

Explore DORA

The impact of cloud for financial services and regulations

Adam Gale – Enterprise Architect
Steve Rackham - CTO for Financial Services



Agenda

Exploring the Digital Operational
Resilience Act (DORA)

Legislation and regulation

What is DORA?

Who does DORA apply to?

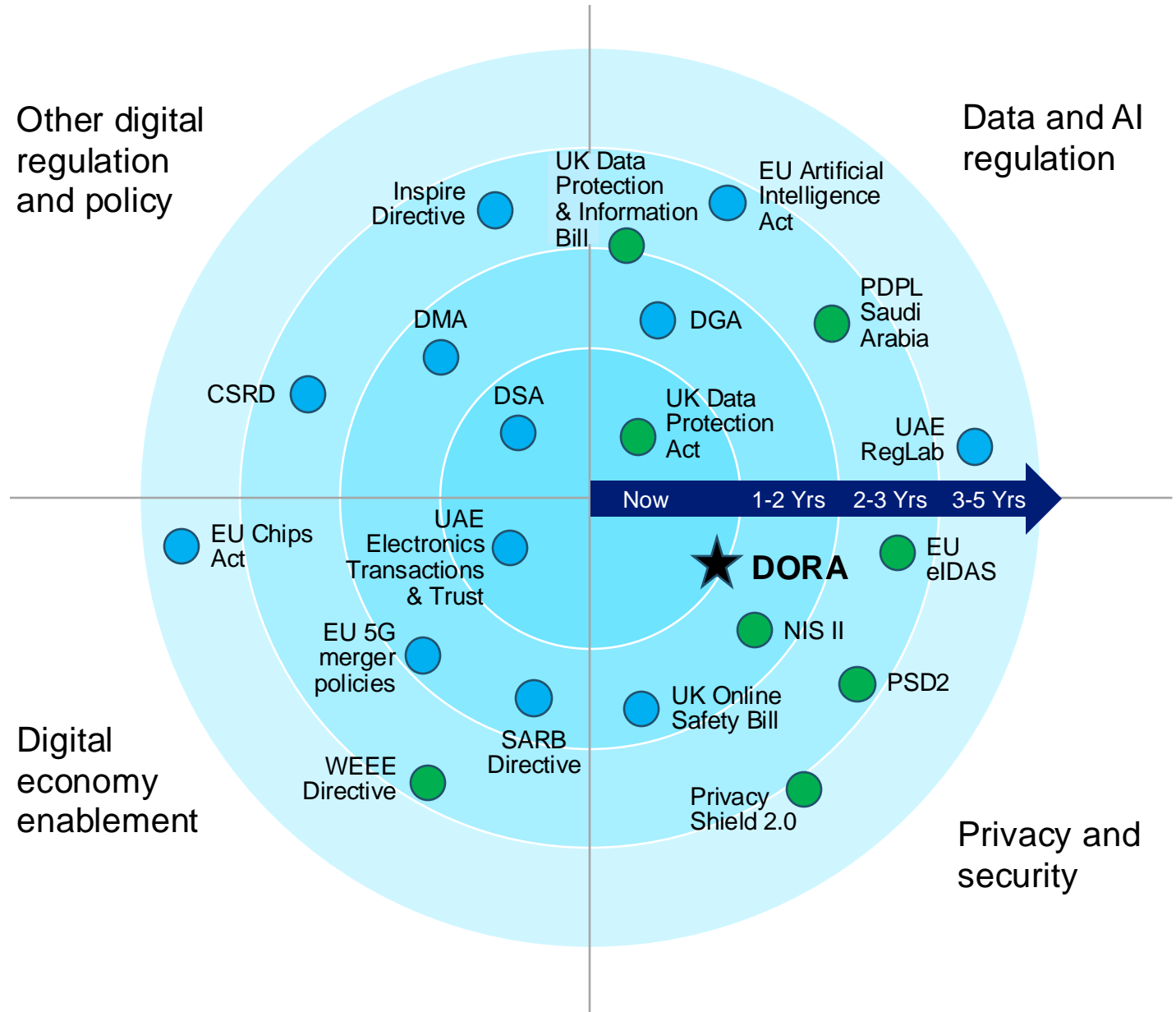
What are the objectives of DORA?

