking Authority, tailored for the financial sector's unique needs.

Adhering to these frameworks can significantly enhance an institution's resilience against ICT-related risks, aligning with DORA's objectives to strengthen the digital operational resilience across the EU's financial sector.

## Step 1: Risk Assessment and Identification of Critical Assets

## USE CASES

II Assets :

## CONTACT

## PDF

Compile a comprehensive inventory of systems, applications, databases, and digital infrastructure. This includes both internally hosted assets and cloud services.

**Identification of Critical Assets :**

Determine the essential business processes and the IT systems that support them. This may include transaction processing systems, customer databases, CRM applications, and other key systems.

**Identify Risks :**

Systematically identify and document all potential risks that could impact ICT systems and operations.

**Risk Analysis :**

Assess potential threats such as cyber attacks, technical failures, human errors, and natural disasters. This should involve an analysis of the likelihood and impact of each risk scenario.

**Business Impact Assessment (BIA) :**

For each critical asset, evaluate the potential impact of a disruption on banking operations. This aids in prioritizing resilience efforts based on the significance of each asset to daily operations.

**Evaluate and Prioritize Risks :**

Evaluate the risks to prioritize them based on their severity and the urgency of mitigation actions required.

**Defining the Level of Risk Appetite :**

In collaboration with key stakeholders, establish the acceptable level of risk for each business process and IT system. This will guide decisions regarding investments in security and resilience.

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

Evaluate and Prioritize Risks :

Evaluate the risks to prioritize them based on their severity and the urgency of mitigation.

Implement Mitigation Strategies :

USE CASES Implement appropriate mitigation strategies to mitigate the prioritized risks, including preventive measures and contingency plans.

CONTACT

PDF

Monitor and Review :

Continuously monitor the risk environment and the effectiveness of implemented mitigation strategies, adjusting as necessary to address new or changing risks.

Enhance ICT Resilience :

Strengthen the resilience of ICT systems against disruptions through robust design, redundancy, and recovery planning.

Compliance with Regulations :

Ensure compliance with all relevant legal, regulatory, and contractual obligations related to ICT risk management.

Stakeholder Communication :

Maintain open and effective communication with all stakeholders regarding ICT risks and the measures taken to manage them.

Deliverables

Risk Analysis Report

Objective

The "Risk Analysis Report" serves to systematically identify, assess, and prioritize risks to the financial entity's operations, particularly focusing on the identification of critical assets as mandated by the Digital Operational Resilience Act (DORA). This comprehensive document aims to inform strategic decision-making and guide the development of effective risk mitigation strategies.

## Key Components

- Risk Identification:** Detailed listing of identified risks, categorized by type (e.g., cyber, operational, systemic) and source (internal vs. external).
- Risk Assessment:** Evaluation of each risk's likelihood and potential impact, employing qualitative and quantitative analysis methods to prioritize risks according to their severity.
- Critical Asset Identification:** Identification and analysis of critical assets and functions likely to be affected by identified risks, highlighting their importance to the entity's operations.
- Risk Mitigation Strategies:** Recommendations for risk mitigation strategies, including preventive measures, response plans, and recovery processes.
- Regulatory Compliance:** Assessment of the entity's risk profile and mitigation strategies in the context of compliance with DORA and other relevant regulations.
- Monitoring and Reporting:** Outline of procedures for ongoing risk monitoring, reporting mechanisms, and feedback loops to ensure continuous risk management.

## Methodology

Explanation of the methodologies and tools used in conducting the risk analysis, including data sources, assessment frameworks, and analytical techniques.

## Conclusion and Recommendations

Concluding remarks summarizing the key findings of the risk analysis, highlighting priority risks, and proposing strategic recommendations for enhancing the entity's operational resilience.

## Scope

This plan covers the processes and criteria for identifying critical assets across the entity, including information systems, data repositories, operational technologies, and essential personnel. It focuses on assets that, if compromised, could significantly impact the entity's operational capability, reputation, or regulatory compliance.

## Key Components

- Identification Criteria:** Definition of criteria used to identify critical assets, considering factors such as asset value, sensitivity, and impact on operations.
- Asset Inventory:** Comprehensive inventory of assets, categorized according to their function and criticality level.
- Risk Assessment Integration:** Integration of the critical asset identification process with broader risk assessment activities to ensure a holistic view of potential threats and vulnerabilities.
- Protection Measures:** Outline of protective measures and controls to safeguard critical assets from identified risks.
- Review and Update Procedures:** Procedures for regularly reviewing and updating the list of critical assets to reflect changes in the operational environment or asset landscape.
- Stakeholder Involvement:** Roles and responsibilities of key stakeholders in the critical asset identification process, ensuring cross-departmental collaboration and expertise.

## Implementation Plan

Details on the phased implementation of the critical assets identification plan, including timelines, milestones, and resource allocation.

## Compliance and Reporting

## Objective

The "Risk Appetite Framework" is designed to articulate the level of risk a financial entity is willing to accept in pursuit of its strategic objectives, in alignment with the Digital Operational Resilience Act (DORA). This framework establishes clear guidelines for risk decision-making, ensuring that all activities are conducted within acceptable risk thresholds to safeguard the entity's operational resilience.

## Scope

This document encompasses the entire spectrum of risks faced by the entity, including but not limited to cybersecurity threats, operational disruptions, and compliance risks. It covers the processes for identifying, assessing, managing, and monitoring risks across the entity's operations.

## Key Components

- Risk Appetite Statement:** A high-level statement that defines the entity's overall willingness to take on risk in the context of its strategic objectives.
- Risk Tolerance Thresholds:** Specific thresholds that quantify the maximum level of risk the entity is willing to accept in various areas of operation.
- Risk Identification and Assessment:** Procedures for identifying and assessing risks within the context of the entity's risk appetite.
- Risk Monitoring and Reporting:** Mechanisms for ongoing monitoring of risk exposures relative to the defined appetite and tolerance levels, including regular reporting to management and relevant stakeholders.
- Roles and Responsibilities:** Clear delineation of roles and responsibilities within the entity for managing risk in accordance with the risk appetite framework.
- Integration with Strategic Planning:** Guidelines for integrating risk appetite considerations into strategic planning, decision-making, and operational processes.

## Implementation Strategy

A detailed plan for implementing the risk appetite framework, including timelines, milestones, and responsibilities for key activities.

## Benefits of the Framework

Discussion on the benefits of implementing a risk appetite framework, including enhanced decision-making, improved resource allocation, and

## Pillar 2 : Operational Resilience Testing

In those interconnected world, cybersecurity threats pose significant risks to individuals, organizations, and nations. The DORA Resilience Act recognizes the critical importance of information sharing in combating these threats. This chapter focuses on the principles, mechanisms, and benefits of cybersecurity information sharing as outlined in the DORA Resilience Act.

Effective cybersecurity information sharing enables stakeholders to proactively detect, prevent, and respond to cyber incidents. By exchanging threat intelligence, best practices, and vulnerabilities, entities can enhance their collective defenses and resilience against cyber threats.

Throughout this chapter, we will explore key aspects of cybersecurity information sharing, including its role in fostering collaboration among public and private sector entities, ensuring privacy and data protection, and promoting trust and transparency.

Use the **TIBER-EU framework** to guide resilience testing. Organize teams for penetration testing and red team attack simulations in collaboration with external partners.

# Step 1: Designing and Planning Resilience Tests

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

Actions to Undertake

## USE CASES

## CONTACT

## PDF

Identify and prioritize systems and processes for resilience testing based on their criticality to business operations.

Develop testing scenarios that reflect potential disruptions, including cyber attacks, system failures, and disaster response.

Plan tests that challenge the organization's ability to respond and recover from disruptions while minimizing impact to operations.

## Deliverables

Resilience Testing Framework Document

## Objective

This document outlines a structured approach to resilience testing for financial entities, aimed at assessing and enhancing their ability to withstand and recover from cyber threats, technical failures, and other disruptions. The framework is designed to ensure comprehensive testing coverage across all critical IT systems and processes, aligning with DORA's emphasis on maintaining digital operational resilience in the financial sector.

## Scope

The Resilience Testing Framework applies to all operational and information systems, including networks, applications, and services critical to the daily functions of financial entities. It encompasses various testing methodologies, such as vulnerability assessments, penetration testing, scenario-based simulations, and disaster recovery exercises.

