

Get ready for DORA

*A guide to help Financial Institutions with
practical cyber governance implementation*

December, 2024

Market Analysis by RSM Business Intelligence Services

Introduction

This report offers a practical and interpretative guide to understanding the Digital Operational Resilience Act (DORA), tailored specifically for financial institutions. In today's increasingly digital financial landscape, operational resilience is not just a regulatory requirement but a critical necessity. DORA represents a landmark in regulatory efforts within the European Union (EU), aimed at ensuring that financial entities are adequately prepared to manage and withstand digital disruptions and cyber threats.

DORA establishes a framework that financial institutions must follow to enhance their digital operational resilience. This includes developing robust ICT risk management strategies, implementing effective incident response protocols, conducting operational resilience testing, managing third-party risks, and ensuring seamless information sharing across the sector. **However, interpreting and implementing these requirements can be challenging, which is where this report comes in.**

We break down the requirements into manageable parts, offering examples that translate the regulatory language into actionable steps that institutions can take.

Our report is designed to help financial institutions navigate the complexities of DORA by offering practical examples and actionable insights. Rather than a mere summary of the regulation, we provide a deep dive into how institutions can effectively apply the principles of DORA in their day-to-day operations. We explore the nuances of DORA, illustrating how they can be integrated into existing frameworks to not only comply with regulatory demands but also to build a stronger, more resilient financial business.

At the end, this report includes a checklist that financial institutions can use to assess their current status and determine key priorities for achieving compliance. **This checklist aids institutions in setting priorities and navigating in the right direction.**

Thank you for reading an RSM Business Consulting report.



DORA Overview

The DORA is a European regulation aimed at enhancing the cyber resilience of financial institutions. It mandates that these institutions must implement comprehensive measures to ensure they can withstand, respond to, and recover from ICT-related disruptions and cyber threats.

Financial entities have until January 17, 2025, to comply with DORA's stringent requirements.

DORA's scope is extensive, covering a wide range of financial entities, including banks, insurance companies, investment firms, and payment service providers. The regulation also applies to critical third-party service providers, ensuring that the entire financial ecosystem is robust and secure. The complete scope can be found in [art. 2 of the regulation](#). DORA aims to build a resilient and secure financial system capable of withstanding the growing complexity of digital risks.

What does it cover?



ICT risk management

Principles and requirements on ICT risk management framework



ICT third-party risk management

Monitoring third-party risk providers
Key contractual provisions



Digital operational resilience testing

Basic and advanced testing



ICT-related incidents

General requirements and reporting of major ICT-related incidents



Information sharing

Exchange of information and intelligence on cyber threats



Oversight of critical third-party providers

Oversight for third-party providers

Technical Definitions



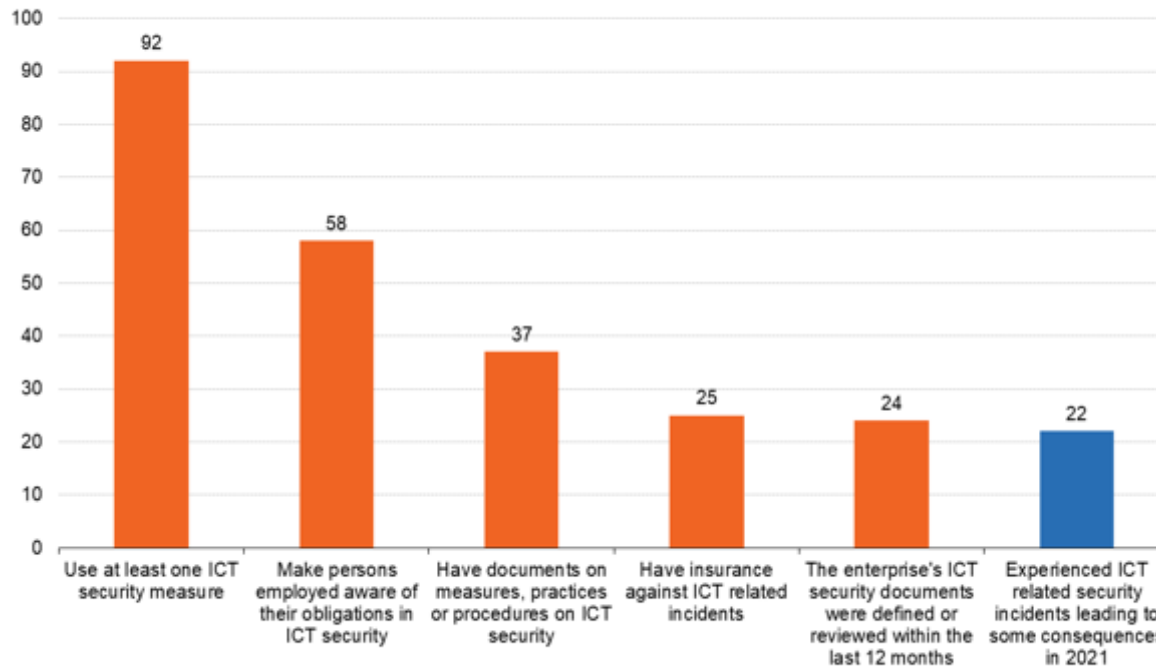
Before we start with the content it is important to understand key technical definitions to help non-technical readers understand the report.

1. **Regulation (EU):** A legal act of the European Union that becomes immediately enforceable as law in all member states simultaneously. It aims to ensure uniform application across the whole EU.
2. **ICT (Information and Communication Technology) Risk Management:** A structured approach to identifying, assessing, and mitigating risks related to ICT systems. This includes the establishment of governance structures, risk management frameworks, and the implementation of specific tools and protocols.
3. **CVE (Common Vulnerabilities and Exposures):** A (publicly or internally available) database that tracks known cybersecurity vulnerabilities. It is used by organisations to identify and mitigate security flaws within their systems.
4. **SQL Injection:** A type of cyber-attack where an attacker injects malicious SQL code into a query, potentially allowing unauthorised access to a database and the data it contains.
5. **Query:** In technical terms, it involves sending a request to a database or information system to retrieve specific data or information based on certain criteria.
6. **Phishing:** A method of cyber-attack where attackers impersonate legitimate entities to trick individuals into revealing sensitive information, such as passwords or credit card details.
7. **Disk Failure:** A hardware failure in a storage device, such as a hard drive, leading to potential data loss or system downtime. It is typically monitored by system health tools to prevent critical failures.
8. **Agent:** Software installed on user PCs or servers that monitors and manages security events. Agents play a critical role in detecting and responding to incidents within an ICT environment.
9. **Active Directory (AD):** A Microsoft directory service that provides centralized management of networked resources, such as user accounts, computers, and security policies in a Windows domain network.
10. **IDS (Intrusion Detection System):** A network security tool that monitors traffic for suspicious activities and alerts security teams to potential threats.
11. **IPS (Intrusion Prevention System):** A network security device that actively monitors and prevents identified threats by blocking or stopping suspicious activities in real-time.
12. **Malware:** Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Examples include ransomware, viruses, and spyware.
13. **Server:** A computer system that provides data, services, or resources to other computers within a network. Servers are essential components of IT infrastructure.
14. **RTS & ITS (Regulatory Technical Standards & Implementing Technical Standards):** Specific standards issued by European regulatory bodies to ensure consistent implementation of EU regulations across member states. RTS provides detailed rules, while ITS focuses on the practical application of these rules.

Background DORA

Growing ICT dependency in the EU

ICT security in enterprises, EU, 2022
(% enterprises)



Source: Eurostat (online data codes: isoc_cisce_ra and isoc_cisce_ic)

eurostat 

Over 90% of enterprises in the EU use the internet for business purposes, and nearly 75% have a website. This highlights the critical role of ICT in daily operations.

In the digital age, Information and Communication Technology (ICT) forms the backbone of modern enterprises. However, the increasing reliance on ICT systems also brings about significant risks that can threaten the operational resilience and security of organizations.

To mitigate these risks, it is crucial to adopt a structured approach to ICT risk management, covering aspects such as governance, incident management, resilience testing, and third-party risk management. This report outlines a comprehensive framework for managing ICT-related risks, drawing on best practices and tailored strategies to ensure organizational resilience.