Prepare for DORA

LEGISLATION AND REGULATION

Regulation and policy

The wider context



WHAT IS DORA?

“DORA IS AN ATTEMPT
TO HARMONIZE AND
BOLSTER SECURITY
ACROSS THE
EU FINANCE SECTOR.”

EBA | EUROPEAN
BANKING
AUTHORITY



WHO DOES DORA APPLY TO?

Who does DORA apply to?

Financial entities operating in the EU

Financial entities

Banks, credit institutions, investment firms, trading venues, payment institutions, crypto-asset service providers and repositories.

ICT third-party service providers

“ICT third-party service provider” means an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, data centres” - DORA

Banks

Credit institutions

Investment firms

Trading venues

Crypto-asset service providers

Payment institutions

Cloud

Alternative investment funds

Central counterparties

Insurance companies

Third party ICT

Electronic money institutions

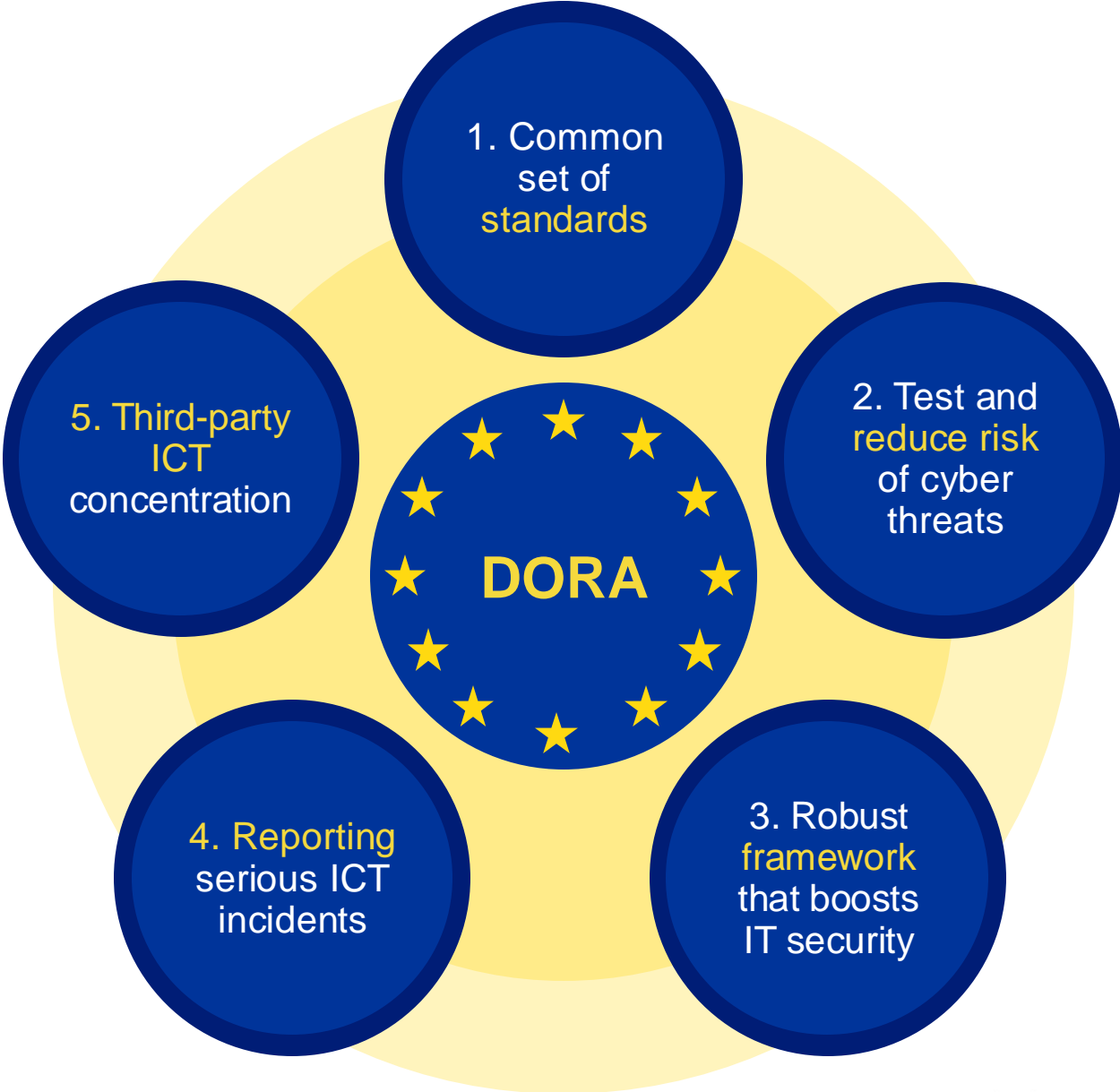
WHAT ARE THE MAIN OBJECTIVES OF DORA?