DORA REGULATIONS	GOVERNANCE AND RISK MANAGEMENT	OPERATIONAL RESILIENCE TESTING	INCIDENT MANAGEMENT AND RECOVERY	ICT THIRD-PARTY RISK	INFORMATION SHARING
	<div><div>USE CASES</div><div><ul style="list-style-type: none"><li>■ <b>Testing Methodologies:</b> Describes various testing methodologies, including their objectives, scope, and execution procedures.</li><li>■ <b>Testing Schedule:</b> Establishes a regular testing cycle, including frequency, prioritization of tests, and processes, and aligns with change management cycles.</li><li>■ <b>Roles and Responsibilities:</b> Defines the roles within the organization responsible for planning, executing, and reviewing resilience tests.</li><li>■ <b>Reporting and Documentation:</b> Outlines requirements for documenting test procedures, findings, and remediation actions, as well as reporting protocols to management and regulatory bodies.</li><li>■ <b>Continuous Improvement:</b> Provides a mechanism for incorporating test results and lessons learned into an ongoing process of resilience enhancement.</li></ul></div></div>				
	<div><div>Implementation Guidelines</div><div>Offers detailed guidance for implementing the testing framework, including prerequisites, tools and resources, stakeholder communication, and coordination with external partners or service providers.</div></div>				
	<div><div>Compliance and Regulatory Alignment</div><div>Ensures that the resilience testing practices comply with relevant regulations and standards, and supports the organization's efforts to meet DORA's requirements for digital operational resilience.</div></div>				
	<div><div>Review and Update Process</div><div>Establishes a structured review process for regularly updating the testing framework to adapt to evolving threats, technological changes, and regulatory developments.</div></div>				
	<div><div>Testing Scenarios and Methodologies</div><div></div></div>				
	<div><div>Objective</div></div>				

## Scope

The scope includes a wide array of testing scenarios and methodologies ranging from technical vulnerability assessments to complex business continuity and disaster recovery exercises. It covers both cyber and physical aspects of operational resilience, encompassing IT systems, network infrastructure, applications, and critical business processes.

## Key Components

- **Scenario-Based Testing:** Outlines specific scenarios to simulate real-life disruptions, including cyber-attacks, technical failures, and natural disasters. It details the objectives, assumptions, and expected outcomes for each scenario.
- **Methodology Framework:** Describes various testing methodologies, such as penetration testing, tabletop exercises, and automated vulnerability scanning, including their applicability, execution procedures, and evaluation criteria.
- **Risk-Based Approach:** Emphasizes a risk-based testing strategy that prioritizes scenarios and methodologies based on the entity's risk profile and regulatory requirements.
- **Integration with Risk Management:** Ensures that testing outcomes are integrated into the entity's overall risk management framework, contributing to a comprehensive understanding of resilience capabilities and improvement areas.

## Implementation Guidelines

Provides detailed guidance on implementing the testing scenarios and methodologies, including planning, resource allocation, stakeholder engagement, and coordination with third-party service providers.

## Documentation and Reporting

Details the requirements for documenting testing processes, findings, and remediation actions. It also outlines reporting protocols to ensure that

relevant insights are communicated to management, regulatory bodies, and other stakeholders.

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

## Continuous Improvement

USE CASES

CONTACT

PDF

Establishes mechanisms for the continuous review and enhancement of testing scenarios and methodologies based on evolving threats,

### Test Planning and Scheduling Timeline

## Objective

The "Test Planning and Scheduling Timeline" document aims to provide a structured and strategic approach to planning, executing, and reviewing digital operational resilience tests. This timeline ensures that financial entities systematically address all aspects of digital resilience, including cybersecurity, data integrity, and business continuity, as mandated by the DORA regulations.

## Scope

The timeline covers all phases of the testing process for digital operational resilience, from initial planning to post-test review. It encompasses various testing types such as vulnerability assessments, penetration tests, and business continuity exercises, ensuring comprehensive resilience across all digital operations.

## Key Components

- Initial Planning:** Identifies objectives, scope, and specific resilience aspects to be tested, aligning with the entity's risk profile and regulatory requirements.
- Resource Allocation:** Outlines the resources needed for each test, including personnel, technology, and budget considerations.
- Scheduling:** Provides a detailed timeline for each test, including preparation, execution, and review phases, ensuring tests are spread throughout the year to minimize operational disruption.
- Stakeholder Engagement:** Details communication plans for engaging internal and external stakeholders, including regulatory bodies, throughout the testing process.
- Execution:** Specifies the procedures for carrying out each test, including roles and responsibilities.
- Review and Remediation:** Establishes a structured process for reviewing test outcomes, identifying remediation actions, and implementing improvements.

7. **Reporting:** Outlines reporting requirements and timelines for internal and external reports, ensuring accountability and transparency.

**DORA  
REGULATIONS**

**GOVERNANCE  
AND RISK  
MANAGEMENT**

**OPERATIONAL  
RESILIENCE  
TESTING**

**INCIDENT  
MANAGEMENT  
AND  
RECOVERY**

**ICT  
THIRD-  
PARTY  
RISK**

**INFORMATION  
SHARING**

## Integration with Risk Management

**USE CASES**

**CONTACT**

**PDF**

Emphasizes the integration of test outcomes with the entity's overall risk management framework, enhancing the entity's resilience posture and compliance with DORA regulations.

## Continuous Improvement

Highlights the importance of updating the testing timeline based on test results, evolving threats, and changes in the regulatory landscape, ensuring ongoing resilience and compliance.

## Step 2: Executing Resilience Tests

### Actions to Undertake

Carry out planned tests, simulating various disruption scenarios to evaluate the effectiveness of response plans.

Engage both internal teams and external partners to ensure comprehensive testing across all critical functions.

Document test results, including any identified weaknesses or failures in existing resilience strategies.

### Deliverables

## Objective

### USE CASES

### CONTACT

### PDF

The "Detailed Report of Test Outcomes" document is designed to provide a comprehensive analysis and evaluation of the outcomes from digital operational resilience tests. This report aims to identify strengths, weaknesses, and areas for improvement in the entity's digital operational resilience, in accordance with the DORA framework.

## Scope

The report covers the outcomes of various resilience tests, including but not limited to cybersecurity penetration tests, vulnerability assessments, and business continuity and disaster recovery exercises. It evaluates the effectiveness of the entity's defenses against potential disruptions and cyber threats.

## Key Components

- Executive Summary:** Provides a high-level overview of the test objectives, methodologies, and key findings.
- Methodology Overview:** Details the approaches and tools used in conducting the resilience tests, ensuring transparency and repeatability.
- Test Results:** Presents a detailed analysis of the test results, including identified vulnerabilities, the impact of simulated disruptions, and the entity's response capabilities.
- Risk Assessment:** Includes an assessment of the risks identified during testing, categorized by severity, and their potential impact on the entity's operations.
- Remediation Actions:** Outlines specific recommendations for addressing identified vulnerabilities and enhancing resilience, including prioritization and suggested timelines.
- Lessons Learned:** Summarizes key insights gained from the testing process, contributing to continuous improvement in resilience practices.
- Next Steps:** Provides a roadmap for implementing remediation actions and suggests areas for further testing and analysis.
- Appendices:** Includes any supporting documentation, such as detailed test logs, evidence of findings, and technical data.

## Compliance and Regulatory Reporting

## Objective

This document provides an in-depth analysis of the effectiveness of an entity's response mechanisms to simulated disruptions and cyber threats encountered during resilience testing. The goal is to evaluate the robustness and efficiency of existing response strategies and incident management processes, aligning with the Digital Operational Resilience Act (DORA) mandates.

## Scope

The scope encompasses the assessment of response strategies across a variety of test scenarios, including cybersecurity incidents, data breaches, system failures, and physical disruptions. It aims to cover all critical aspects of the entity's operational resilience, from technical response capabilities to communication and coordination efforts.

## Key Components

- Incident Response Timeline:** Chronicles the timeline of events from the detection of an incident through to its resolution, highlighting response times and key actions taken.
- Response Strategies Evaluation:** Assesses the effectiveness of the deployed response strategies, including the use of automated tools, team coordination, and execution of contingency plans.
- Communication Efficiency:** Analyzes the timeliness and clarity of communications both internally within the organization and externally with stakeholders and regulatory bodies.
- Impact Mitigation:** Evaluates the entity's ability to minimize the impact of incidents on operations, services, and stakeholders.
- Recovery Process:** Reviews the efficiency and effectiveness of recovery processes, including system restoration and data recovery activities.
- Challenges and Obstacles:** Identifies any challenges or obstacles encountered during the response and recovery processes, including areas for improvement.

Describes the methodologies and criteria used to evaluate response effectiveness, including qualitative assessments, quantitative metrics, and benchmarking against industry best practices.

Recommendations for Improvements Based on Test Results

Objective

This document aims to provide actionable recommendations for enhancing the digital operational resilience of financial entities based on the outcomes of resilience testing. It focuses on identifying areas of improvement to mitigate vulnerabilities, strengthen defenses, and optimize incident response mechanisms, aligning with the Digital Operational Resilience Act (DORA).

Scope

The recommendations cover a broad spectrum of resilience aspects, including cybersecurity, data protection, system availability, and business continuity. They are derived from a comprehensive analysis of test results, including vulnerability assessments, penetration tests, and business impact analyses.

Key Components

- 1. **Vulnerability Remediation:** Specific recommendations to address identified vulnerabilities in IT systems, applications, and processes.
- 2. **Cybersecurity Enhancements:** Suggestions for strengthening cybersecurity measures, including firewalls, intrusion detection systems, and encryption protocols.
- 3. **Business Continuity Planning:** Recommendations for improving business continuity and disaster recovery plans to ensure operational resilience.
- 4. **Incident Response Optimization:** Strategies to enhance incident response capabilities, including team training, communication plans, and simulation exercises.