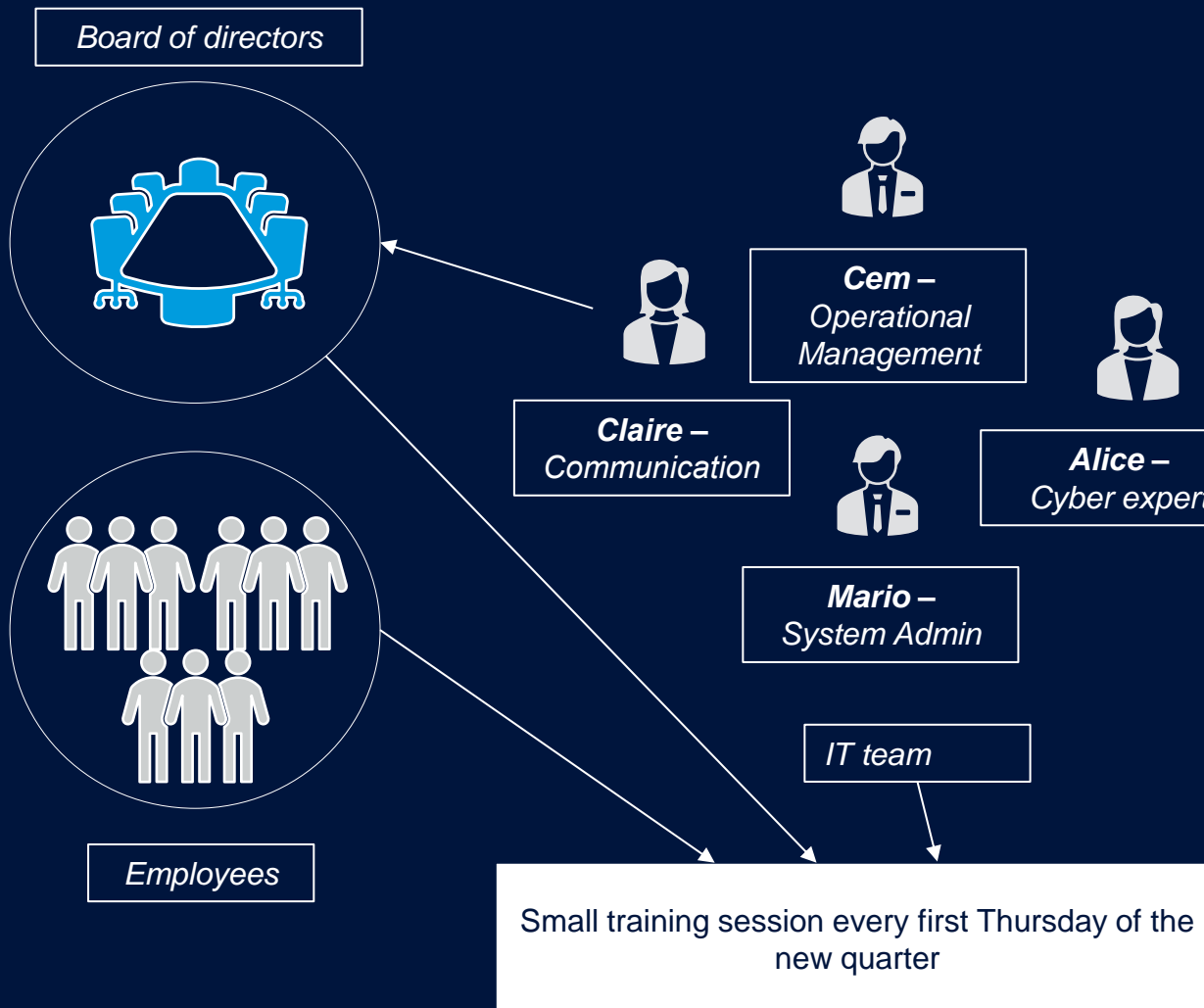
Key Statistics:

- **Cybersecurity Incidents:** In 2022, 68% of large enterprises in the EU reported at least one ICT security incident, underscoring the significant risks associated with ICT systems (European Commission, 2022).
- **Financial Impact:** The average cost of a data breach globally was \$4.24 million in 2021, highlighting the potential financial risks that ICT-related incidents can pose to organizations.

Pillar 1: ICT Risk Management

A. Governance and Organization

Effective ICT risk management begins with the establishment of clear governance structures. These structures define the roles and responsibilities of various stakeholders within the organization, ensuring that each aspect of risk management is adequately covered. Here is an example:



Key Personnel

Role/Responsibility

**Claire
(Communication)**

Manages internal and external communication during incidents, ensuring that all stakeholders are informed.

**Cem
(Operational Management)**

Oversees the operational response to incidents, focusing on maintaining business continuity.

**Alice
(Tech/Cyber)**

Handles cybersecurity measures and responds to technical threats.

**Mario
(System Admin)**

Maintains system integrity and coordinates technical responses during incidents.

Now we have a clear and defined team to manage the company's risks, each with their own specialities and defined roles.

Regular training sessions are essential to keep the team prepared. These sessions should be scheduled at the start of each quarter, focusing on the latest threats, updates in protocols, and the deployment of new tools.

Pillar 1: ICT Risk Management

B. ICT Risk Management Framework



Financial entities are required to maintain a robust, comprehensive, and well-documented ICT risk management framework as an integral part of their overall risk management system. This framework should enable them to address ICT risks promptly, efficiently, and thoroughly, ensuring a high level of digital operational resilience. A robust ICT risk management framework is vital for identifying, assessing, and mitigating risks. This framework should encompass policies, procedures, protocols, and tools designed to manage risks effectively.

Risk Identification and Assessment

The first step in managing risks is to clearly identify them. An exhaustive list of potential risks should be developed, categorized into cyber risks, system risks, and real-world risks.

Categories of Risks	Examples
Cyber Risks	<ul style="list-style-type: none">- Internal ransomware- Phishing attacks- Malware- Insider threats- Data breaches- Vulnerabilities in production environments
System Risks	<ul style="list-style-type: none">- Hardware failures- Network disruptions
Real-World Risks	<ul style="list-style-type: none">- Fires- Natural disasters- Grid congestion

Each identified risk must be assessed in terms of its potential impact and criticality. This assessment helps prioritize the organization's response to different risks.

Example of Risk Assessment:

Risk	Possible Impact	Criticality
Internal ransomware	Affects production and development environments	Extreme
Phishing	Leads to data leaks and unauthorized access	High
Malware	Affects individual user systems	High

Calculating the potential costs associated with each risk is also crucial for prioritizing risk mitigation efforts, as required by DORA.

Pillar 1: ICT Risk Management

B. ICT Risk Management Framework



For all identified risks, specific procedures and protocols must be developed to mitigate the impact of incidents.

Procedures:

- Define and implement procedures to limit risks and their impacts.

Example: In the case of ransomware:

- A SIEM (Security Information and Event Management system): This is a tool used to monitor and analyze security events in real-time. It helps identify and respond to potential threats quickly.
- **Monitoring of binaries:** Binaries are executable files that can run on a computer. Monitoring them means keeping an eye on these files to detect any suspicious activity that might indicate a ransomware attack.
- **Outgoing flow control:** This refers to managing and controlling the data that leaves your network. It helps ensure that sensitive data isn't being transmitted to unauthorized sources, which is crucial in preventing data breaches during a ransomware attack.

Each step contains one or several actions; they must be executed, logged, and commented on. In the case of:

We isolate the machine

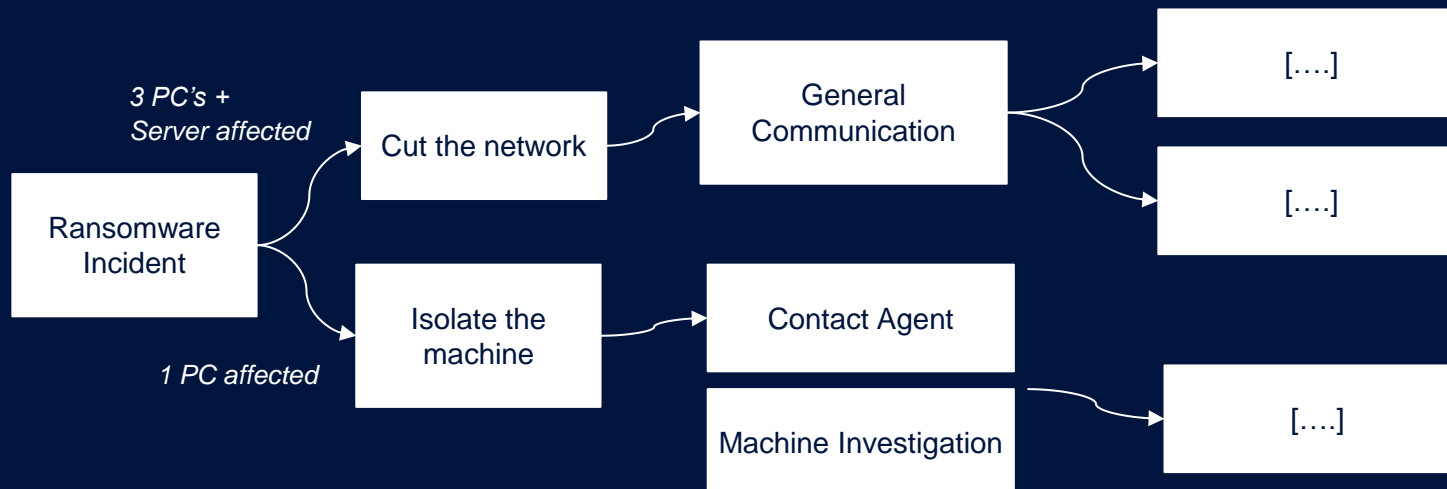
- *Execution time: 11:12*
- Comments: none
- Performed by: Alice

Agent contact

- *Start time: 11:17*
- Comments: Explain reason why incident occurred. Agent explained what happened and took time to reassure user by evaluating and providing user with tips.
- Performed by: Alice & Claire
- *Task completed: 11:29*

Protocols

Implement an incident management protocol related to the risk.



To be continued

Pillar 1: ICT Risk Management

B. ICT Risk Management Framework



Having the right set of tools is crucial for identifying, managing, and mitigating security incidents. Below are some examples and considerations for each category of tools:

List the tools in place and those necessary for incident resolution.

Examples:

SIEM Systems

- Examples include **SEKOIA, ELK Stack, Wazuh**: Tools for real-time monitoring, threat detection, and incident response.

Antivirus/Endpoint Protection

- **Windows Defender**: Built-in protection for Windows systems.
- **Third-Party Solutions**: Examples include McAfee, Symantec, or Sophos for additional security.

Remote Access Tools

- **TeamViewer, AnyDesk, RDP (Remote Desktop Protocol)**: For secure remote access to systems during an incident.

Communication Tools

- **Telephone Systems, Messaging Apps (Teams, Slack, Signal)**: For real-time communication and coordination during incidents.

Incident Management Systems

- **JIRA Service Desk, ServiceNow**: Platforms for tracking and managing incident responses.

Backup and Recovery Tools

- **Veeam, Acronis**: Essential for data backup and disaster recovery.

Monitoring and Detection

- **Nagios, Prometheus**: Tools for continuous system monitoring and early detection of issues.

