E-BOOK

Meeting the requirements of DORA with NetApp

EU Digital Operational Resilience Act

NetApp

Contents

What is DORA?

The Digital Operational Resilience Act (DORA), which will come into enforcement in 2025, is a regulatory act that addresses the significant concerns of cyber resilience in the financial sector and critical third-party ICT service providers (cloud).

DORA provides specific guidance to mitigate the risk of cloud concentration inherent in the finance sector.

DORA can be broken down into five key areas: ICT risk management, digital operational resilience testing, third- party ICT (cloud) risk management, incident reporting, and information sharing. DORA brings all existing legislation under one harmonizing act and provides specific technical guidance.

DORA (English) | DORA (French) | DORA (Spanish)

DORA (German) | Learn more

Who does DORA apply to?

DORA applies to finance entities operating in the European Union. With other countries releasing similar legislation, DORA will have far reaching implications for all financial entities and cloud providers. Specifically, DORA applies to:

- Banks
- Credit institutions
- Investment firms
- Trading venues and repositories
- ICT third-party service providers (cloud)
- And more

"To ensure consistency around the ICT risk management requirements applicable to the financial sector, the regulation covers a range of financial entities regulated at Union level, namely credit institutions, payment institutions, electronic money institutions, investment firms, crypto-asset service providers, central securities depositories, central counterparties, trading venues, trade repositories, managers of alternative investment funds and management…"

DORA, Article 2: Scope

More about DORA

What are the consequences of noncompliance?

DORA will be enforced with significant financial penalties if organizations are found to be noncompliant. The amounts will be calculated and can be **1% of the average daily worldwide turnover.**

What are the requirements of DORA?

DORA is broken into detailed Articles that logically provide detailed guidance on subjects and requirements that are critical to cyber resilience. **This document covers how NetApp can help you meet these requirements.**

Article 25

General principles

Article 25 is a key Article within DORA that has gained the most attention. Article 25 focuses on third-party ICT providers (cloud providers) and the risks posed to financial entities by overconsolidation and reliance on single providers.

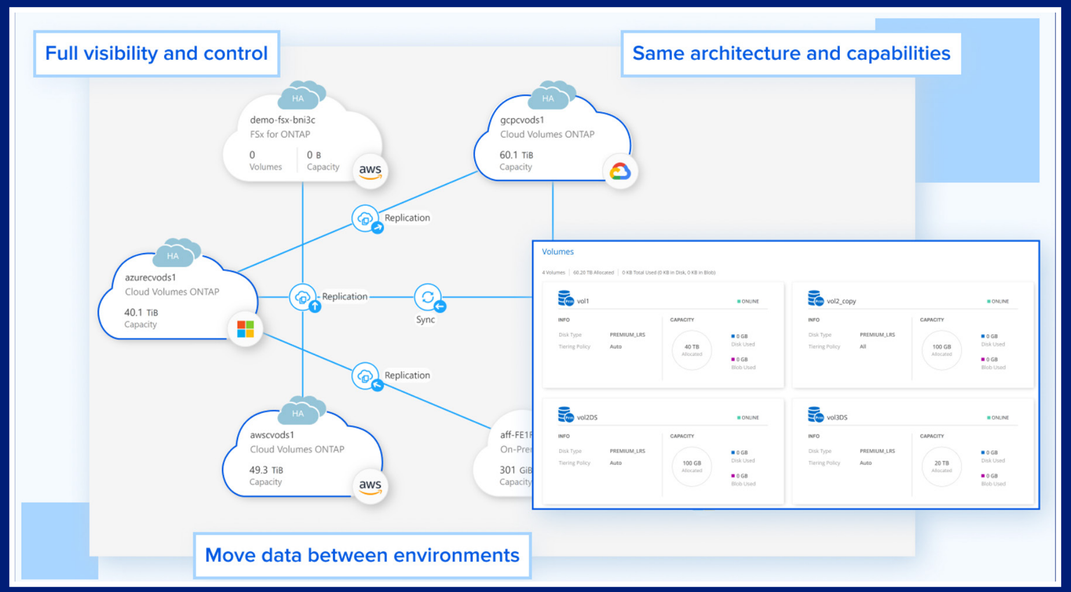
This Article provides guidance and a set of rules to reduce this risk, including adopting a multicloud strategy and planning data repatriation.