Key goals for DORA regulation

Strengthening the financial sector's resilience	Strengthen third- party ICT providers	Establishing robust measures and controls on systems	Provide detailed guidance	Provide guidance on critical ICT providers
<p>The EU's aim with DORA is that of strengthening the financial sector's resilience to ICT-related incidents and introduces very specific and prescriptive requirements that are homogenous across EU member states.</p>	<p>Critical ICT third-parties which provide ICT-related services to financial institutions, such as cloud platforms, data analytics and audit services, are also subject to this new regulation.</p>	<p>Establishing robust measures and controls on systems, tools and third parties, by having the right operational continuity plans in place, while testing their effectiveness continually</p>	<p>This act provides a very specific set of criteria, templates and instructions that will shape how financial organisations manage ICT and cyber risks.</p>	<p>Suppliers will be published by the JCEI. Considerations will be made as to systemic impact and importance. The degree of reliance on one provider for important functions (concentration of services provided).</p>

FUNDAMENTALS OF DORA

Five main pillars of DORA



Five main pillars of DORA

1. Common set of standards

- **Collaborate** with other financial entities
- **Minimize** ICT threats' ability to spread
- **Support** entities defensive and detection
- **Data extraction** ability

2. Test and reduce risk of cyber threats

- **Testing** must be proportionate to entities size, business and risk profile
- **Red/purple team** assessment

3. Robust framework that boosts IT security

- **Resilient systems and tools** minimize the impact of risk
- Continuously identify **new risks** (threat hunting)
- Documented **business continuity plans**
- **Comms plan** and responsibilities

4. Reporting serious ICT incidents

- Log and **monitor incidents**
- Classify incidents by **ESA* standards**
- **Report** to relevant authorities
- Use **standard templates** provided

5. Third-party ICT concentration

- **Monitor risks** from third-party providers
- Convergence on **supervisory approach**
- Ensure service providers adhere to **Union Oversight Framework**

WHAT'S THE MOTIVATION?

Why customers and organizations
should care

Penalty

1%
worldwide turn

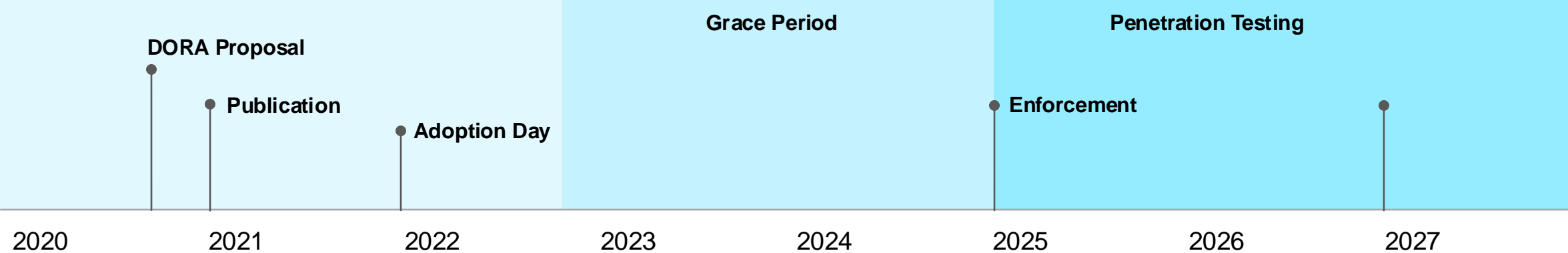
A periodic penalty payment of **1% of the average daily worldwide turnover**

Failure to provide information and documentation

Will not allow investigation and control

Failure to submit remediation report recommendation

DORA timeline



▲
Today

1. Build awareness, assign roles
2. Data discovery
3. Gap analysis
4. Planning and collaboration
5. Execution
6. Feedback

HOW CAN NETAPP HELP?