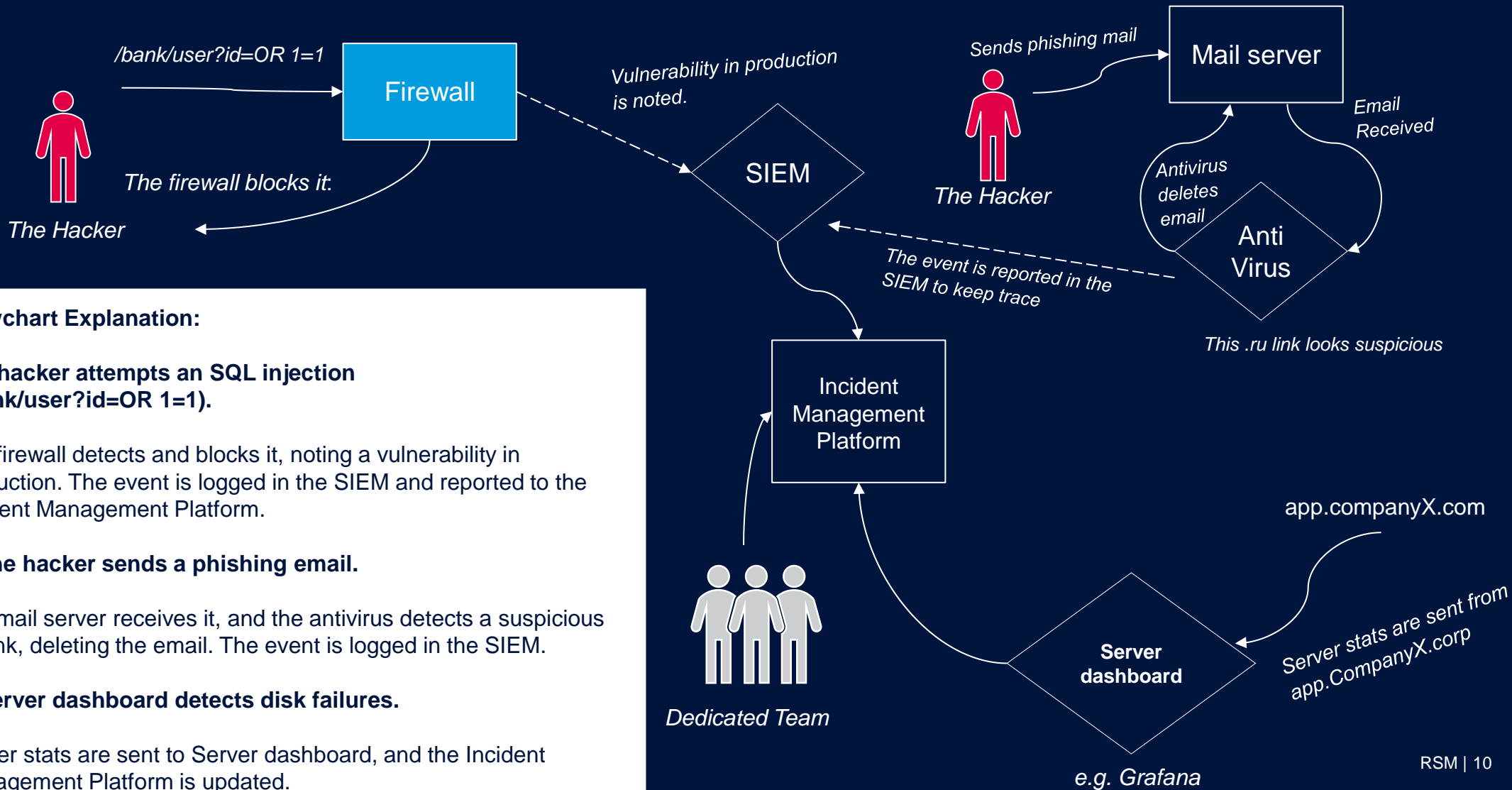
Incident Response Procedures

- **Runbooks, SOPs, Training Simulations**: Documents and tools to guide and practice effective incident response.

Pillar 1: ICT Risk Management

C. Protection and Prevention

To ensure the protection of ICT systems and prevent incidents, it's essential to implement proactive measures. While having robust incident management and procedures in place is crucial, focusing on prevention is equally important. By assessing our risks and the needs of our information systems, we can take strategic actions to enhance our security posture and minimize potential threats.



Flowchart Explanation:

1. A hacker attempts an SQL injection (`/bank/user?id=OR 1=1`).

The firewall detects and blocks it, noting a vulnerability in production. The event is logged in the SIEM and reported to the Incident Management Platform.

2. The hacker sends a phishing email.

The mail server receives it, and the antivirus detects a suspicious `.ru` link, deleting the email. The event is logged in the SIEM.

3. Server dashboard detects disk failures.

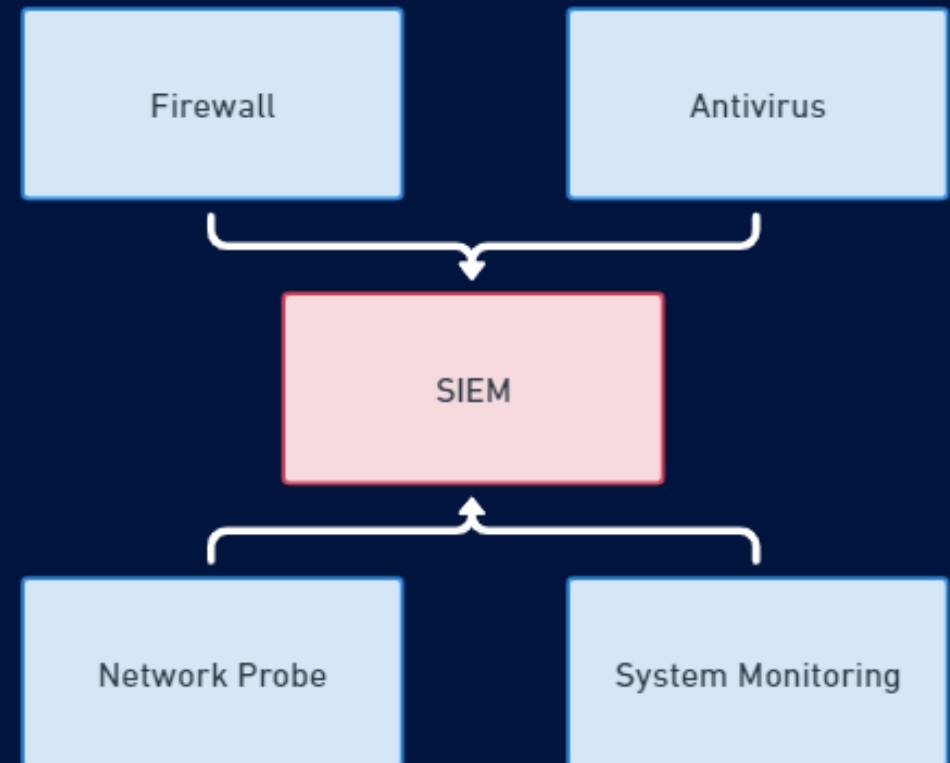
Server stats are sent to Server dashboard, and the Incident Management Platform is updated.

Pillar 1: ICT Risk Management

D. Detection

Regarding the implementation of mass threat detection mechanisms, we can highlight the implementation of the following systems:

- **SIEM**
 - Agent on user PCs
 - Agent on servers
- **Firewall**
 - Web threat detection on production
- **Antivirus**
 - Blocking of common threats
 - Basic analysis management (binary, mail, files)
- **Network Probe**
 - Detection of network anomalies
- **System Monitoring**
 - Detection of system anomalies