5. **System Architecture Improvements:** Proposals to optimize system architecture for greater resilience, such as redundancy, failover mechanisms, and disaster recovery plans, to ensure that resilience practices align with current regulatory requirements and industry standards.

7. **Future Testing:** Suggestions for future resilience tests to continuously assess and improve operational resilience.

[USE CASES](#)[CONTACT](#)[PDF](#)

## Implementation Guidelines

Provides a roadmap for implementing the recommendations, including prioritization based on risk assessment, resource allocation, and timelines

### Step 3: Reviewing and Enhancing Resilience Measures

#### Actions to Undertake

Analyze test results to identify and understand the root causes of any failures or shortcomings in operational resilience.

Update and enhance resilience plans and strategies based on test findings and identified areas for improvement.

Implement changes and conduct follow-up tests to ensure that enhancements effectively strengthen operational resilience.

Adoption of Metasploit for penetration tests and Cyber Range for attack simulations.

Post-test analyses to identify and correct vulnerabilities.

## Objective

USE CASES

CONTACT

PDF

This document outlines the updated operational resilience plans formulated in response to the findings from recent resilience testing and assessments. It aims to enhance the financial entity's preparedness against a wide range of potential disruptions, ensuring compliance with the Digital Operational Resilience Act (DORA) and bolstering the entity's overall operational resilience.

## Scope

The revised plans encompass improvements across all facets of operational resilience, including but not limited to cybersecurity defenses, data integrity protocols, business continuity strategies, and incident response mechanisms. The scope extends to all operational areas that could impact the financial entity's ability to deliver critical services.

## Key Components

- Assessment of Current Plans:** A comprehensive review of existing operational resilience plans to identify gaps and areas for enhancement.
- Integration of Test Findings:** Incorporation of insights and vulnerabilities identified during resilience testing into the revised plans.
- Enhanced Cybersecurity Measures:** Updated strategies for protecting against cyber threats and securing data assets.
- Improved Business Continuity Practices:** Refined procedures to ensure the continuous delivery of critical services during disruptions.
- Strengthened Incident Response:** Optimized incident response plans to minimize the impact of disruptions and facilitate rapid recovery.
- Regulatory Alignment:** Adjustments to ensure the revised plans meet current and anticipated regulatory requirements under DORA.
- Stakeholder Engagement:** Strategies for involving key stakeholders in the planning process and ensuring clear communication during incidents.

## Implementation Strategy

Details the approach for implementing the revised operational resilience plans, including timelines, responsibilities, resource allocation, and

monitoring mechanisms to track progress and effectiveness.

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

## Continuous Improvement Process

USE CASES

CONTACT

PDF

Resilience is an ongoing process of regularly reviewing and updating the operational resilience plans based on evolving threats, technological advancements, and regulatory changes, ensuring sustained resilience and compliance.

Updated Response Strategies and Procedures

### Objective

The aim of this document is to outline the enhancements made to the entity's response strategies and procedures following a comprehensive review of existing measures and recent resilience test outcomes. These updates are designed to bolster the entity's capability to effectively respond to and recover from operational disruptions, in line with the mandates of the Digital Operational Resilience Act (DORA).

### Scope

This document encompasses revised strategies and procedures across various response domains, including cybersecurity incident response, data breach management, system failure recovery, and physical security breaches. It aims to cover all critical aspects necessary for maintaining operational continuity and protecting against potential threats.

### Key Components

- Incident Detection and Analysis:** Enhanced processes for the early detection of incidents and comprehensive analysis to determine their scope and impact.
- Incident Response Coordination:** Updated coordination mechanisms among internal teams and external partners to ensure swift and effective response actions.
- Communication Plans:** Refined communication strategies for internal stakeholders and external parties, including customers, regulators, and the public, ensuring timely and accurate information dissemination.
- Recovery and Restoration:** Improved procedures for the rapid recovery of affected systems and services, minimizing downtime and operational impact.

## Implementation and Monitoring

Details the implementation plan for the updated response strategies and procedures, including timelines, responsible parties, and monitoring mechanisms to assess effectiveness and identify areas for further improvement.

## Regulatory Compliance

Ensures that the updated response strategies and procedures align with current regulatory requirements and best practices, maintaining compliance with DORA and other relevant standards.

### Follow-Up Test Results and Final Resilience Assessment

## Objective

The objective of this document is to present the outcomes of follow-up resilience tests conducted after the initial implementation of updated resilience measures. It aims to provide a comprehensive assessment of the financial entity's operational resilience against the backdrop of the Digital Operational Resilience Act (DORA), highlighting areas of success and pinpointing remaining vulnerabilities.

## Scope

This assessment covers the range of follow-up tests performed, including but not limited to, cybersecurity penetration tests, business continuity simulations, and disaster recovery exercises. It evaluates the entity's enhanced defenses, response strategies, and recovery capabilities in the face of potential operational disruptions.

## Key Components

1. **Overview of Follow-up Tests:** A summary of the tests conducted, including their scope, methodologies, and objectives.
2. **Analysis of Results:** A detailed analysis of the test results, highlighting areas of improvement, resilience, effectiveness of measures, and any detected vulnerabilities.
3. **Comparison with Initial Assessments:** A comparative analysis between initial and follow-up test results to quantify improvements and identify areas that require attention.
4. **Final Resilience Assessment:** An overall assessment of the entity's operational resilience, considering the outcomes of both initial and follow-up tests.
5. **Recommendations for Continued Enhancement:** Actionable recommendations for addressing any remaining vulnerabilities and further strengthening resilience measures.
6. **Next Steps and Strategic Recommendations:** Guidance on future resilience testing cycles, continuous improvement strategies, and long-term resilience planning.

## Implementation and Monitoring

Outlines the approach for implementing the final recommendations, including monitoring strategies to ensure continuous improvement in operational resilience.

## Regulatory Compliance and Reporting

Ensures that the entity's operational resilience testing and assessment practices are in compliance with DORA requirements, including necessary reporting to regulatory bodies.

## Pillar 3 : Incident Management and Recovery

As digital technologies become increasingly integral to business operations, the need for robust ICT Incident Management and Cyber Threat Reporting mechanisms has never been more critical. These processes are essential for detecting, responding to, and mitigating the impacts of cybersecurity incidents and threats. An effective incident management strategy ensures that an organization can swiftly address security breaches, minimize operational disruptions, and reduce the risk of data loss or theft. Additionally,

systematic cyber threat reporting supports the early identification of potential threats and vulnerabilities, enabling organizations to strengthen their defenses against future attacks.

**DORA  
REGULATIONS**

**GOVERNANCE  
AND RISK  
MANAGEMENT**

**OPERATIONAL  
RESILIENCE  
TESTING**

**INCIDENT  
MANAGEMENT  
AND  
RECOVERY**

**ICT  
THIRD-  
PARTY  
RISK**

**INFORMATION  
SHARING**

Step 1: Establishing ICT Incident Management Protocols

**USE CASES**

**CONTACT**

**PDF**

Actions to Undertake

Develop an ICT incident response plan tailored to identify, manage, and mitigate incidents efficiently.

Implement detection systems and establish protocols for immediate incident reporting.

Train the incident response team on standard operating procedures and simulation exercises.

Deliverables

Incident Response Plan

Objective

The "Incident Response Plan" is a comprehensive document that outlines the procedures and protocols a financial entity will follow in the event of an ICT security incident. This plan is developed to ensure a coordinated and effective response to incidents that could impact the entity's information and technology systems, in compliance with the Digital Operational Resilience Act (DORA).

Scope

The plan covers the full spectrum of potential ICT incidents, including cybersecurity breaches, data leaks, system failures, and other events that

could threaten the operational integrity or security of the entity's ICT environment.

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

## Key Components

USE CASES

CONTACT

PDF

1. **Incident Identification:** Procedures for the detection and identification of ICT incidents, including the use of monitoring tools and indicators of compromise.
2. **Incident Classification:** Guidelines for classifying incidents based on their severity, impact, and urgency, to prioritize response efforts accordingly.
3. **Response Team:** Roles and responsibilities of the incident response team, including internal staff and external partners.
4. **Response Procedures:** Step-by-step response procedures for different types of incidents, detailing containment, eradication, and recovery actions.
5. **Communication Plan:** Communication protocols for informing internal stakeholders, regulators, and potentially affected parties.
6. **Documentation and Reporting:** Requirements for documenting incidents and response actions, including post-incident reporting to management and regulatory bodies.
7. **Post-Incident Review:** Processes for conducting post-incident reviews to analyze the response, identify lessons learned, and implement improvements to the incident response plan and overall security posture.

## Training and Exercises

Provisions for regular training and simulation exercises to ensure the incident response team and relevant personnel are prepared to execute the plan effectively.

## Review and Update Process

Mechanisms for the ongoing review and updating of the incident response

Threat Intelligence Reports

## Objective

The "Threat Intelligence Reports" are designed to provide financial entities with detailed and actionable intelligence on emerging and evolving cyber threats. These reports are a critical component of an effective ICT incident management protocol, as mandated by the Digital Operational Resilience

Act (DORA), enabling entities to proactively identify, assess, and respond to potential threats to their ICT infrastructure and operations.