How to prepare

The requirements of DORA

Key articles

Article 28 General principles

Article 25

General principles

Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework and in accordance with the following principles:

1. Financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation and applicable financial services legislation.
2. Financial entities' management of ICT third party risk shall be implemented in light of the principle of proportionality, taking into account:
 - (a) the scale, complexity and importance of ICT-related dependencies,
 - (b) the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and to the potential impact on the continuity and quality of financial services and activities, at individual and at group level.
3. As part of their ICT risk management framework, financial entities shall adopt and regularly review a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in point (g) of Article 5(9). That strategy shall include a policy on the use of ICT services provided by ICT third-party service providers and shall apply on an individual and, as relevant, on a sub-consolidated and consolidated basis. The management body shall regularly review the risks identified in respect of outsourcing of critical or important functions.
4. As part of their ICT risk management framework, financial entities shall maintain and update at entity level and, at sub-consolidated and consolidated levels, a Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

The contractual arrangements referred to in the first subparagraph shall be appropriately documented, distinguishing between those that cover critical or important functions and those that do not.

Financial entities shall report at least yearly to the competent authorities information on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the services and functions which are being provided.

Article 9 Protection and prevention

Article 8

Protection and Prevention

1. For the purposes of adequately protecting the ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the functioning of the ICT systems and tools and shall minimise the impact of such risks through the deployment of appropriate ICT security tools, policies and procedures.
2. Financial entities shall design, procure and implement ICT security strategies, policies, procedures, protocols and tools that aim at, in particular, ensuring the resilience, continuity and availability of ICT systems, and maintaining high standards of security, confidentiality and integrity of data, whether at rest, in use or in transit.
3. To achieve the objectives referred to in paragraph 2, financial entities shall use state-of-the-art ICT technology and processes which:
 - (a) guarantee the security of the means of transfer of information;
 - (b) minimise the risk of corruption or loss of data, unauthorized access and of the technical flaws that may hinder business activity;
 - (c) prevent information leakage;
 - (d) ensure that data is protected from poor administration or processing-related risks, including inadequate record-keeping.
4. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall:
 - (a) 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;
 - (b) following a risk-based approach, establish a sound network and infrastructure management using appropriate techniques, methods and protocols including implementing automated mechanisms to isolate affected information assets in case of cyber-attacks;
 - (c) implement policies that limit the physical and virtual access to ICT system resources and data to what is required only for legitimate and approved

Article 10 Detection

(f) have appropriate and comprehensive policies for patches and updates.

For the purposes of point (b), financial entities shall design the network connection infrastructure in a way that allows it to be instantaneously severed and shall ensure its compartmentalisation and segmentation, in order to minimise and prevent contagion, especially for interconnected financial processes.

For the purposes of point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols enabled for emergency changes.

Article 9

Detection

1. Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 15, including ICT network performance issues and ICT-related incidents, and to identify all potential material single points of failure.

All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 22.
2. The detection mechanisms referred to in paragraph 1 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.
3. 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.
4. Financial entities referred to in point (f) of Article 2(1) shall, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors and request re-transmission of any such erroneous reports.

Article 11 Response and recovery

Article 10

Response and recovery

1. As part of the ICT risk management framework referred to in Article 5(1) and based on the identification requirements set out in Article 7, financial 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.
2. Financial entities shall implement the ICT Business Continuity Policy referred to in paragraph 1 through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aimed at:
 - (a) recording all ICT-related incidents;
 - (b) ensuring the continuity of the financial entity's critical functions;
 - (c) quickly, appropriately and effectively responding to and resolving all ICT-related incidents, in particular but not limited to cyber-attacks, in a way which limits damage and prioritises resumption of activities and recovery actions;
 - (d) activating without delay dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and preventing further damage, as well as tailored response and recovery procedures established in accordance with Article 11;
 - (e) estimating preliminary impacts, damages and losses;
 - (f) setting out communication and crisis management actions which ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 13, and reported to competent authorities in accordance with Article 17.
3. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall implement an associated ICT Disaster Recovery Plan, which, in the case of financial entities other than microenterprises, shall be subject to independent audit reviews.
4. Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.
5. As part of their comprehensive ICT risk management, financial entities shall:
 - (a) test the ICT Business Continuity Policy and the ICT Disaster Recovery Plan at least yearly and after substantive changes to the ICT systems;
 - (b) test the crisis communication plans established in accordance with Article 13.