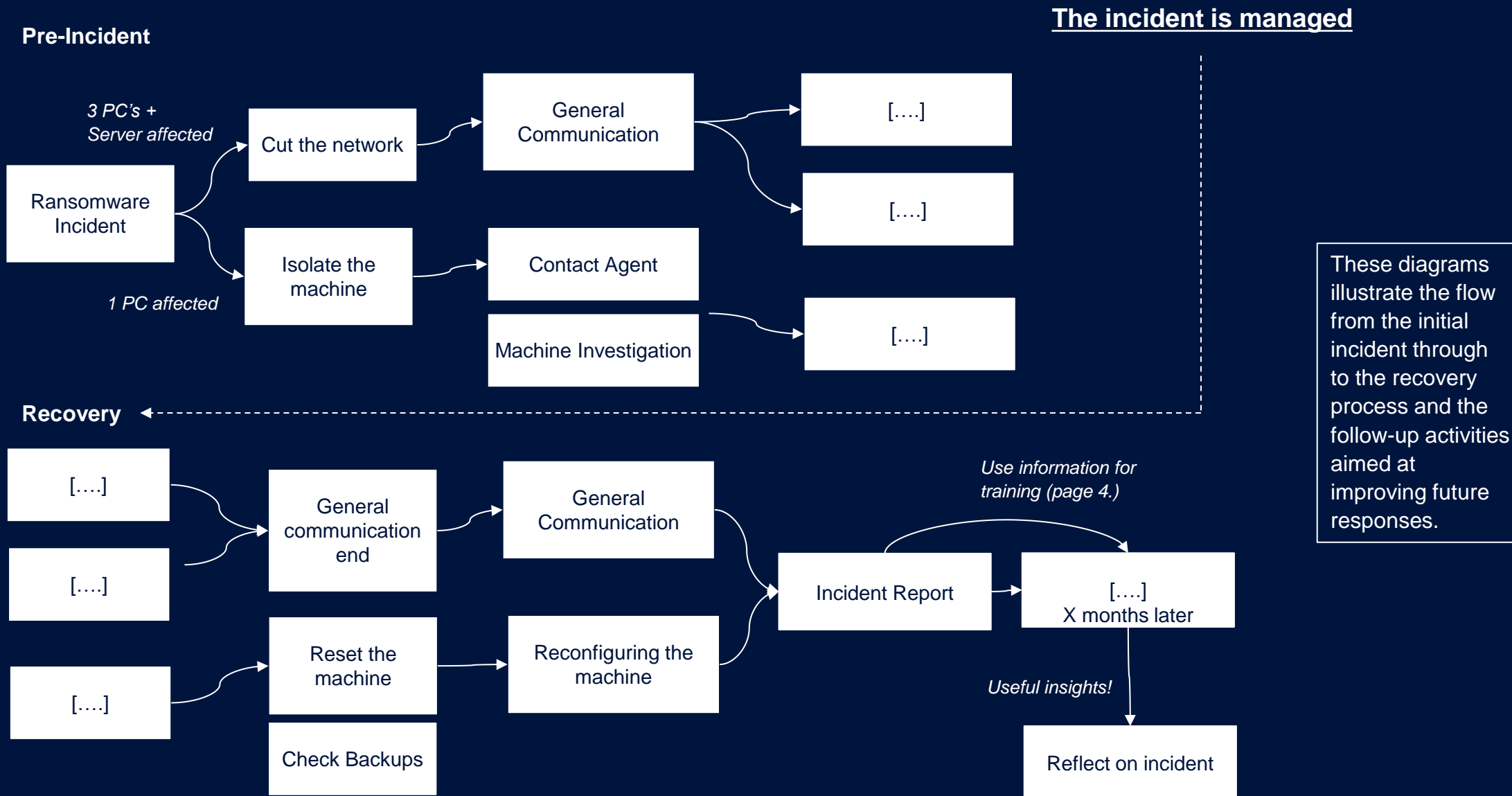


Do not forget to conduct an annual review of the implemented products to improve their characteristics with previous incident reports, aiming for continuous improvement.

Pillar 1: ICT Risk Management

E. Intervention and Recovery

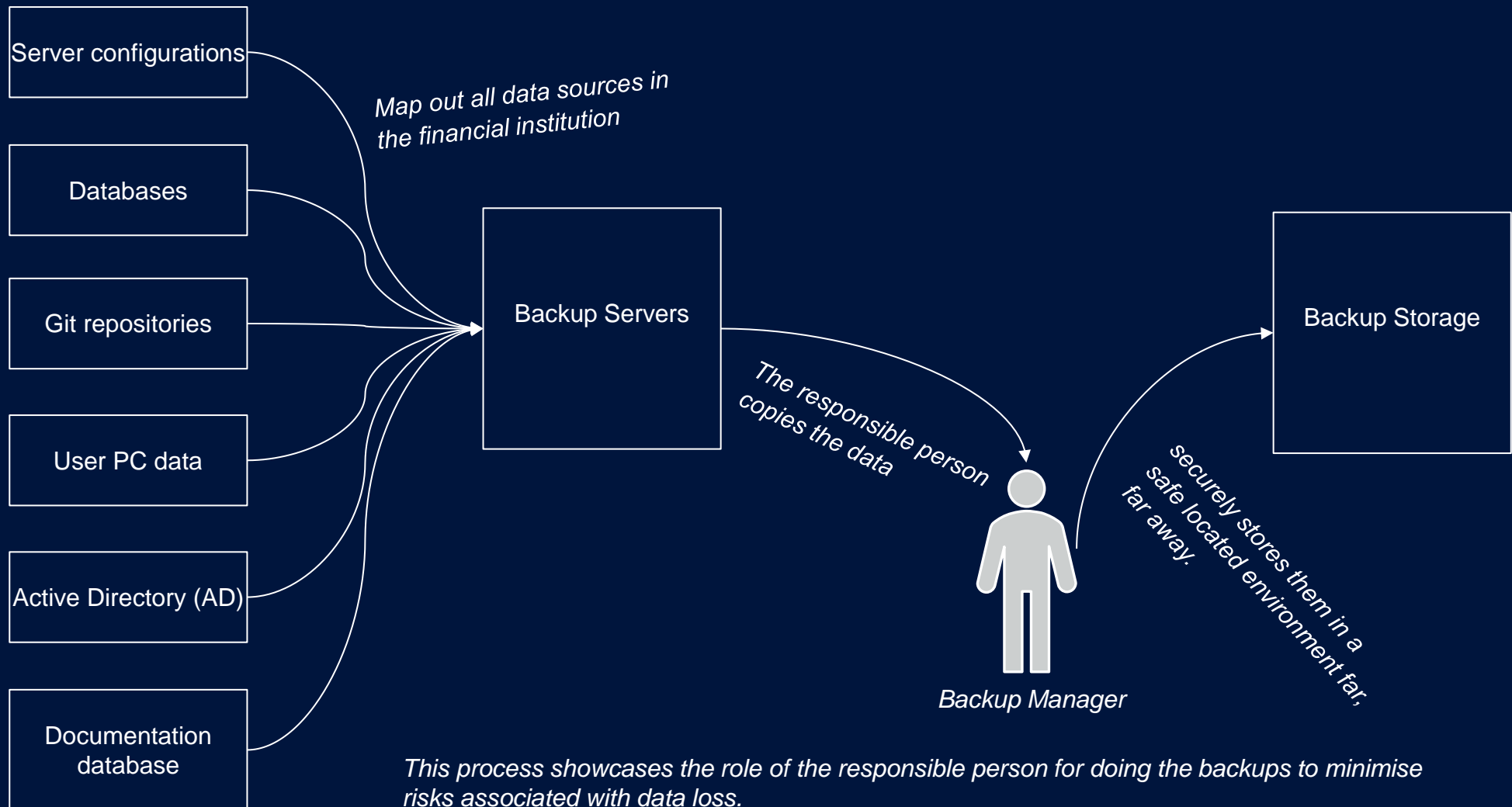
Develop and implement intervention and recovery plans following incidents, aligning with a "reverse tree" structure within the incident management protocol.



Pillar 1: ICT Risk Management

F. Backups

DORA mandates regular backups of critical data are mandated to ensure the resilience and continuity of ICT systems. The following diagram illustrates the backup process, highlighting the key data sources, the role of backup servers, and the responsibilities of the Backup Manager in ensuring secure data storage.



Pillar 2 - Incident Management

A. ICT Incident Management Framework



Building on the governance framework, organizations must develop a comprehensive incident management framework that includes detection, classification, and reporting of ICT incidents. This framework should be designed to ensure a rapid and effective response to any ICT-related incident. Regular internal training sessions should be conducted to ensure all team members are familiar with the incident management framework. These sessions should cover the latest threats, response procedures, and the use of relevant tools.

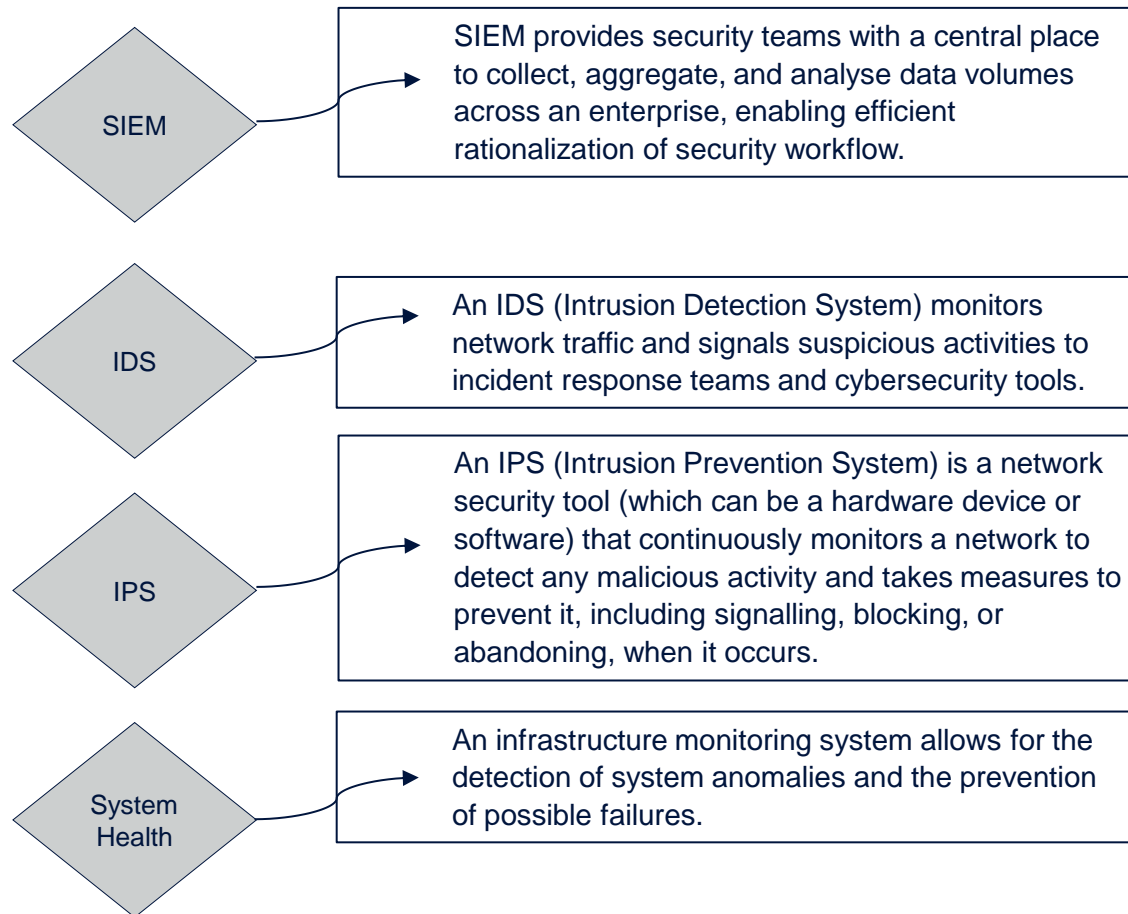
Example Training Scenario:

1. Elena (new team member) is introduced to the documentation.
2. Alice (experienced team member) explains the documentation and procedures.
3. The team conducts a malware test to ensure readiness.