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

## Scope

USE CASES

CONTACT

PDF

The reports cover a wide range of cyber threats, including malware, phishing, advanced persistent threats (APTs), insider threats, and vulnerabilities in hardware and software. They aim to provide a comprehensive view of the threat landscape, including tactics, techniques, and procedures (TTPs) used by adversaries, as well as indicators of compromise (IoCs) that can aid in detection and response.

## Key Components

- Executive Summary:** A high-level overview of the key findings, aimed at senior management to quickly grasp the current threat landscape.
- Threat Descriptions:** Detailed analysis of each identified threat, including its nature, origin, target, and potential impact on the financial sector.
- Analysis of TTPs:** In-depth examination of the tactics, techniques, and procedures employed by threat actors, providing insights into their methodologies.
- Indicators of Compromise (IoCs):** Specific technical indicators that organizations can use to detect malicious activity related to the reported threats.
- Recommended Mitigations:** Practical recommendations for mitigating the identified threats, including preventive measures, detection strategies, and response plans.
- Regulatory Implications:** Analysis of the compliance implications of the identified threats, considering the requirements of DORA and other relevant regulations.

## Methodology

An outline of the methodologies used to gather and analyze threat intelligence, including sources of information, analytical tools, and collaboration with external cybersecurity organizations.

## Distribution and Access

Guidelines for the secure distribution and access of the threat intelligence reports, ensuring that sensitive information is protected and only accessible to authorized personnel.

## Objective

### USE CASES

### CONTACT

### PDF

The "Incident Detection and Reporting Procedures" document establishes a structured approach for the timely detection, assessment, and reporting of ICT incidents within financial entities. In compliance with the Digital Operational Resilience Act (DORA), these procedures are designed to ensure that potential and actual cybersecurity incidents are identified and communicated effectively, facilitating rapid response and mitigation efforts to protect the entity's operational integrity.

## Scope

The procedures apply to all types of ICT incidents that could affect the confidentiality, integrity, or availability of the entity's data and systems. This includes, but is not limited to, cybersecurity breaches, data leaks, service outages, and system failures.

## Key Components

- Detection Mechanisms:** Description of the tools, technologies, and processes employed to monitor and detect potential ICT incidents, including anomaly detection systems and intrusion detection systems (IDS).
- Assessment Criteria:** Guidelines for assessing the severity and impact of detected incidents to prioritize response efforts based on predefined criteria.
- Reporting Channels:** Established channels and protocols for internal reporting of incidents to relevant stakeholders, including incident response teams, senior management, and legal departments.
- External Reporting Obligations:** Procedures for reporting incidents to external parties, such as regulatory authorities, law enforcement, and affected customers, in compliance with legal and regulatory requirements.
- Documentation Requirements:** Requirements for documenting incidents and response activities, ensuring thorough record-keeping for post-incident analysis and compliance purposes.
- Roles and Responsibilities:** Clear definition of roles and responsibilities for all personnel involved in the incident detection and reporting process.

## Training and Awareness

Mechanisms for the regular review and updating of detection and reporting procedures to reflect changes in the threat landscape, technological advancements, and regulatory requirements.

Incident Analysis and Forensics

## Objective

The "Incident Analysis and Forensics" document outlines the methodologies and procedures for conducting thorough investigations into ICT incidents within financial entities. This critical component of ICT incident management protocols, as mandated by the Digital Operational Resilience Act (DORA), aims to determine the root causes of incidents, assess their impact, and gather evidence for remedial actions and potential legal proceedings.

## Scope

The scope of this document includes the analysis of cybersecurity breaches, system failures, data integrity issues, and any other ICT incidents that could compromise the operational resilience of the financial entity. It covers the entire process from the initial detection of an incident to the final reporting, including evidence preservation, analysis, and documentation.

## Key Components

- Incident Response Team:** Identification of team members responsible for incident analysis and forensics, outlining their roles, responsibilities, and required qualifications.
- Evidence Collection and Preservation:** Procedures for securely collecting and preserving digital evidence related to the incident, ensuring its integrity for potential legal actions.
- Analysis Methodologies:** Detailed methodologies for analyzing incident data to identify the cause, methods used by attackers, and the extent of the impact on the entity's ICT infrastructure.

4. **Forensic Tools and Techniques:** Description of forensic tools and techniques used in the investigation, including software for data acquisition, analysis, and reporting, and guidelines for maintaining the integrity of the incident analysis, including the use of chain of custody and preventing similar incidents in the future.

6. **Legal Considerations:** Overview of legal considerations in conducting forensic investigations, including compliance with data protection laws and cooperation with law enforcement agencies.

## Training and Development

Details on training programs for the incident response team, ensuring members are proficient in the latest forensic methodologies and tools.

## Continuous Improvement

Mechanisms for incorporating lessons learned from incident analyses into the entity's cybersecurity practices and incident management protocols.

### Risk Management Framework

The "Risk Management Framework" is a critical deliverable within the "Establishing ICT Incident Management Protocols" chapter under DORA. This framework outlines a comprehensive approach to identifying, assessing, managing, and mitigating ICT-related risks within financial entities. It serves as a guide to ensure the operational resilience of the financial sector against various ICT threats and vulnerabilities.

## Components of the Framework

- **Risk Identification:** Procedures for identifying potential ICT risks that could impact the financial entity's operations, including both internal and external threats.
- **Risk Assessment:** Methodologies for evaluating the severity and likelihood of identified risks, considering the potential impact on the entity's critical functions and services.
- **Risk Mitigation:** Strategies and actions to mitigate identified risks to acceptable levels, including the implementation of protective measures and controls.
- **Risk Monitoring and Reporting:** Ongoing monitoring of the risk landscape and reporting mechanisms to keep management informed of risk status and incidents.
- **Governance:** Roles and responsibilities within the organization for risk management, ensuring accountability and effective oversight.

- **Compliance:** Alignment with legal and regulatory requirements related to ICT risk management and operational resilience.

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

## Importance of the Framework

USE CASES

CONTACT

PDF

The "Risk Management Framework" is vital for establishing a proactive and structured approach to managing ICT risks. It enables financial entities to enhance their resilience, ensuring continuity of operations and protection of

### Stakeholder Communication Plan

This document outlines the strategic approach to communicating with stakeholders during and after ICT incidents, in alignment with the Digital Operational Resilience Act (DORA). The plan ensures timely, accurate, and effective communication to maintain trust and transparency with clients, regulators, partners, and the public.

## Objective

The objective of the "Stakeholder Communication Plan" is to establish predefined communication protocols to manage information dissemination during ICT incidents, minimizing misinformation and maintaining operational integrity.

## Scope

The scope includes all internal and external stakeholders impacted by ICT incidents, detailing communication channels, messaging strategies, and escalation procedures.

## Key Components

1. **Stakeholder Identification:** Categorization of stakeholders and determination of their information needs and preferences.
2. **Communication Channels:** Specification of primary and secondary communication channels tailored to stakeholder groups.
3. **Message Development:** Guidelines for crafting clear, concise, and consistent messages, including templates for various incident types.
4. **Roles and Responsibilities:** Assignment of communication roles within the incident response team, including spokespersons.
5. **Timelines:** Timeline for initial communication and subsequent updates to stakeholders during incident management.
6. **Regulatory Reporting:** Procedures for meeting regulatory reporting requirements, ensuring compliance with DORA and other applicable regulations.

7. **Review and Testing:** Regular review and testing of the communication plan to ensure effectiveness and readiness.

**DORA  
REGULATIONS**

**GOVERNANCE  
AND RISK  
MANAGEMENT**

**OPERATIONAL  
RESILIENCE  
TESTING**

**INCIDENT  
MANAGEMENT  
AND  
RECOVERY**

**ICT  
THIRD-  
PARTY  
RISK**

**INFORMATION  
SHARING**

## Implementation Strategy

**USE CASES**

**CONTACT**

**PDF**

Detailed strategy for implementing the communication plan, including training for spokespersons and simulation exercises.

By adhering to the "Stakeholder Communication Plan," financial entities

### Training and Awareness Programs

Educational initiatives aimed at bolstering the cybersecurity knowledge and practices of the workforce, thus minimizing the risk of human error-induced incidents.

## Step 2: Cyber Threat Reporting and Information Sharing

### Actions to Undertake

Set up a system for internal reporting of cyber threats to designated officers within the organization.

Establish communication channels with external financial authorities and industry partners for threat intelligence sharing.

Create a database for documenting and analyzing reported cyber threats to enhance defensive strategies.

### Deliverables

Cyber Threat Reporting Guidelines

These guidelines aim to establish a consistent and effective framework for reporting cyber threats within financial entities, in accordance with DORA **USE CASES**. The goal is to enhance operational resilience **CONTACT** PDF improving threat detection, information sharing, and incident response.

## Scope

These guidelines apply to all financial entities regulated under DORA, including banks, insurance companies, asset managers, and payment service providers. They cover all types of cyber threats that could affect the continuity and integrity of financial services.