Article 12 Backup policies, recovery methods

Article 11

Backup policies and recovery methods

1. For the purpose of ensuring the restoration of ICT systems with minimum downtime and limited disruption, as part of their ICT risk management framework, financial entities shall develop:
 - (a) a backup policy specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the sensitivity of the data;
 - (b) recovery methods.
2. Backup systems shall begin processing without undue delay, unless such start would jeopardize the security of the network and information systems or the integrity or confidentiality of data.
3. 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.

For financial entities referred to in point (g) of Article 2(1), the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.
4. Financial entities shall maintain redundant ICT capacities equipped with resources capabilities and functionalities that are sufficient and adequate to ensure business needs.
5. Financial entities referred to in point (f) of Article 2(1) shall maintain or ensure that their ICT third-party providers maintain at least one secondary processing site endowed with resources, capabilities, functionalities and staffing arrangements sufficient and appropriate to ensure business needs.

The secondary processing site shall be:
 - (a) located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;

General principles

Article 28

Article 28

General principles

Article 28 is a key Article within DORA that has gained the most attention. Article 28 focuses on **third-party ICT providers** and the risks posed to financial entities by over-consolidation 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.

“ Entities shall put in place exit strategies 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 and securely and integrally transfer them to alternative providers or reincorporate them in house. ”

- DORA, Article 28: General Principles

General principles

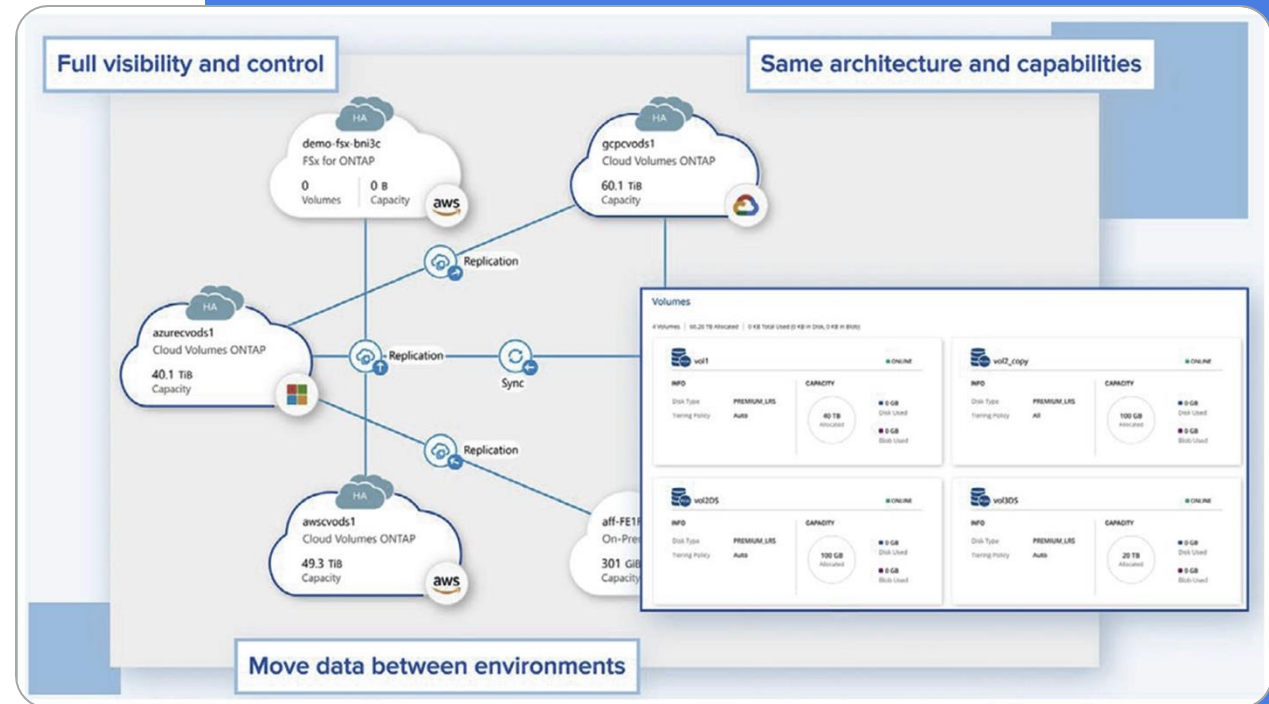
Article 28

Cloud Volumes ONTAP, FSxN, ANF, GCNV

NetApp® Cloud Volumes ONTAP 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.