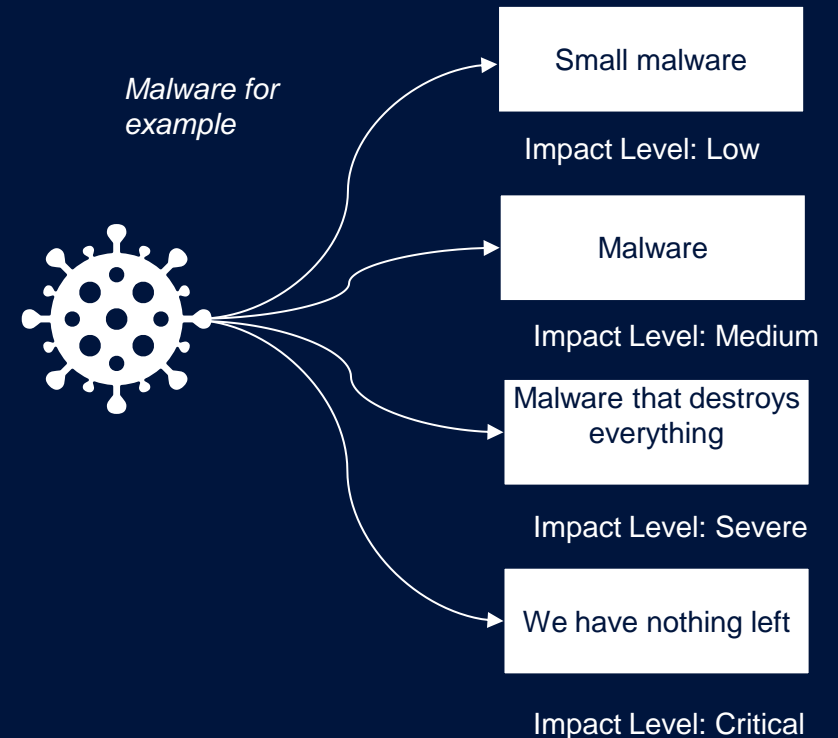
Pillar 2 - Incident Management

B. Incident Detection and Classification

Establish detection mechanisms in a timely manner and precise classification of incidents related to ICT. A small exhaustive list of tools to implement:



Then, during an incident, with data from different classification platforms and the context of the incident, it is necessary to classify it within a severity level.



Pillar 2 - Incident Management

C - Learning and Continuous Improvement



Below illustrates how an organisation can leverage information from various sources to drive continuous improvement in its incident management processes.

<i>Company X</i>	<i>Risk Team</i>	<i>Internet</i>
Cyber report	Incident feedback	Cyber trends
Objectives	Details of major incident	Current threats
Resources	Areas for improvement	New technologies

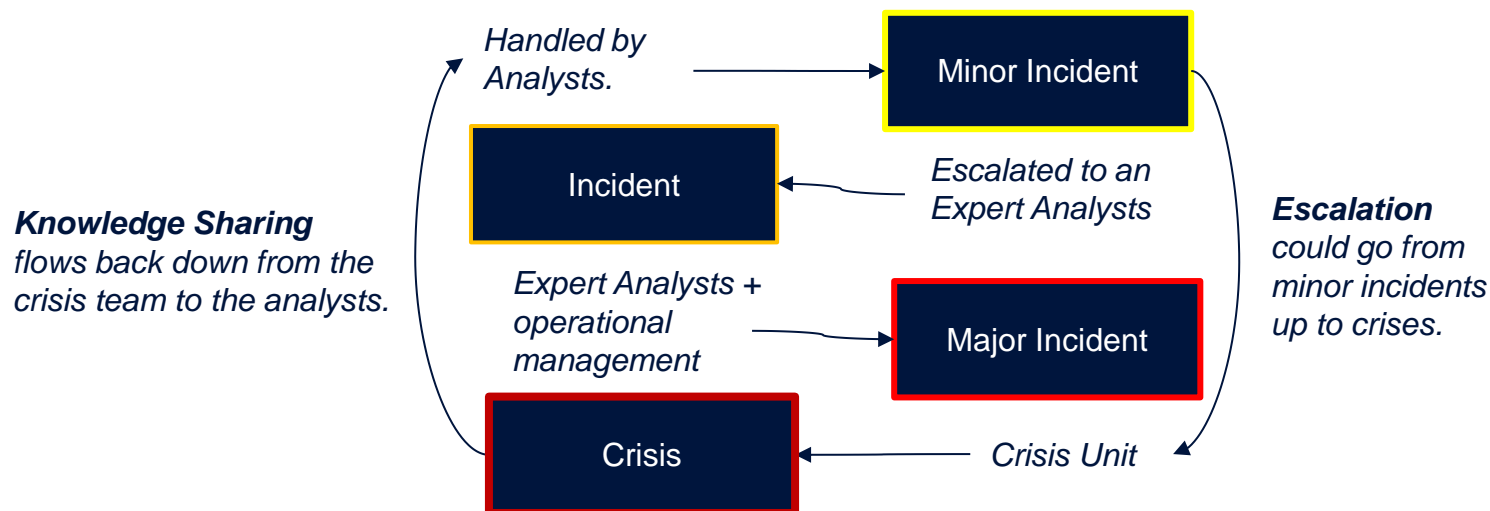


These elements lead to a 'Big Meeting'

Conclusion

- Change in procedures
- Buying a new tool
- Training on specific threat
- Changing the training scenario

D - Incident Escalation Procedure



This section details the structured process for escalating incidents within the organization to ensure they are managed at the appropriate level:

- **Process:** Minor incidents are handled by analysts. More complex issues are escalated to expert analysts and, if needed, to a crisis unit.
- **Knowledge Sharing:** Insights from incidents are shared back with the team to improve future responses.

Pillar 3: Digital Operational Resilience Testing



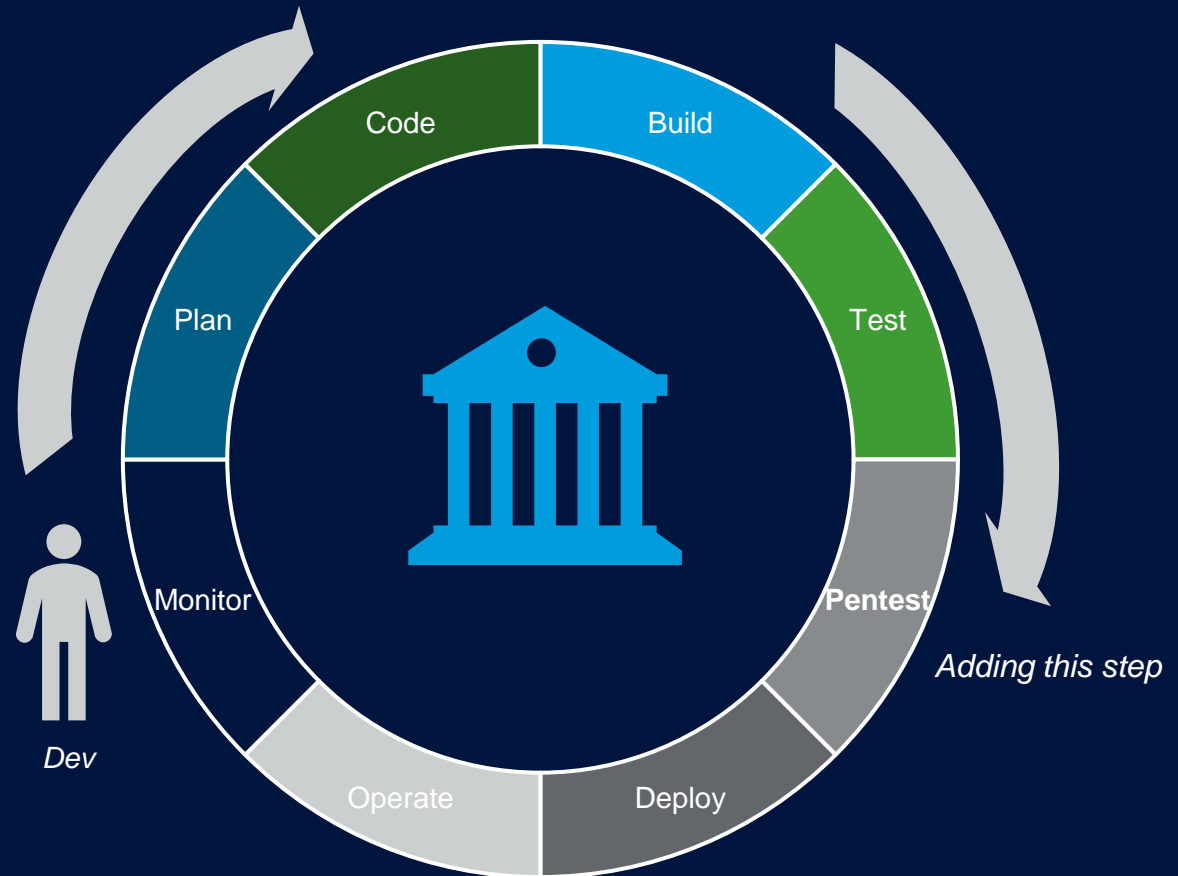
A. Testing Framework

Establish a structured framework for regularly testing digital operational resilience. For training exercises, it is beneficial to conduct simulations on an environment identical to the production system. These simulations can be further enhanced by integrating them into the CI/CD pipeline, ensuring that resilience testing is an ongoing and integral part of the development process.