## Key Principles

- **Threat Identification:** Define processes for proactive identification and classification of cyber threats.
- **Immediate Reporting:** Establish procedures for the immediate reporting of cyber incidents to management, regulatory authorities, and, if necessary, affected stakeholders.
- **Information Sharing:** Promote information sharing about threats and vulnerabilities within the financial community and with competent public bodies.
- **Analysis and Assessment:** Provide guidelines for the analysis of cyber incidents and the assessment of their impact on operations and financial stability.
- **Response and Recovery:** Outline steps for an effective response to incidents and recovery of affected services.
- **Continuous Review and Improvement:** Institute a post-incident review process to learn lessons and continuously improve cybersecurity measures.

## Reporting Procedures

- **Reporting Format:** Define the standard format for incident reports, including essential information to be provided.
- **Reporting Channels:** Identify official channels for reporting incidents, both internally and to competent authorities.
- **Reporting Deadlines:** Specify deadlines for reporting different types of cyber incidents.

## Training and Awareness

Implement training and awareness programs to ensure all staff understand their responsibilities in terms of reporting cyber threats.

## Revision and Update

Establish a schedule for regular review of the guidelines to adapt them to evolving cyber threats and regulatory requirements.

### External Communication Protocols

## Objective

The purpose of these protocols is to establish standardized procedures for external communications related to cyber incidents, ensuring consistent, accurate, and timely information sharing with external stakeholders, including regulators, customers, and the public, in compliance with DORA requirements.

## Scope

These protocols apply to all external communications following a cyber incident within financial entities regulated under DORA. This encompasses communications with regulatory bodies, customers, partners, media, and other external parties potentially affected by or interested in the incident.

## Key Principles

- **Transparency:** Provide clear, accurate, and sufficient information about the incident's nature, scope, and impact.

## Communication Channels

Identify and utilize appropriate channels for different stakeholders, including press releases, social media, direct communications to customers, and regulatory filings.

## Communication Templates

Develop standardized templates for various types of incidents to ensure quick and consistent responses. Templates should be customizable to fit the specifics of each incident.

## Roles and Responsibilities

Define roles within the organization responsible for managing external communications during a cyber incident, including a primary spokesperson.

## Training and Drills

Conduct regular training for staff involved in external communications and perform drills to simulate the response to a cyber incident.

## Review and Update

Regularly review and update the communication protocols to reflect changes in regulatory requirements, communication channels, and organizational structure.

Following these External Communication Protocols will help ensure that

## Objective

### USE CASES

### CONTACT

### PDF

The Cyber Threat Database is designed to serve as a comprehensive repository for storing, categorizing, and analyzing information on cyber threats, vulnerabilities, incidents, and their countermeasures. Its purpose is to enhance the cybersecurity posture of financial entities by facilitating informed decision-making and proactive threat response, in alignment with DORA's emphasis on digital operational resilience.

## Scope

This database covers a wide range of cyber threats, including malware, ransomware, phishing attacks, DDoS attacks, and other cyber-related security incidents that could potentially impact the operational resilience of financial entities regulated under DORA. It serves as a central resource for security analysts, IT professionals, and decision-makers within these organizations.

## Key Features

- **Threat Intelligence:** Collects and aggregates threat intelligence from various sources, including industry reports, security bulletins, and incident response activities.
- **Vulnerability Tracking:** Records and tracks known vulnerabilities affecting systems, applications, and infrastructure relevant to the financial sector.
- **Incident Analysis:** Provides tools for the detailed analysis of security incidents, including attack vectors, impacted assets, and the effectiveness of deployed countermeasures.
- **Countermeasure Repository:** Catalogues effective security measures, best practices, and mitigation strategies to address identified threats and vulnerabilities.
- **Search and Reporting:** Offers advanced search capabilities and customizable reporting features to support cybersecurity research and compliance reporting.

## Access and Collaboration

The database is accessible to authorized personnel within the organization, supporting collaboration across different departments to ensure a unified cybersecurity approach. It also enables controlled sharing of anonymized

threat information with industry partners and regulatory bodies to foster a collective defense strategy.

**DORA  
REGULATIONS**

**GOVERNANCE  
AND RISK  
MANAGEMENT**

**OPERATIONAL  
RESILIENCE  
TESTING**

**INCIDENT  
MANAGEMENT  
AND  
RECOVERY**

**ICT  
THIRD-  
PARTY  
RISK**

**INFORMATION  
SHARING**

## Data Security and Privacy

**USE CASES**

**CONTACT**

**PDF**

Implements stringent data security and privacy measures to protect sensitive information contained within the database, ensuring compliance with data protection regulations and industry standards.

## Maintenance and Updates

Regularly updated to reflect the latest threat landscape, with continuous monitoring for new threats and vulnerabilities. Maintenance activities include data verification, quality control, and the integration of user

### Pillar 4 : ICT Third-Party Risk

In today's interconnected business environments, organizations increasingly rely on third-party ICT service providers to support critical operations and deliver key services. While these partnerships offer numerous benefits, including enhanced operational efficiency and access to specialized expertise, they also introduce a range of risks that must be carefully managed. ICT Service Provider Risk Management is a comprehensive approach designed to identify, assess, mitigate, and monitor the risks associated with outsourcing ICT services. Effective risk management ensures that service provider engagements do not expose the organization to undue risk, safeguarding data integrity, operational resilience, and compliance with relevant regulations.

## Step 1: Identification of ICT Service Providers

### Actions to Undertake

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

USE CASES

CONTACT

PDF

Establish criteria for evaluating the risk each service provider poses to the organization's resilience.

Deliverables

Vendor Risk Assessments

Comprehensive evaluations of potential and existing service providers to identify and assess risks related to service delivery, data security, and compliance.

Third-Party Audits and Compliance Reports

Regular audits and reviews of service provider operations to verify compliance with agreed-upon standards and regulatory requirements.

Risk Mitigation Plans

Development and implementation of strategies to reduce identified risks to acceptable levels, including contingency planning for critical service disruptions.

Incident Response Coordination

Establishment of communication and response protocols to ensure timely and coordinated action in the event of a security incident involving a service provider.

Contract Management Processes

Robust procedures for managing contracts with ICT service providers, including regular reviews and renegotiations to address changing risk landscapes.

## Step 2: Assessment of ICT Service Provider Risks

USE CASES

CONTACT

PDF

### Actions to Undertake

Conduct risk assessments for each ICT service provider based on the established criteria.

Identify and document any dependencies and potential single points of failure.

Evaluate the service providers' own risk management and resilience measures.

### Deliverables

ICT Service Provider Risk Assessment Report

#### Objective

The ICT Service Provider Risk Assessment Report aims to systematically evaluate the risks associated with leveraging external ICT service providers. This evaluation is critical to ensuring that financial entities maintain robust operational resilience in line with the mandates of the Digital Operational Resilience Act (DORA). The report identifies potential vulnerabilities and risk exposures from third-party engagements and proposes mitigation strategies to safeguard the entity's digital operations.

#### Scope

The scope of this report includes a comprehensive assessment of all external ICT service providers engaged by the financial entity. It covers various dimensions of risk, including cybersecurity, data privacy, service availability, and compliance risks. The assessment extends to

subcontractors and fourth parties where applicable, to ensure a complete view of the supply chain risk landscape.

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

## Key Components

USE CASES

CONTACT

PDF

- 1. Provider Profile Overview:** Summarizes the services provided, the criticality of these services to the entity's operations, and an overview of the service providers' IT infrastructure and security posture.
- 2. Risk Identification and Analysis:** Details identified risks associated with each ICT service provider, including an analysis of potential impact on the entity's operational resilience.
- 3. Control and Mitigation Measures:** Evaluates the effectiveness of existing controls implemented by the service providers and outlines additional mitigation measures to address identified risks.
- 4. Compliance Assessment:** Assesses the ICT service providers' compliance with relevant regulations, industry standards, and contractual obligations.
- 5. Risk Monitoring and Management:** Recommends strategies for ongoing monitoring, management, and reporting of ICT service provider risks.
- 6. Action Plan:** Proposes a prioritized action plan to address significant risks, including timelines and responsibilities.

## Methodology

Describes the methodology employed to conduct the risk assessment, including data sources, assessment criteria, and risk evaluation techniques.

## Conclusion and Recommendations

Provides a summary of key findings and prioritized recommendations for enhancing the entity's management of ICT service provider risks, ensuring alignment with DORA's operational resilience objectives.

This "ICT Service Provider Risk Assessment Report" serves as an essential

Dependencies and Single Points of Failure Analysis

## Objective

The objective of this document is to provide a detailed analysis of dependencies and single points of failure within the ICT service supply

This report encompasses an examination of all critical ICT services and components utilized by the financial entity, including both internal systems and external service providers. It aims to map out the interdependencies among these components and identify any single points of failure that could pose significant risks to the entity's operational continuity.

## Key Components

- 1. Dependency Mapping:** Visual and descriptive mapping of the relationships between all critical ICT services and components, highlighting interdependencies.
- 2. Single Points of Failure Identification:** Identification and analysis of single points of failure within the mapped dependencies, including the potential impact of failure on operations.
- 3. Risk Assessment:** Assessment of the risks associated with identified dependencies and single points of failure, considering factors such as likelihood of failure and potential severity of impact.
- 4. Control and Mitigation Strategies:** Recommendations for control measures and mitigation strategies to address identified risks, including diversification of service providers, implementation of redundancy measures, and enhancement of monitoring and incident response capabilities.
- 5. Compliance Considerations:** Analysis of compliance with DORA requirements related to the management of ICT service provider risks and operational resilience.
- 6. Recommendations for Improvement:** Prioritized recommendations for reducing dependency risks and eliminating single points of failure, with suggested timelines and responsibilities for implementation.