NetApp is the only provider with a comprehensive set of tools and a single management pane to meet these demands.

Cloud Volumes

NetApp® Cloud Volumes enables you to meet the requirements of DORA with the ability to create, replicate, back up, scan, classify, and tier data in any cloud. NetApp also meets the DORA requirement of being able to reincorporate workloads back in house in the event of a cloud failure. All workloads are visible and controlled from a single console, with the ability to enforce your data security requirements with additional cyber-resilience tools, as required by DORA.

Learn more



“Entities shall put in place exit strategies (from the Cloud) in order to take into account risks that may emerge at the level of ICT third-party service provider, in particular a possible failure…

Entities shall identify alternative solutions and develop transition plans enabling them to remove the contracted functions and the relevant data from the ICT third-party service provider (Cloud) and securely and integrally transfer them to alternative providers or reincorporate them in house.”

- DORA, Article 25: General principles

Article 8

Protection and prevention

Article 8, which forms the basis of protection and critically, prevention, discusses the use of the latest tools and standards to make sure that your data is protected, in transit and at rest. It also includes requirements for preventing data from being corrupted by unauthorized access, leakage, and poor administration.

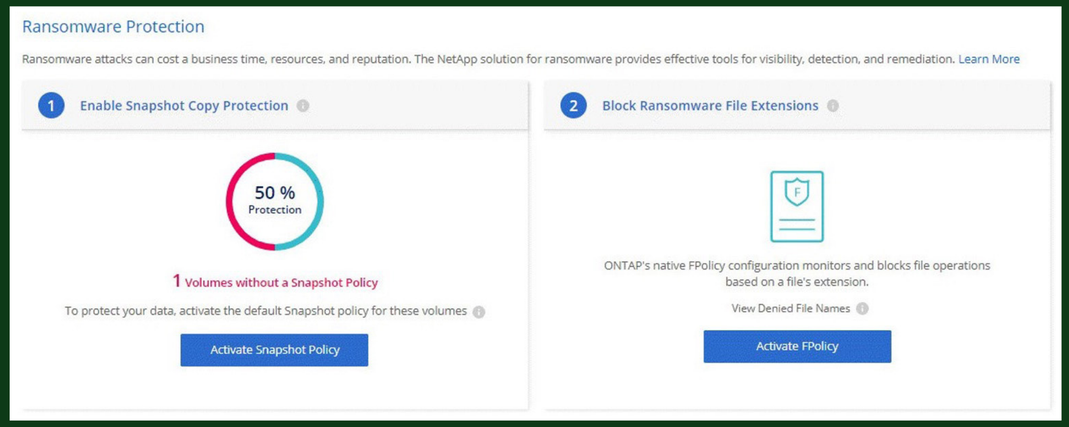
NetApp® powerful tools and solutions such as NetApp Cloud Data Sense and ransomware address these challenges.

Analyze file access permissions

Understanding your data is the beginning of protection and prevention. Our governance capabilities include constant insights into your first level of defense: file and folder level permissions. With **NetApp® Cloud Data Sense** permissions analysis, enhanced filtering capabilities, and auditing, you can tighten your security and make sure that the right people get access to the right data, at the right level.

Malicious file blocking

Based on access permissions set across your data estate, data gets created only where it's allowed, and that includes files encrypted by ransomware during an attack. With **NetApp ONTAP®** file access notification framework **(Fpolicy)**, you can block file creation and other operations based on known ransomware file extensions. This policy can be implemented even if an attacking user or computer instance has write permissions to folders.



"Minimise the risk of corruption or loss of data, unauthorized access…

Prevent information leakage… Develop and document an

information security policy defining rules to protect the confidentiality, integrity, and availability of theirs, and their customers' ICT resources, data and information assets."

- DORA, Article 8: Protection and prevention

Article 8

Active Directory monitoring

Your Active Directory retains a lot of information and is responsible for many functionalities of your domain assets, including resource allocation, authentication, authorization, and more. Therefore, it's a "holy grail" for infiltrators who can use it to gain access, escalate privileges, and collect information on your network. It's important to constantly monitor your Active Directory with tools like **NetApp® Cloud Data Sense** to find anomalous activities or unnecessary privilege allocations and to remove possible security gaps.