Protection and prevention

Article 9

Article 9

Protection and prevention

Article 9, 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.

“ **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.

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

- DORA, Article 9: Protection and Prevention

Protection and prevention

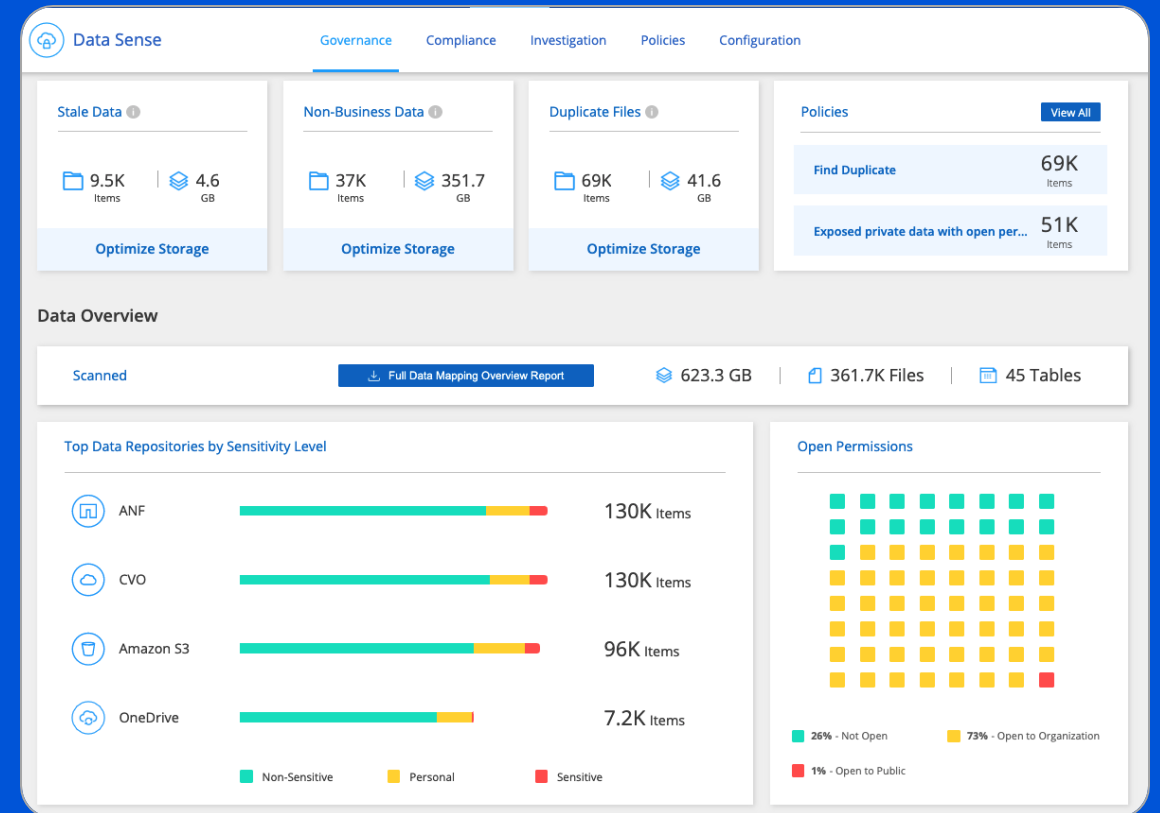
Article 9

Analyse 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® BlueXP classification** 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.



Protection and prevention

Article 9

Malicious file blocking

Based on access permissions, 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.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection

50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

Protection and prevention

Article 9

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.