## Methodology

Overview of the methodologies used to conduct the analysis, including data collection techniques, risk evaluation methods, and tools for dependency mapping.

## Conclusion

## Objective

The "Service Provider Resilience Evaluation" document aims to assess the resilience of ICT service providers engaged by financial entities, ensuring these providers have robust mechanisms in place to maintain service continuity and protect against disruptions. This evaluation supports financial entities in complying with the Digital Operational Resilience Act (DORA) by ensuring their critical operations are supported by resilient ICT services.

## Scope

This evaluation covers all external ICT service providers that supply critical services and infrastructure to the financial entity. It includes an assessment of their resilience in the face of cyber threats, technical failures, and other operational disruptions. The scope extends to the examination of service provider policies, procedures, and controls related to resilience and recovery capabilities.

## Key Components

- Provider Resilience Framework:** An analysis of the service provider's resilience framework, including governance structures, risk management processes, and resilience strategies.
- Incident Management and Recovery:** Evaluation of the service provider's incident response, disaster recovery, and business continuity plans, including their testing and validation processes.
- Service Continuity Capabilities:** Assessment of the provider's capabilities to ensure service continuity in the event of disruptions, including redundancy, failover processes, and backup systems.
- Compliance and Regulatory Adherence:** Review of the service provider's compliance with relevant regulations and standards, including data protection and cybersecurity requirements.
- Third-Party and Subcontractor Management:** Examination of how the service provider manages risks associated with their own third-party vendors and subcontractors.
- Risk Assessment and Mitigation:** Insights into the provider's risk assessment processes and how identified risks are mitigated, especially those that may impact the financial entity.

## Conclusion and Recommendations

Provides a summary of the evaluation findings, highlighting areas of strength and concern. It offers recommendations for the financial entity to address any identified gaps in service provider resilience, ensuring alignment with DORA requirements and enhancing overall operational resilience.

Conducting a "Service Provider Resilience Evaluation" is crucial for

## Step 3: Implementation of Risk Management Controls

### Actions to Undertake

Develop and implement risk management controls to mitigate identified risks associated with ICT service providers.

Establish service level agreements (SLAs) that include compliance with the organization's security and resilience standards.

Set up continuous monitoring mechanisms to oversee service provider performance and adherence to SLAs.

Regular due diligence and auditing processes to ensure supplier compliance.

Risk Management Controls Framework

## Objective

The "Risk Management Controls Framework" document is designed to establish a comprehensive set of controls and measures aimed at identifying, assessing, monitoring, and mitigating the various risks associated with ICT and digital operations within financial entities. This framework is developed to support entities in meeting the Digital Operational Resilience Act (DORA) requirements, ensuring a robust defense against operational disruptions and cyber threats.

## Scope

The framework covers the entire spectrum of ICT-related risks, including cybersecurity threats, data breaches, system failures, and third-party service provider vulnerabilities. It applies to all digital and ICT operations within the entity, spanning across internal systems, external services, and interconnected networks.

## Key Components

- Risk Identification:** Processes and tools for the systematic identification of digital and ICT risks.
- Risk Assessment:** Methodologies for evaluating the impact and likelihood of identified risks, including qualitative and quantitative measures.
- Risk Mitigation:** Strategies and measures for mitigating risks, including preventive controls, detective controls, and corrective actions.
- Monitoring and Reporting:** Continuous monitoring of the risk environment and reporting mechanisms to ensure timely awareness and response to emerging risks.
- Compliance Management:** Controls to ensure compliance with relevant regulations, standards, and best practices, including DORA's requirements.
- Incident Management:** Procedures for the effective management and response to ICT-related incidents, minimizing impact and

## Implementation Guidelines

Detailed guidelines for the implementation of the risk management controls framework, including roles and responsibilities, timelines, and resource allocation.

### Conclusion

Summarizes the importance of the risk management controls framework in enhancing the entity's operational resilience, aligning with DORA's objectives, and safeguarding against a broad range of digital and ICT risks.

#### Service Level Agreements with ICT Providers

### Objective

The purpose of this document is to outline the establishment of Service Level Agreements (SLAs) between financial entities and their ICT service providers. These agreements are essential for defining the standards of service, performance metrics, and the responsibilities of both parties, ensuring that ICT services align with the operational resilience requirements set forth by the Digital Operational Resilience Act (DORA).

### Scope

The scope of these SLAs encompasses all ICT services procured by the financial entity, including cloud computing, data storage, cybersecurity solutions, and software applications. The agreements cover the delivery, management, and support of these services, focusing on the aspects critical to maintaining operational resilience.

### Key Components

- Service Description:** Detailed description of the services provided, including technical specifications and performance expectations.

2. **Performance Metrics:** Definition of key performance indicators (KPIs) and service level objectives (SLOs) to measure service quality and availability. Specifics of the provider's responsibilities in managing risks related to service delivery, including cybersecurity and data protection measures.
3. **Risk Assessment:** Identification and evaluation of risks to service continuity, including recovery time objectives (RTOs) and recovery point objectives (RPOs).
4. **Incident Response and Reporting:** Protocols for incident management, including reporting requirements, escalation procedures, and communication plans.
5. **Compliance and Auditing:** Agreement on compliance with relevant regulations and standards, and the right to conduct audits to verify compliance and service effectiveness.
6. **Remedies and Penalties:** Conditions under which penalties or remedies may be applied for failure to meet service levels, including compensation mechanisms for service disruptions.
7. **Termination and Exit Strategy:** Terms for contract termination, including data retention, service transition, and exit support to ensure continuity of operations.

## Implementation Guidelines

Guidance for negotiating and implementing SLAs with ICT providers, including considerations for risk assessment, due diligence, and ongoing monitoring of service levels.

## Conclusion

Emphasizes the critical role of SLAs in managing relationships with ICT providers, ensuring service quality, and maintaining operational resilience in compliance with DORA regulations.

### Service Provider Monitoring Procedures

## Objective

The "Service Provider Monitoring Procedures" document outlines the systematic approach financial entities must adopt to monitor and review the performance and risk management practices of their ICT service providers. This process is critical for ensuring that service delivery aligns with the operational resilience objectives mandated by the Digital Operational Resilience Act (DORA).

## Scope

## Key Components

1. **Monitoring Framework:** Establishment of a structured framework for ongoing monitoring of service providers, including key performance indicators (KPIs) and risk indicators.
2. **Performance Review Procedures:** Detailed procedures for conducting periodic performance reviews, assessing service level compliance, and evaluating the effectiveness of risk controls.
3. **Incident Response and Reporting:** Protocols for managing and reporting incidents involving service providers, detailing response strategies, escalation paths, and communication plans.
4. **Risk Assessment Updates:** Guidelines for updating risk assessments based on monitoring outcomes, changing risk landscapes, or emerging threats.
5. **Audit and Compliance Checks:** Procedures for conducting audits of service providers, ensuring adherence to contractual obligations, regulatory requirements, and industry standards.
6. **Remediation and Improvement Actions:** Mechanisms for addressing deficiencies identified during monitoring, including timelines for remediation and follow-up verification.

## Implementation and Communication

Strategies for implementing the monitoring procedures within the entity's operational framework, including roles and responsibilities, resource allocation, and communication channels.

## Conclusion

Emphasizes the importance of effective and systematic monitoring of ICT service providers as a critical component of operational resilience, in compliance with DORA's requirements.

By adopting the "Service Provider Monitoring Procedures," financial entities

In the digital era, cybersecurity information sharing has emerged as a pivotal component for enhancing the collective resilience of the financial sector. The Digital Operational Resilience Act (DORA) recognizes the importance of establishing robust channels for sharing cybersecurity-related information among financial entities, regulatory bodies, and other stakeholders. This chapter introduces the foundational principles and objectives that guide cybersecurity information sharing practices under DORA, emphasizing the role of collaboration in preempting, mitigating, and responding to cyber threats effectively.

## Objectives of Cybersecurity Information Sharing

The primary objectives of cybersecurity information sharing under DORA include:

- **Promoting Transparency:** Facilitating an open exchange of information regarding cyber threats, vulnerabilities, and incidents to foster a culture of transparency within the financial sector.
- **Enhancing Situational Awareness:** Improving the collective situational awareness of cyber risks, enabling financial entities to make informed decisions and prioritize cybersecurity measures.
- **Facilitating Timely Response:** Accelerating the dissemination of critical cybersecurity intelligence, ensuring that financial entities can respond to and mitigate the impact of cyber incidents promptly.
- **Building Collective Resilience:** Strengthening the resilience of the financial ecosystem by pooling resources, knowledge, and best practices in cybersecurity management.

This introduction sets the stage for a detailed exploration of the mechanisms, protocols, and best practices that underpin effective cybersecurity information sharing within the framework of DORA. By adhering to these guidelines, financial entities can contribute to a more secure and resilient digital operational environment, safeguarding not only their operations but also the broader financial system from cyber threats.