Multi-admin verification overview

You can use multi-admin verification to make sure that certain operations, such as deleting volumes or NetApp Snapshot™ copies, can be executed only after approval from designated administrators. This verification prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data.

End-to-end encryption

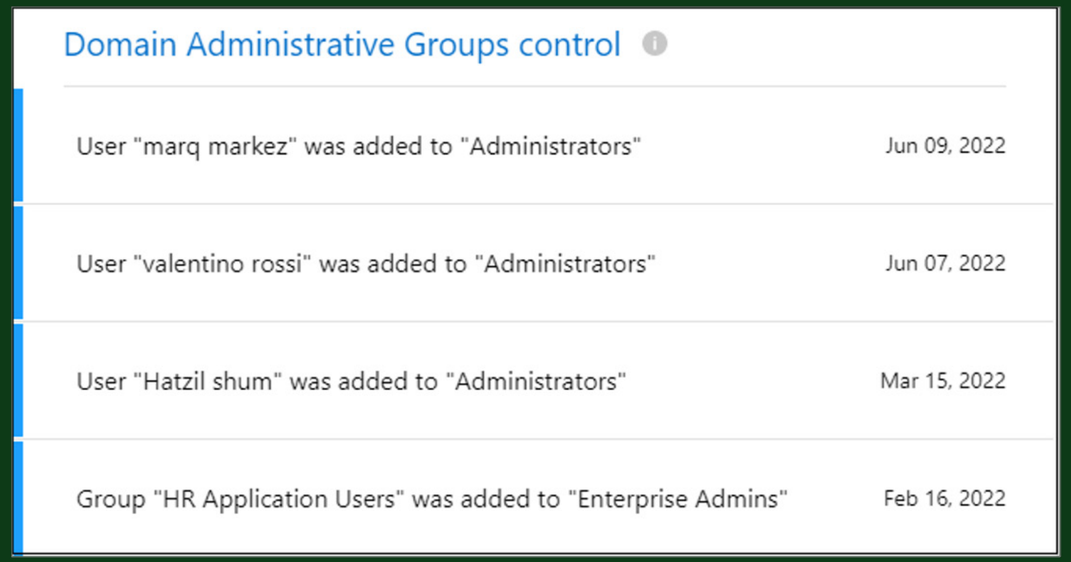
NetApp meets all of DORA's backup requirements by providing end-to-end with AES 256-bit encryption at rest, TLS/HTTPS encryption in flight, and customer-managed key (CMK).

Learn more

"Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated controls systems to prevent access.

Guarantee the security of the means of transfer of information."

- DORA, Article 8: Protection and prevention



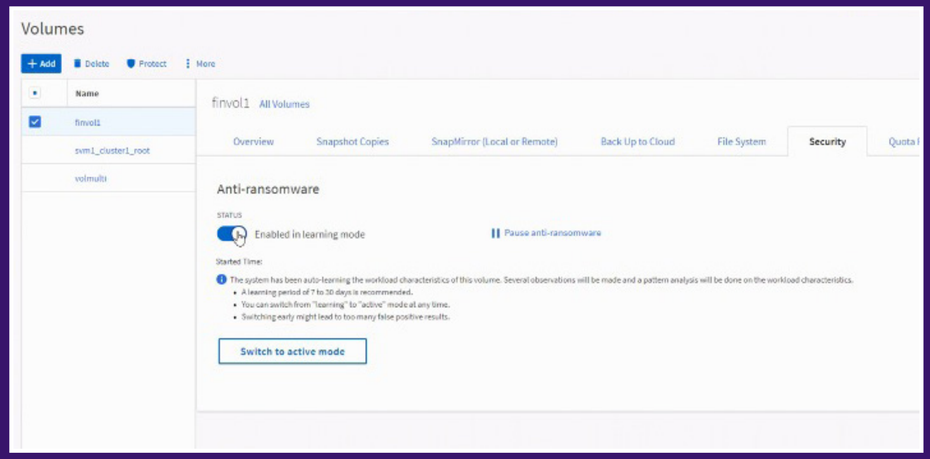
Article 9

Detection

Article 9 lays out requirements for having mechanisms in place to detect anomalous activities and regularly test them. These mechanisms are required to have multiple layers of control, including alerting and automated incident response. Entities are required to dedicate the appropriate amount of resources to monitoring for their size.