CI/CD Pipeline Overview

A CI/CD pipeline automates software development, testing, and deployment to deliver code changes quickly and reliably. Here's a summary of the steps:

1. **Plan:** Define requirements and features.
2. **Code:** Developers write and commit code.
3. **Build:** Compile the code into a deployable format.
4. **Test:** Run automated tests to catch bugs.
5. **Pentest:** Conduct penetration testing to find security vulnerabilities.
6. **Deploy:** Release the application to production.
7. **Operate:** Manage the live application.
8. **Monitor:** Continuously track performance and security.



What is CI/CD?

CI (Continuous Integration): Frequently merges code changes, triggering automated builds and tests to catch issues early.

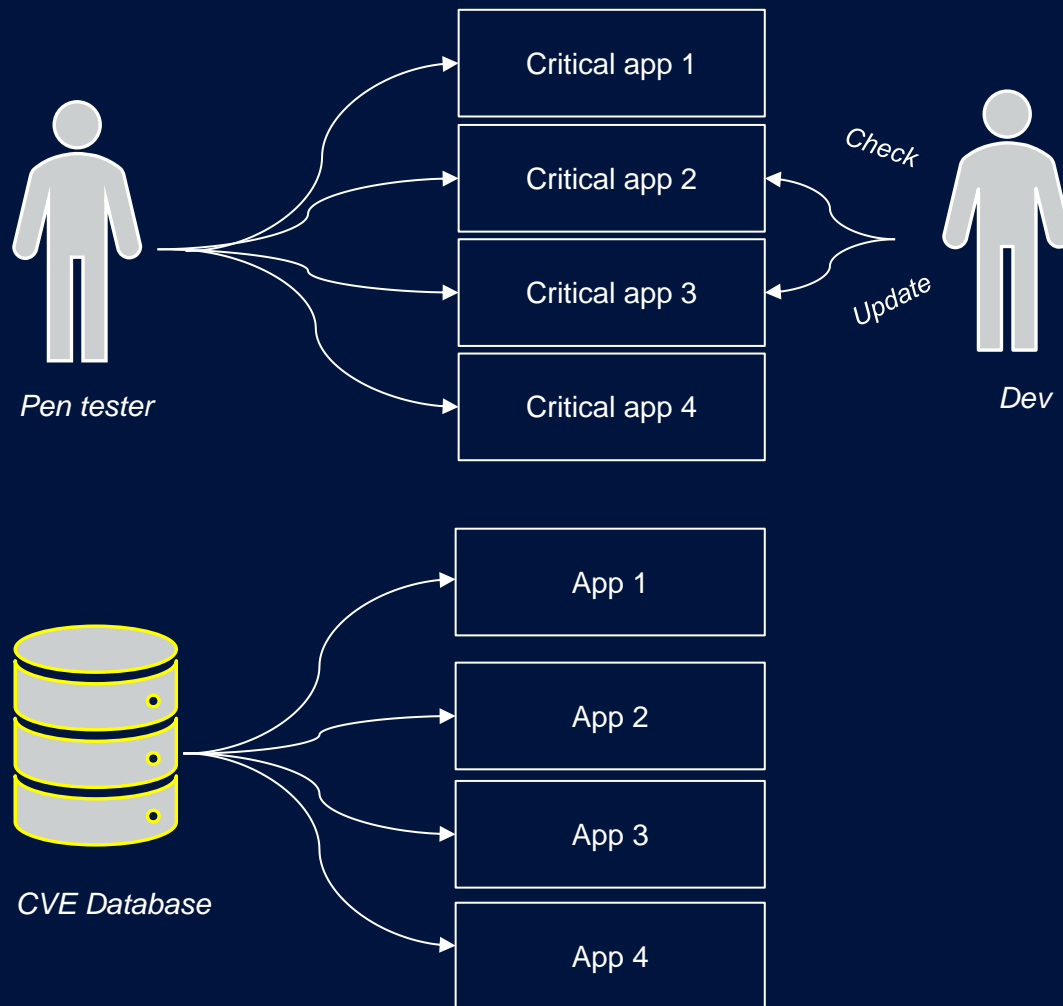
CD (Continuous Delivery/Deployment): Ensures the application is always ready for deployment. Continuous Delivery might require manual approval for deployment, while Continuous Deployment automates the entire process, pushing changes directly to production.

Incorporating a Pentest step ensures that security is continuously integrated into the development process.

Pillar 3: Digital Operational Resilience Testing

B. Vulnerability Assessments

In line with ensuring the security and resilience of ICT systems, it is crucial to regularly identify and address vulnerabilities within both the systems and processes. The attached visuals illustrate the workflow for this process.



Example Workflow:

1. Pen tester Evaluation:

- **Critical app 1:** Passes the security assessment.
- **Critical app 2:** Raises concerns that require further inspection.
- **Critical app 3:** Identified with a vulnerability that necessitates a security patch.
- **Critical app 4:** Passes the security assessment.

2. Developer Action:

- Based on the pen tester's findings, developers either check or apply necessary patches to the applications to ensure all vulnerabilities are addressed.

Additional Component: CVE Integration

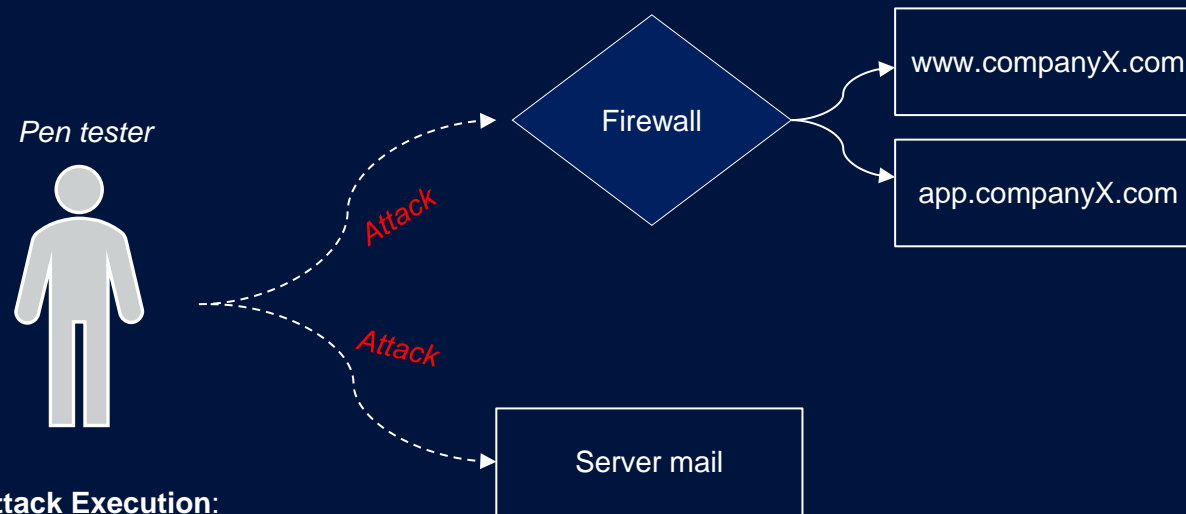
- **CVE Database:** The workflow includes regularly checking live applications against the Common Vulnerabilities and Exposures (CVE) database. This helps in identifying known security flaws within systems.
- **Application Check:** Applications (1-4) are evaluated against the CVE database to ensure they are free from classic security vulnerabilities.

This structured approach helps maintain a robust security posture, addressing both newly discovered and existing vulnerabilities effectively.

Pillar 3: Digital Operational Resilience Testing

C. Penetration Testing

The diagram provides a visual representation of the process involved in simulating real attacks to identify and correct security weaknesses within an organization's infrastructure. The attached visuals demonstrate this process.



Simulating Real Attacks Workflow:

1. Pen tester Simulation:

- Pen testers are tasked with simulating attacks on the organization's systems.

○ Targets:

- **www.companyX.com:** The primary web application of the organization.
- **app.companyX.com :** The backend or secondary application.
- **Mail Server:** The organization's email server.

2. Attack Execution:

- The pen tester launches an attack that first encounters the organization's **Firewall**. The firewall is the initial defense line, designed to filter out and block unauthorized access attempts. If the firewall fails to block the attack, it proceeds to the specific targets:
 - **www.companyX.com:** The web application is tested for vulnerabilities that could be exploited by the attacker.
 - **app.companyX.com:** Similarly, the backend application is tested for weaknesses.

3. Mail Server Attack:

- A separate attack is directed at the **Mail Server**. The purpose here is to test the mail server's resilience against potential threats, such as phishing or unauthorized access attempts.

4. Outcome and Follow-Up:

- The diagram poses questions about the subsequent steps after the attack on each target. This suggests that after identifying vulnerabilities, further actions will be necessary to remediate these weaknesses.

D - Advanced Threat-Led Penetration Testing (TLPT)

Similar to section C, but with more complex attacks.

Pillar 3: Digital Operational Resilience Testing

E. Ensure Resilience of Critical Systems



In the event of a system incident with an application or service, it could lead to a complete unavailability of the service, directly impacting operational efficiency and potentially leading to significant financial and reputational damage.

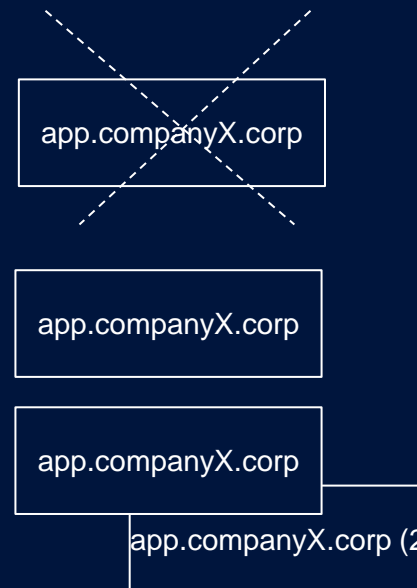


Consider the application "app.companyX.corp" as the critical system.