## Step 1: Establishing a Cybersecurity Information Sharing Framework

### Actions to Undertake

**DORA  
REGULATIONS**

**GOVERNANCE  
AND RISK  
MANAGEMENT**

**OPERATIONAL  
RESILIENCE  
TESTING**

**INCIDENT  
MANAGEMENT  
AND  
RECOVERY**

**ICT  
THIRD-  
PARTY  
RISK**

**INFORMATION  
SHARING**

**USE CASES**

**CONTACT**

**PDF**

Collaborate with the financial sector-specific information sharing community through platforms like MISP Financial Sector.

## Deliverables

### Cybersecurity Information Sharing Policy Document

The "Cybersecurity Information Sharing Policy Document" serves as a cornerstone for establishing a structured and secure framework for sharing cybersecurity-related information within the financial sector. This policy document is crafted to align with the principles and mandates of the Digital Operational Resilience Act (DORA), aiming to enhance the collective cybersecurity posture of financial entities through effective collaboration and information exchange.

## Policy Objectives

This policy document outlines the objectives for cybersecurity information sharing, including:

- Strengthening the sector's ability to detect, prevent, and respond to cyber threats.
- Creating a culture of transparency and cooperation among financial entities.
- Ensuring the protection and confidentiality of shared information.
- Complying with regulatory requirements under DORA.

## Scope of Information Sharing

The document specifies the types of information to be shared, which may include threat intelligence, vulnerability disclosures, incident reports, and best practices for cybersecurity risk management.

## Participation Guidelines

Detailed guidelines for participation, including eligibility criteria for entities wishing to join the information-sharing framework, responsibilities of participants, and the process for onboarding new members.

# Data Protection and Confidentiality

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

## Roles and Responsibilities

USE CASES

CONTACT

PDF

Clear definition of roles and responsibilities for all parties involved in the information-sharing process, including the designation of a central coordinating body.

## Implementation and Governance

Framework for the implementation and governance of the information-sharing policy, including mechanisms for monitoring compliance, resolving disputes, and updating the policy as needed.

MISP Integration Plan

### Objective

The "MISP Integration Plan" is designed to facilitate the structured integration of the Malware Information Sharing Platform & Threat Sharing (MISP) into the financial entity's cybersecurity framework. This plan aims to enhance the entity's capability to share, receive, and analyze cybersecurity threat information efficiently, in alignment with the objectives of the Digital Operational Resilience Act (DORA).

### Scope

The scope of this plan includes the technical integration of MISP, training of personnel on its use, and the establishment of processes for sharing and managing cybersecurity information within the MISP platform.

### Key Components

- Technical Integration:** Detailed steps for the technical setup of MISP, including server configuration, security measures, and integration with existing cybersecurity tools.
- Data Governance:** Policies for data management within MISP, focusing on data quality, confidentiality, and integrity.
- User Training:** A training program for relevant staff on how to use MISP effectively, covering threat intelligence sharing, analysis techniques, and best practices.
- Sharing Protocols:** Establishment of protocols for sharing information within MISP, including guidelines on what information to

## Implementation Timeline

A phased timeline for the implementation of the MISP integration plan, outlining key milestones, responsibilities, and expected completion dates.

## Monitoring and Evaluation

Strategies for monitoring the effectiveness of MISP integration and its impact on the financial entity's cybersecurity posture, with provisions for periodic evaluation and adjustments to the plan as necessary.

### Financial Sector Collaboration Agreements

## Objective

The "Financial Sector Collaboration Agreements" document aims to formalize partnerships and collaborative efforts among financial entities for sharing cybersecurity information and best practices. This initiative is designed to enhance the collective resilience of the financial sector against cyber threats, in accordance with the Digital Operational Resilience Act (DORA).

## Scope

The scope of these agreements includes the sharing of threat intelligence, vulnerability information, incident reports, and mitigation strategies among participating financial entities. The agreements outline the framework for collaboration, focusing on improving the detection, prevention, and response to cybersecurity threats within the sector.

## Key Components

1. **Participation Criteria:** Defines the eligibility criteria for financial entities wishing to participate in the collaboration agreements.
2. **Information Sharing:** Establishes the scope, standards, and protocols for sharing threat intelligence, security information, and indicators of compromise (IoCs) while ensuring the protection of sensitive data and compliance with regulatory requirements.
3. **Roles and Responsibilities:** Details the roles and responsibilities of participating entity, including investigations for contributing and utilizing the shared information.
4. **Security and Confidentiality:** Specifies measures to ensure the security and confidentiality of shared information, protecting against unauthorized access and data breaches.
5. **Governance Structure:** Outlines the governance structure for overseeing the collaboration agreements, including the establishment of a coordinating body or committee.
6. **Dispute Resolution:** Provides mechanisms for resolving disputes among participants related to information sharing or agreement interpretation.
7. **Review and Amendment:** Describes the process for reviewing and amending the agreements to adapt to evolving cybersecurity threats and regulatory changes.

## Benefits of Collaboration

Highlights the benefits of sector-wide collaboration, including enhanced threat intelligence, accelerated incident response times, and a unified approach to cybersecurity challenges.

## Step 2: Participating in Threat Intelligence Sharing

### Actions to Undertake

Actively share indicators of compromise (IoCs) and other cybersecurity threat information with peers.

Develop internal procedures for analyzing, processing, and disseminating threat intelligence from MISP.

## Threat Intelligence Sharing Reports

### Objective

The "Threat Intelligence Sharing Reports" are designed to provide comprehensive insights into current cybersecurity threats, vulnerabilities, and incidents relevant to the financial sector. This initiative, mandated under the Digital Operational Resilience Act (DORA), aims to facilitate the exchange of timely and actionable threat intelligence among financial entities, enhancing the sector's collective ability to preempt, mitigate, and respond to cyber threats effectively.

### Scope

The reports cover a wide range of cybersecurity topics, including but not limited to malware trends, phishing campaigns, advanced persistent threats (APTs), and emerging vulnerabilities. They aim to encompass all relevant threat intelligence that could impact the operational resilience of financial entities.

### Key Components

- Threat Descriptions:** Detailed analysis of identified threats, including their mechanisms, targets, and potential impact on the financial sector.
- Vulnerability Assessments:** Assessments of current vulnerabilities within financial entities' IT systems and infrastructure, including severity ratings and recommended mitigation strategies.
- Incident Reports:** Summaries of recent cybersecurity incidents within the sector, including attack vectors, consequences, and lessons learned.
- Best Practices:** Compilation of cybersecurity best practices and preventive measures to enhance entities' defenses against identified threats.

5. **Regulatory Updates:** Updates on regulatory changes or guidance relevant to cybersecurity and operational resilience within the

DORA  
REGULATIONS

GOVERNANCE  
AND RISK  
MANAGEMENT

OPERATIONAL  
RESILIENCE  
TESTING

INCIDENT  
MANAGEMENT  
AND  
RECOVERY

ICT  
THIRD-  
PARTY  
RISK

INFORMATION  
SHARING

USE CASES

Distribution of Reports and Access

CONTACT

PDF

Guidelines for the distribution of reports among participating entities, ensuring secure access to threat intelligence while maintaining confidentiality and data protection standards.

## Feedback and Collaboration Mechanisms

Procedures for entities to provide feedback on reports and contribute their

Internal Threat Intelligence Handling Procedures

### Objective

The "Internal Threat Intelligence Handling Procedures" document outlines the structured approach for managing and utilizing threat intelligence within a financial entity. These procedures aim to ensure that threat intelligence is effectively processed, analyzed, and acted upon to enhance the entity's cybersecurity posture, in line with the Digital Operational Resilience Act (DORA).

### Scope

This document covers the entire lifecycle of threat intelligence within the organization, including collection, processing, dissemination, and storage of intelligence. It applies to all forms of threat intelligence, whether obtained from external sources, shared through industry collaborations, or generated internally.

### Key Components

- Collection:** Guidelines for collecting threat intelligence from various sources, ensuring relevance and reliability of the information.
- Processing:** Procedures for processing and analyzing collected intelligence to assess its applicability and urgency.
- Dissemination:** Protocols for disseminating actionable intelligence to relevant stakeholders within the organization, ensuring timely and secure communication.

## Roles and Responsibilities

Definition of roles and responsibilities for staff involved in threat intelligence handling, including training requirements to ensure competence and compliance with these procedures.

## Compliance and Auditing

Measures to ensure compliance with legal, regulatory, and policy requirements related to threat intelligence handling, including provisions for regular audits and reviews of the procedures.

### Cybersecurity Collaboration Workshops and Training Sessions

## Objective

The objective of "Cybersecurity Collaboration Workshops and Training Sessions" is to foster a culture of knowledge sharing and collective defense within the financial sector against cyber threats. These initiatives, recommended under the Digital Operational Resilience Act (DORA), aim to equip financial entities and their personnel with the latest cybersecurity practices, threat intelligence insights, and collaborative strategies for enhancing sector-wide resilience.