Storage anomaly detection

Using machine learning capabilities, **NetApp® ONTAP®** is able to identify and prevent or limit sophisticated ransomware attacks by continuously analyzing workloads (available in **ONTAP 9.10.1** and later). This antiransomware feature uses workload analysis in NAS (NFS and SMB) environments to proactively detect and warn about abnormal activity that could point to a ransomware attack. When the system detects an attack, antiransomware creates a new **NetApp Snapshot™** copy in addition to the ongoing protection from scheduled Snapshot copies.



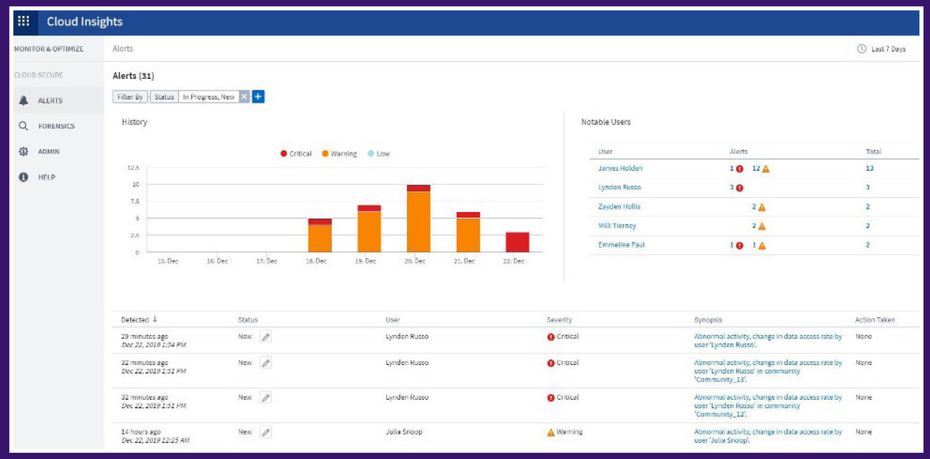
"The detection mechanisms … shall enable multiple layers of control, define alert thresholds and criteria to trigger ICT-related incident detection and ICT-related incident response processes, and shall put in place automatic alert mechanisms for relevant staff in charge of ICT-related incident response."

- DORA, Article 9: Detection

Article 9

User anomaly detection

Ongoing user behavior analytics (UBA) is required to identify and prevent or limit sophisticated ransomware attacks. **NetApp® UBA** capability tracks the behavior of individual users and communities to identify typical data access patterns. It then reports when behavior differs from the normal observed pattern. In such cases, UBA can proactively respond by denying access to files and folders where suspicious activity is taking place and take further action to protect your data by using the feature **Cloud Secure**, within **Cloud Insights** and **FPolicy** external mode.



“Financial entities shall have in place mechanisms to promptly detect anomalous activities. All detection mechanisms … shall be regularly tested. Financial entities shall devote sufficient resources and capabilities, with due consideration to their size, business and risk profiles, to monitor user activity, occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.”

- DORA, Article 9: Detection

Learn more

Article 10

Response and recovery

Article 10 covers details about response and recovery, including dedicated and comprehensive ICT business continuity plans. Plans should include recording all incidents, ensuring continuity of critical financial functions, quick and appropriate responses to cyberthreats, containment measures, and communication plan. There are requirements for redundancies and switch-overs from primary to secondary.

With a history of industry-leading response and recovery solutions, NetApp is well-positioned to meet all the requirements of DORA.

Immutable data copies

Data stored in **NetApp® ONTAP®** systems is protected by **NetApp Snapshot™** copies, which are point-in-time, read-only images of your data that show exactly what your data looked like at the moment the copy was made. Because Snapshot images are read-only, captured data can't be encrypted and locked by ransomware. With the **NetApp FlexClone®** and **SnapRestore®** technologies, you can restore an entire volume or individual files from a Snapshot copy in the event of a ransomware attack, significantly faster than with any other recovery method.