Should an incident compromise this service, the availability of the service could be completely disrupted.

However, with a redundant service in place, the maximum impact would likely be a reduction in capacity, while maintaining usability of the service.

Therefore, it is advisable to implement appropriate replication of the service to ensure its resilience.



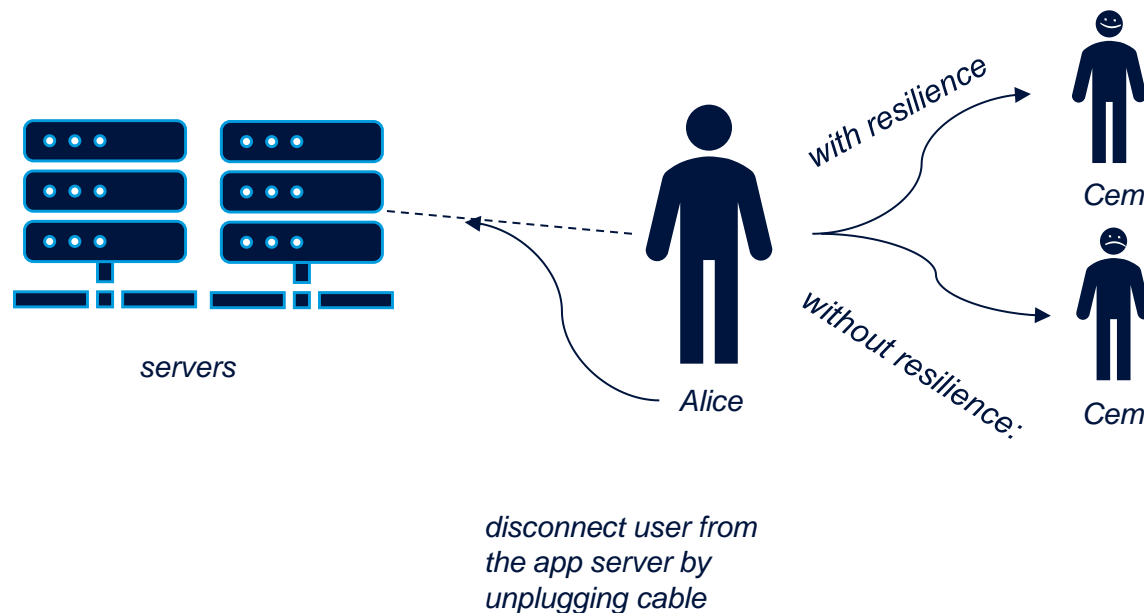
- **Without Redundancy:**
If the primary system is compromised without any redundant systems in place, the availability of the service would be entirely disrupted, leading to a complete outage.
- **With Redundancy:**
The presence of a redundant service could mitigate such disruptions, ensuring that even if the capacity is reduced, the service remains operational.

It is recommended that organizations implement strategic replication of their critical services. This involves not only duplicating key components of the IT infrastructure but also ensuring these components are effectively synchronized and can operate independently if needed. Such measures will safeguard against the potential cascading effects of system failures and enhance the organization's overall resilience.

Pillar 3: Digital Operational Resilience Testing

F. Scenario-Based Resilience Testing

The diagram illustrates the concept of scenario-based resilience testing for critical systems, specifically focusing on the effects of having or not having redundancy in place.



It might not be a good idea to test this in production, but testing on a production clone is advisable

Scenario Overview:

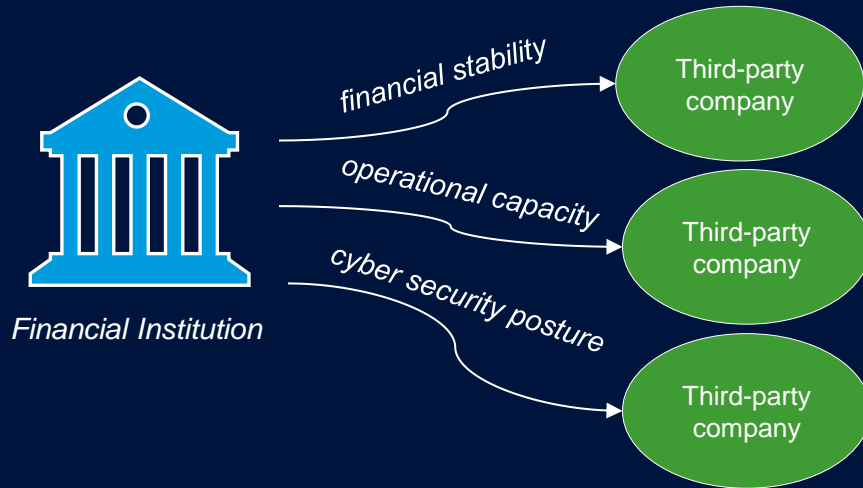
1. **Alice** is in the server room and deliberately unplugs the server cable for the application. This simulates a failure or incident scenario.
2. **Outcomes:**
 - The diagram splits into two paths, demonstrating what happens with and without resilience:
 - **Without Resilience:**
 - **Cem** on this path is shown frustrated, as indicated by the exclamation ("Why isn't it working!"). This represents a scenario where the service goes down completely due to the incident, causing a service outage.
 - **With Resilience:**
 - On the resilient path, **Cem** remains calm and unaffected, as indicated by the smile. This shows that even though the server was unplugged, the service continues to operate normally, thanks to the resilience measures in place like having failover systems in place

Failover is a backup operational mode that automatically switches to a standby database, server or network if the primary system fails, or is shut down for servicing.

Pillar 4: ICT Third Party Risk Management

B. Due Diligence & Risk Assessment

Due diligence involves thoroughly assessing third-party service providers' financial stability, operational capacity, and cybersecurity posture before and during engagement.



In ICT Third Party Risk Management, thorough due diligence is essential. The visual highlights the key areas of assessment:

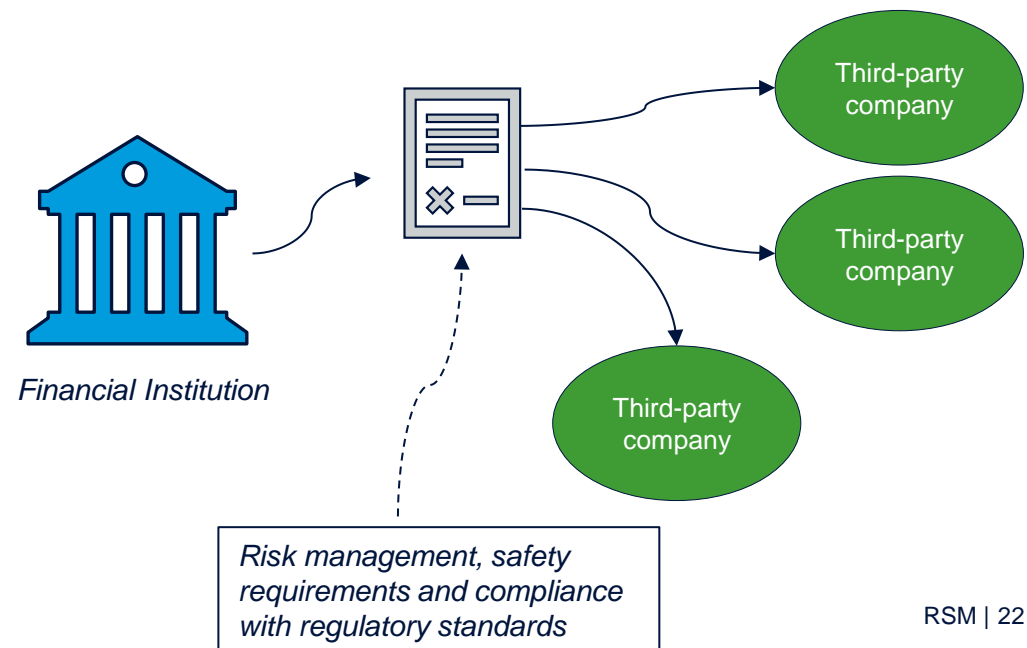
- **Financial Stability:** Ensuring third-party providers are financially sound.
- **Operational Capacity:** Verifying they can meet service demands.
- **Cybersecurity Posture:** Evaluating their security measures to protect data.

C. Contractual Arrangements

Contracts with third-party service providers must include provisions for risk management, security requirements, and compliance with regulatory standards.

In line with DORA, contracts with third-party ICT service providers must include specific clauses that address:

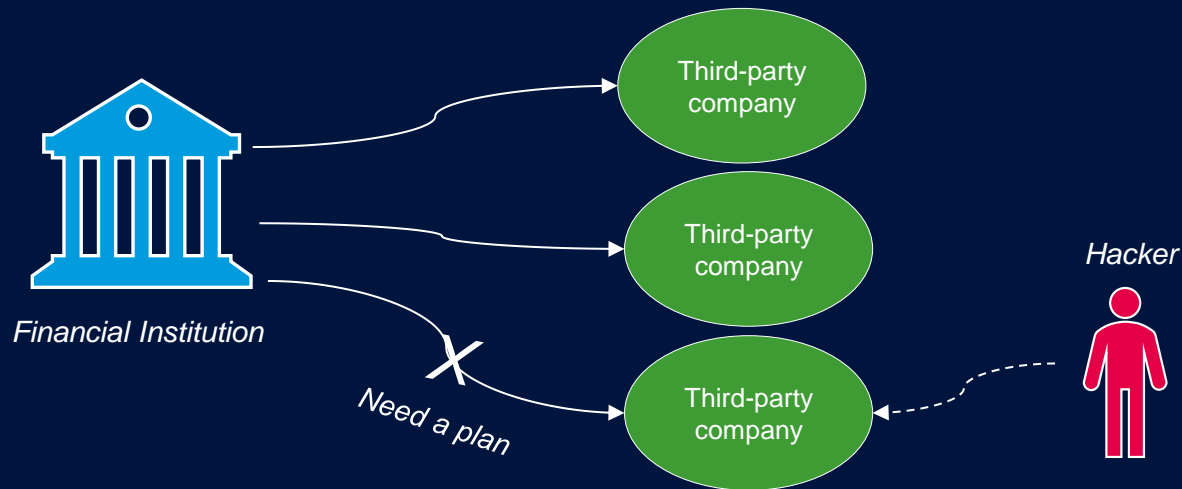
- **Risk Management:** Outlining the provider's responsibilities in identifying, managing, and mitigating risks associated with their services.
- **Security Requirements:** Detailing the security measures that must be implemented to protect the institution's data and systems.
- **Regulatory Compliance:** Ensuring that the service provider adheres to all relevant regulatory standards, particularly those mandated by DORA.