## Scope

The scope of these workshops and training sessions includes the dissemination of current cyber threat landscapes, sharing of best practices in threat detection and response, and the development of collaborative strategies for threat intelligence sharing among financial entities.

DORA REGULATIONS

GOVERNANCE AND RISK MANAGEMENT

OPERATIONAL RESILIENCE TESTING

INCIDENT MANAGEMENT AND RECOVERY

ICT THIRD-PARTY RISK

INFORMATION SHARING

USE CASES

CONTACT

PDF

1. **Workshop Agenda:** Detailed schedule of various cybersecurity topics, including threat intelligence analysis, incident response planning, and the use of shared cybersecurity tools and frameworks.

2. **Training Curriculum:** Structured training sessions designed to enhance the cybersecurity skills of participants, focusing on practical exercises, case studies, and simulations.

3. **Collaboration Exercises:** Interactive exercises aimed at promoting teamwork and collaboration among entities, simulating real-world scenarios to improve collective response strategies.

4. **Expert Panels and Guest Speakers:** Sessions led by cybersecurity experts, offering insights into emerging threats and innovative defense mechanisms.

5. **Feedback and Evaluation:** Mechanisms for collecting feedback from participants to assess the effectiveness of the workshops and training sessions, guiding future improvements.

### Participation and Access

Guidelines for financial entities on how to participate in these workshops and training sessions, including registration processes, prerequisites, and access to training materials.

### Outcomes and Benefits

Expected outcomes include enhanced cybersecurity awareness among financial entities, improved readiness to tackle cyber threats, and strengthened networks for collaborative defense within the financial sector.

By participating in "Cybersecurity Collaboration Workshops and Training

## Step 3: Enhancing Sector-Wide Cyber Resilience

### Actions to Undertake

Use shared threat intelligence to enhance your organization's cyber

Regularly review and update cyber resilience strategies to reflect the evolving threat landscape.

Collaboration with regulatory authorities for effective collective defense.

Active participation in information sharing networks to stay informed of the latest threats and trends.

### Deliverables

Cyber Defense Enhancement Report

### Objective

The "Cyber Defense Enhancement Report" aims to document and assess the efforts and initiatives undertaken by financial entities to bolster their cyber defense capabilities. This report supports the overarching goal of the Digital Operational Resilience Act (DORA) to enhance sector-wide cyber resilience, providing insights into progress made, challenges encountered, and opportunities for further enhancements in cyber defense strategies.

### Scope

This report covers a comprehensive analysis of cyber defense mechanisms, including technological solutions, procedural updates, employee training programs, and collaboration efforts within the financial sector. It aims to highlight the advancements made in protecting against, detecting, and responding to cyber threats.

### Key Components

DORA REGULATIONS	1. <b>Technological Advancements:</b> Overview of new technologies and tools implemented to strengthen cyber defenses, including (e.g., AI, cloud security, and zero-trust architectures).			
	<b>GOVERNANCE AND RISK MANAGEMENT</b>	<b>OPERATIONAL RESILIENCE TESTING</b>	<b>INCIDENT MANAGEMENT AND RECOVERY</b>	<b>ICT THIRD-PARTY RISK</b>
2. <b>Procedural Updates:</b> Description of updated cybersecurity policies and procedures aimed at enhancing operational resilience against cyber threats.				
3. <b>Training and Awareness:</b> Summary of training in PDF/es designed to improve cybersecurity awareness and skills among employees at all levels within financial entities.				

- 4. **Collaboration and Information Sharing:** Insights into collaborative efforts and information-sharing mechanisms established with other financial entities, regulatory bodies, and cybersecurity organizations to enhance sector-wide cyber resilience.
- 5. **Challenges and Mitigation Strategies:** Analysis of challenges faced in enhancing cyber defenses and the strategies employed to mitigate these challenges.
- 6. **Recommendations for Further Enhancements:** Actionable recommendations for financial entities to continue improving their cyber defense capabilities in alignment with DORA's objectives.

## Methodology

Explanation of the methodology used to gather data, assess cyber defense enhancements, and develop the report, including tools, surveys, interviews, and analysis techniques.

## Conclusion

Concluding remarks emphasizing the importance of ongoing efforts to enhance cyber defense capabilities and the critical role of collaboration and information sharing in achieving sector-wide cyber resilience.

Sector-Wide Best Practices Documentation

## Objective

The "Cyber Defense Enhancement Report" aims to document and assess the efforts and initiatives undertaken by financial entities to bolster their cyber defense capabilities. This report supports the overarching goal of the Digital Operational Resilience Act (DORA) to enhance sector-wide cyber resilience, providing insights into progress made, challenges encountered, and opportunities for further enhancements in cyber defense strategies.

DORA REGULATIONS	GOVERNANCE AND RISK MANAGEMENT	OPERATIONAL RESILIENCE TESTING	INCIDENT MANAGEMENT AND RECOVERY	ICT THIRD- PARTY RISK	INFORMATION SHARING
This report covers a comprehensive analysis of the current state of cyber defense mechanisms, including technological solutions, procedural updates, employee training programs, and collaboration efforts within the financial sector. The purpose of this report is to highlight the areas for improvement and provide actionable recommendations to enhance the overall resilience of the financial system against cyber threats.					
USE CASES	CONTACT				PDF

## Key Components

- Technological Advancements:** Overview of new technologies and tools implemented to strengthen cyber defenses, including advancements in threat intelligence platforms, security operations centers (SOCs), and encryption technologies.
- Procedural Updates:** Description of updated or newly established cybersecurity policies and procedures aimed at enhancing operational resilience against cyber threats.
- Training and Awareness Programs:** Summary of training initiatives designed to improve cybersecurity awareness and skills among employees at all levels within financial entities.
- Collaboration and Information Sharing:** Insights into collaborative efforts and information-sharing mechanisms established with other financial entities, regulatory bodies, and cybersecurity organizations to enhance sector-wide cyber resilience.
- Challenges and Mitigation Strategies:** Analysis of challenges faced in enhancing cyber defenses and the strategies employed to mitigate these challenges.
- Recommendations for Further Enhancements:** Actionable recommendations for financial entities to continue improving their cyber defense capabilities in alignment with DORA's objectives.

## Methodology

Explanation of the methodology used to gather data, assess cyber defense enhancements, and develop the report, including tools, surveys, interviews, and analysis techniques.

## Conclusion

Concluding remarks emphasizing the importance of ongoing efforts to enhance cyber defense capabilities and the critical role of collaboration and information sharing in achieving sector-wide cyber resilience.

## Objective

USE CASES

CONTACT

PDF

The "Updated Cyber Resilience Strategies" document aims to provide a comprehensive overview of the revised strategies and practices adopted by financial entities to bolster their cybersecurity and operational resilience. This update, in line with the mandates of the Digital Operational Resilience Act (DORA), reflects the evolving cyber threat landscape and the need for continuous enhancement of cyber defenses within the financial sector.

## Scope

The scope of these strategies includes the identification, protection, detection, response, and recovery from cyber incidents. It encompasses technological solutions, procedural guidelines, personnel training, and collaboration efforts both within and across entities in the financial sector.

## Key Components

- Strategic Objectives:** Clear articulation of the strategic objectives guiding the entity's cyber resilience efforts, aligned with DORA's requirements.
- Threat Identification and Assessment:** Updated mechanisms for the ongoing identification and assessment of cyber threats and vulnerabilities.
- Defense Mechanisms:** Enhanced technological and procedural defense mechanisms implemented to protect against identified threats.
- Incident Detection and Analysis:** Advanced tools and processes for the timely detection and analysis of cybersecurity incidents.
- Response and Recovery Plans:** Comprehensive response and recovery plans to minimize the impact of cyber incidents and ensure rapid restoration of services.
- Training and Awareness Programs:** Expanded training and awareness programs to ensure that all personnel are equipped to contribute to cyber resilience efforts.
- Collaboration and Information Sharing:** Strengthened collaboration and information-sharing initiatives with other financial entities, regulatory bodies, and cybersecurity organizations.
- Regulatory Compliance:** Assurance of compliance with DORA and other relevant cybersecurity regulations and standards.

## Implementation Plan

A detailed plan outlining the steps for implementing the updated cyber resilience strategies, including timelines, responsibilities, and resource allocation.

**DORA  
REGULATIONS**

**GOVERNANCE  
AND RISK  
MANAGEMENT**

**OPERATIONAL  
RESILIENCE  
TESTING**

**INCIDENT  
MANAGEMENT  
AND  
RECOVERY**

**ICT  
THIRD-  
PARTY  
RISK**

**INFORMATION  
SHARING**

**USE CASES**

**Monitoring and Evaluation**

**PDF**

Procedures for the ongoing monitoring and evaluation of the effectiveness of the updated strategies, ensuring adaptability to the evolving cyber threat landscape.

GPT for DORA regulations



## GPT for DORA Framework

Cryptaguard have created a GPT specialized on DORA

[GPT for DORA regulations](#)

## Contact Us

For more information or inquiries, please feel free to reach out to us. You can either fill out the form below or send us an email directly:

[info@regulation-dora.eu](mailto:info@regulation-dora.eu)

**Cryptaguard** © 2024 All rights reserved.