Professional Services

With their extensive experience, NetApp Professional Services can help develop business continuity plans for your critical workloads and create clear communication paths if a crisis arises. NetApp Professional Services can advise you on all technical aspects of DORA requirements and provide templates for best practises.

Learn more

"…containment measures, processes and technologies suited to each type of ICT-related incident and preventing further damage, as well as tailored response and recovery.

As part of the ICT risk management framework … entities shall put in place a dedicated and comprehensive ICT Business Continuity Policy as an integral part of the operational business continuity policy of the financial entity.

Entities … shall have a crisis management function, which, in case of activation of their ICT Business Continuity Policy or ICT Disaster Recovery Plan, shall set out clear procedures to manage internal and external crisis communications."

- DORA, Article 10: Detection

Article 11

Backup policies and recovery methods

Article 11 is one of the most detailed and prescriptive Articles. It covers requirements for backup methods, including specifying scope and frequency based on data criticality. DORA also requires dedicated clean rooms where data can be restored to avoid reinfection.

NetApp® backup and recovery technologies cover these requirements, leaving no area of compromise.

Air gap copies

Air gapping backups can prevent bad actors and ransomware from accessing your insurance policy. Unlike traditional methods that create a physical separation between primary and secondary data media, **NetApp® SnapLock® Compliance** software takes capability to a new level by logically air gapping your data without any need for physical separation. SnapLock prevents your production data and **Snapshot™** copies from being tampered with, resulting in a logical air gap of your data that is quickly accessible, safe from deletion, and immutable.

MetroCluster

NetApp MetroCluster configurations combine array-based clustering with synchronous replication to deliver continuous availability, immediately duplicating all of your mission-critical data on a transaction-by-transaction basis.

Tamper Proof Snaps

Use the SnapLock compliance clock feature to lock Snapshot copies for a specified period so that they cannot be deleted until the expiration time is reached. Locking Snapshot copies makes them tamperproof, protecting them from ransomware threats. You can use locked Snapshot copies to quickly recover data if a volume is compromised by a ransomware attack.

Learn more

“When restoring backup data using own systems, financial entities shall use ICT systems that have an operating environment different from the main one, that is not directly connected with the latter and that is securely protected from any unauthorized access or ICT corruption.

…recovery plans shall enable the recovery of all transactions at the time of disruption.”

- DORA, Article 11: Backup policies and recovery methods

Article 4

Governance and Organsation
Article 4 firmly places responsibility for ICT risk with the overall management of the organisation (C-Suite).

Technology plays a key part in the solution but overall, this becomes a business decision on how much risk are organisations will accept.