Pillar 4: ICT Third Party Risk Management

D. Business Continuity and Exit Strategies

To ensure resilience and minimize disruptions caused by third-party service providers, it is crucial to develop comprehensive business continuity plans and exit strategies.



The visual emphasizes the need for proactive planning to address potential vulnerabilities and ensure that your organization can maintain stability, even when relying on third-party services.

- **Business Continuity Plans:** These plans are necessary to maintain operations if a third-party provider fails or is compromised. They ensure that alternative measures are in place to keep critical business functions running smoothly.
- **Exit Strategies:** Exit strategies are designed to mitigate the impact of severing ties with a third-party provider. These strategies provide a clear roadmap for transitioning services away from a provider with minimal disruption, especially in the face of risks such as security breaches or provider insolvency.

5. Conclusion



01

Cybersecurity Framework:

DORA establishes a stringent framework for financial institutions, requiring robust ICT risk management, operational resilience testing, and third-party risk management to safeguard against digital disruptions.



02

Strategic Planning:

Organisations must develop and implement detailed plans for incident response, business continuity, and exit strategies to ensure seamless operations even in the face of crises.



03

Proactive Risk Management:

Continuous assessment, monitoring, and updating of risk management protocols, security measures, and contractual arrangements with third-party providers are crucial to maintaining compliance and resilience.



04

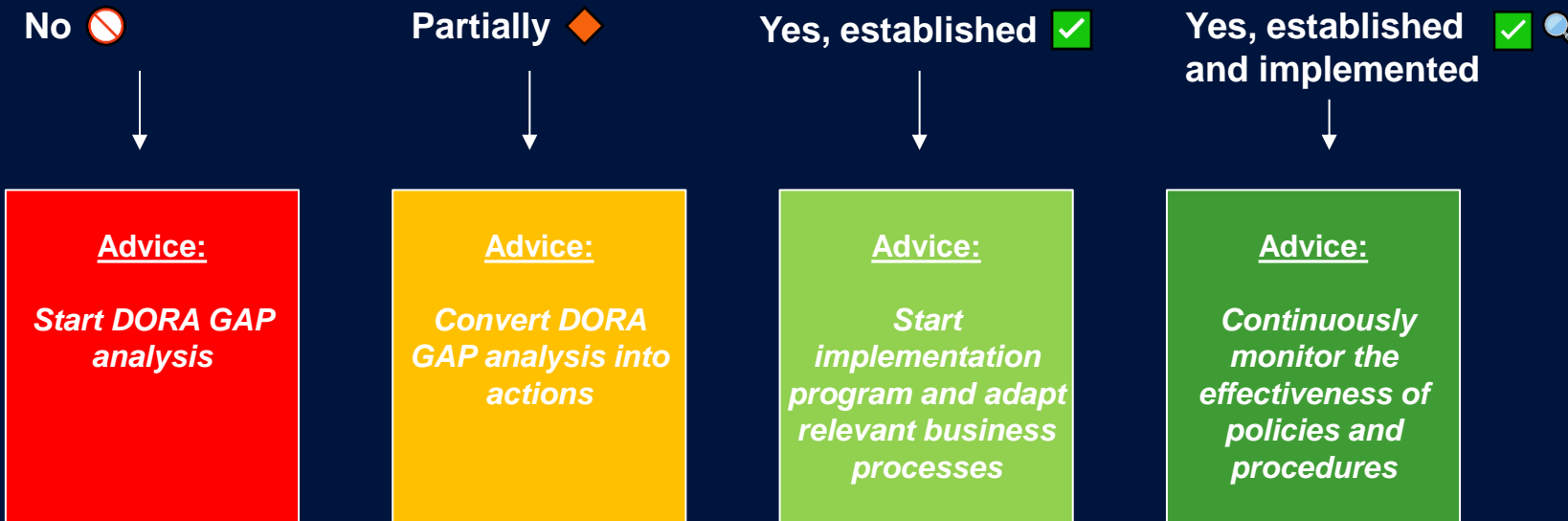
Continuous Improvement:


Regular reviews, training, and testing are essential to adapt to evolving threats, enhance resilience, and ensure that all processes and systems align with DORA's regulatory requirements.

5. Next steps 1/4

To ensure compliance with DORA, it's important for financial institutions to understand where they currently stand regarding the regulatory requirements. The following checklist provides a clear framework to help identify areas needing improvement. Financial institutions are encouraged to **conduct a GAP analysis based on the responses** to determine the necessary actions to achieve full compliance. The next pages will provide the reader with a checklist that can be answered with the options presented below. In order to help financial institutions answer the questions below, they can utilise the information presented in this report.

Possible Response Options



 **The Dutch Authority for Financial Markets (AFM) has its own perspective on DORA, which diverges from the strict text of the regulation and will prioritize the following questions. Understanding the AFM's view is crucial, as it will help understand their supervisory approach:**

Based on assessments of ICT control measures, the AFM has reviewed how financial institutions rated themselves. This has been distilled into ten key DORA themes. Organisations can use these insights, along with the following checklist to assess their preparedness for DORA.














5. Next steps 2/4

Area	Question	No	Partially	Yes, Established	Yes, Established and Implemented
Governance (Art. 5)	Has the governing body established a governance and control framework for managing ICT risks? This includes defining clear tasks and responsibilities for ICT functions, setting up an ICT risk function, budget allocation, periodic evaluations, reporting lines, and an internal ICT audit plan.	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures
ICT Risk Management (Art. 6)	Have you set up a framework for ICT risk management as part of your overall risk management system? This involves establishing a risk analysis methodology, risk register (including action plans), and periodic evaluations.	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures
ICT Asset Inventory (Art. 8)	Do you maintain an inventory of all information- and ICT-related assets, including all business processes supported by third-party ICT services? This should be documented in a register that clearly identifies whether the assets support critical processes.	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures

Additional Notes:

- See RTS 15 and Article 16(3) for further clarification regarding ICT Asset Inventory.
- See Section III of RTS 15 and Article 16(3) for more details about the specific regulatory requirements.













5. Next steps 3/4

Area	Question	No	Partially	Yes, Established	Yes, Established and Implemented
Information Security Policy (Art. 9)	Have you established an ICT security policy that ensures availability, integrity, and security of ICT systems?	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures
Business Continuity (Art. 11-12)	Have you established a business continuity plan that includes impact analyses, a communication plan, periodic testing, and an overview of events?	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures
Backup and Recovery (Art. 12)	Do you have established backup and recovery policies and procedures?	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures
Awareness and Training (Art. 13)	Have you developed training programs on ICT security and digital operational resilience?	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures

Additional Notes:

- See RTS 15 and Article 16(3) for further clarification regarding the specific areas of Information Security Policy, Backup and Recovery, and Business Continuity.

5. Next steps 4/4

Area	Question	No	Partially	Yes, Established	Yes, Established and Implemented
Incident Management (Art. 17-23)	Have you established a process for detecting and handling ICT-related incidents, including use of an incident register and support for mandatory reporting?	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures
Digital Resilience Testing Program (Art. 24-27)	Have you established a risk-based program for testing digital operational resilience, including policies and procedures for following up on findings?	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures
Third-party ICT Risk Management (Art. 28-30)	Have you established policies for managing ICT services from third-party providers that support critical or important business processes?	 Advice: Start DORA GAP analysis	 Advice: Convert DORA GAP analysis into actions	 Advice: Start implementation program and adapt relevant business processes	 Advice: Continuously monitor the effectiveness of policies and procedures

Additional Notes:

- See RTS 18(3), RTS 20(a) and ITS 20(b) for further details on Incident Management.
- See RTS 26(11) for more information on Digital Resilience Testing.
- See RTS 28(1), RTS 30(5) and ITS 28(9) for additional insights into Third-party ICT Risk Management.

*This checklist is designed to facilitate a self-assessment process for financial institutions to evaluate their readiness and compliance with DORA. By identifying gaps early, organizations can set clear priorities for implementing necessary changes and enhancements in their ICT risk management strategies. Financial institutions should update their GAP analysis periodically as they progress towards full compliance to ensure continuous improvement and readiness by the **January 17, 2025, deadline.***

Want to know more about the possible impact for your company?
Please do not hesitate to contact us



Mario van den Broek
Strategy consultant
Mvdbroek@rsmnl.nl



Herman Annink
Strategy consultant
Hannink@rsmnl.nl



Mourad Seghir
Strategy consultant
Mseghir@rsmnl.nl

Please let us know what you think



 *For our Dutch readers, we have also recorded a podcast regarding DORA:*

Podcastaflevering

**DORA: Een Praktische Gids voor de Grootste Uitdaging
voor Financiële Instellingen sinds de 2008 Hervormingen**

 RSM Pulse

RSM Netherlands Business Consulting Services B.V.

Mercuriusplein 9
2132 HA Hoofddorp
Nederland
+31 23 5300 400
www.rsmnl.com

Our firm is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm, each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.