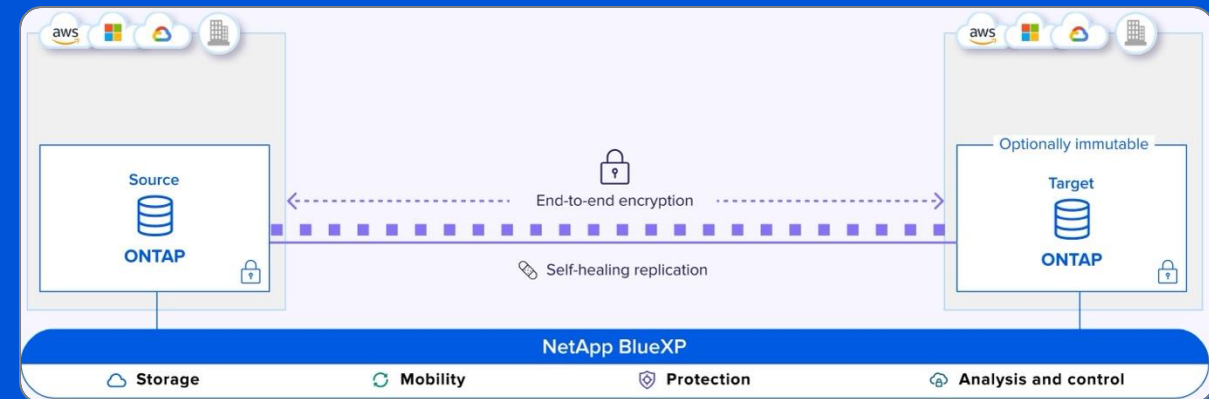
End-to-end encryption

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).

Add at least one approval group to continue

Name	Approvers	Email Address	Default Group
PrimaryMAV	<div style="border: 1px solid gray; padding: 2px; display: inline-block;">admin × admin2 ×</div>	MAV@judsonian.com	<input checked="" type="checkbox"/>

+ Add



Detection

Article 10

Article 10 Detection

Article 10 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.

“ **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.

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 10: Detection

Detection

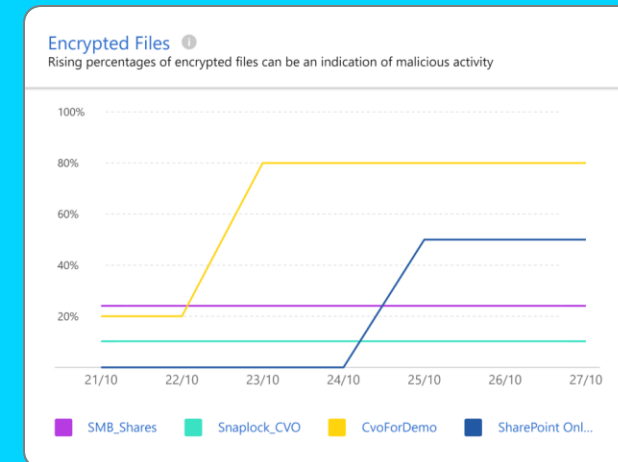
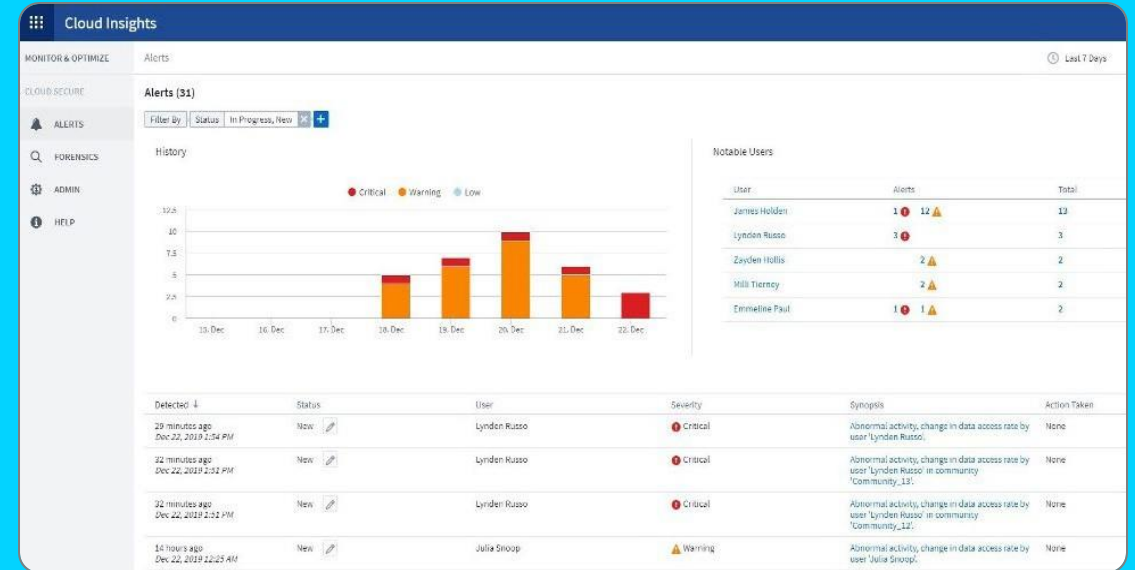
Article 10