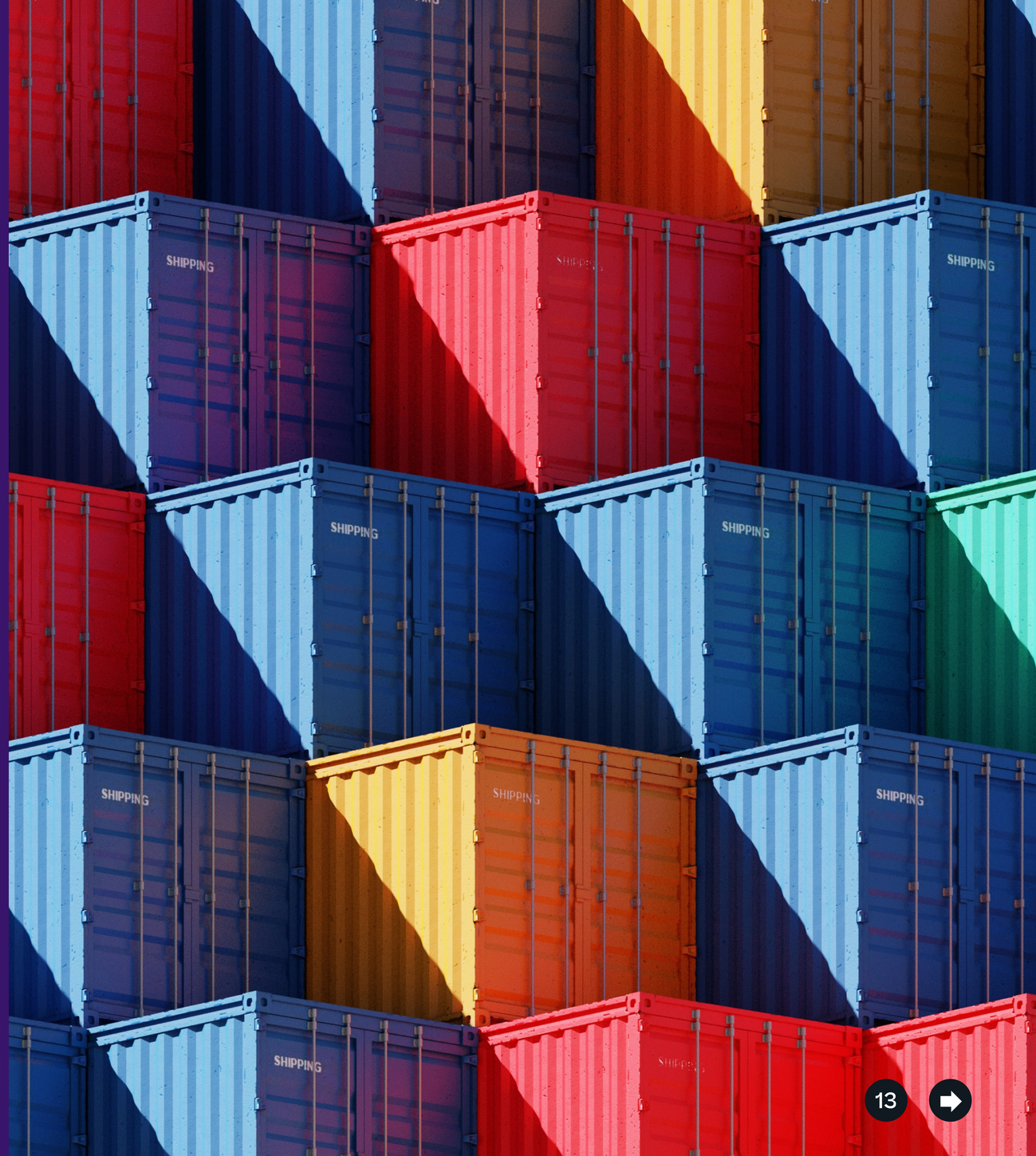
Furth more, the management suit or board must be trained in the risks of ICT risk and threats on an annual business to enable these decisions to made.

"The management body of the financial entity shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework.

- **Bear the final responsibility for managing the financial entity's ICT risks**
- **Determine the appropriate risk tolerance**
- **Allocate and periodically review appropriate budget**

Members of the management body shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity."

- DORA, Article 4: Governance and Organisation



Still unsure about where to begin?

NetApp Professional Services

Meeting DORA requirements can be complex and daunting. Begin the journey with NetApp's professional services tailored to your DORA requirements.

Learn more

NetApp Ransomware Protection and Recovery Service

NetApp® Ransomware Protection and Recovery service can assess your environment in the context of DORA and meet the demanding DORA requirements and provide ongoing protection.

Learn more

NetApp Data Protection & Security Assessment

The DPSA identifies gaps in your current data protection strategy and delivers an actionable, proactive plan to minimize potential risks by:

- Uncovering risk exposure and security vulnerabilities in ONTAP and Cloud Volumes ONTAP environments
- Providing a detailed gap analysis and actionable recommendations for your data protection strategy and policies

Learn more

About NetApp

Learn more at www.netapp.com

Steve Rackham
CTO for Financial Services
Email

Peter Dean
Vertical Lead, Financial Services Industry
Worldwide Industry Solutions
Email

Adam Gale
Business Cloud Architect - NetApp
Email

About NetApp
NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data services, and CloudOps solutions to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, harnessing observability and AI to enable the industry's best data management. As the only enterprise-grade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility. In addition, our data services create a data advantage through superior cyber resilience, governance, and application agility. Our CloudOps solutions provide continuous optimization of performance and efficiency through observability and AI. No matter the data type, workload, or environment, with NetApp you can transform your data infrastructure to realize your business possibilities.

NetApp

+1 877 263 8277