User anomaly detection

(UBA) is required to identify and prevent or limit sophisticated ransomware attacks. UBA capability **tracks the behaviour** of individual users and communities to identify typical data access patterns. It then reports when behaviour differs from the normal observed pattern. In such cases, UBA can proactively respond by denying access to files and folders where suspicious activity is found.

Encryption Monitor

Tracking encryption events is key defence against ransomware. Automated responses such as Snapshots or breaking replication to prevent infection spreading help protect against this.



Response and recovery

Article 11

Article 11 Response and recovery

Article 11 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.

“ ...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 11: Response and Recovery

Response and recovery

Article 11

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

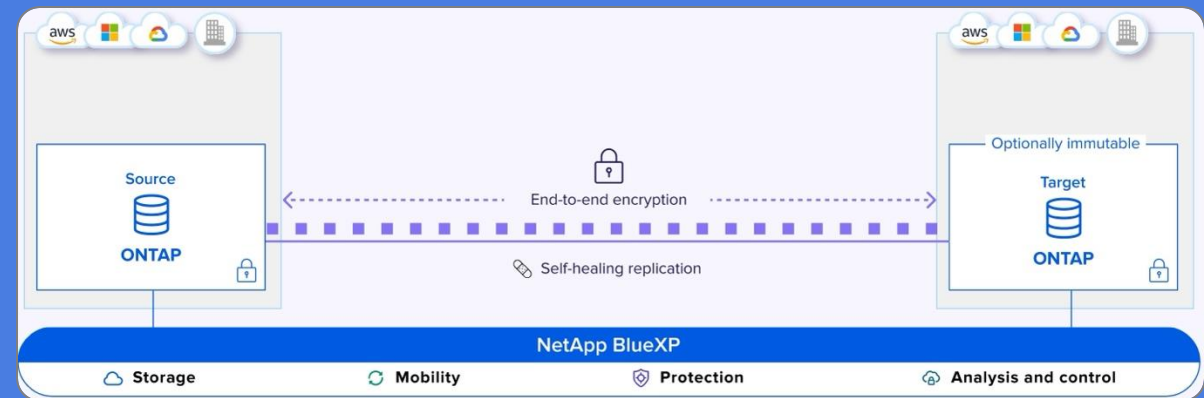
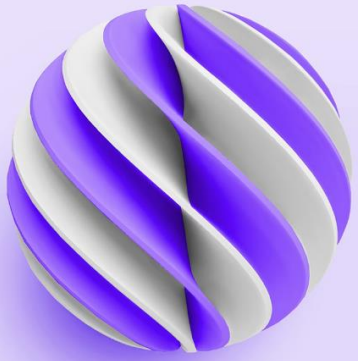
Immutable data copies

NetApp systems are protected by **Snapshot copies**, which are point-in-time, read-only images of your data. Because Snapshot images are read-only, captured data can't be encrypted and locked by ransomware. With the **FlexClone and SnapRestore**, 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.

HOME / SERVICES / Professional Services

Consulting and Professional Services

Quickly evolve your IT environment to meet growing business expectations and demand for data services—no matter where your data resides.



Backup policies, recovery methods

Article 12

Article 12

Backup policies, recovery methods

Article 12 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

“ 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 12: Backup policies, recovery methods

Backup policies, recovery methods

Article 12

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

You 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 recover data if a volume is compromised by a ransomware attack.

Air gap copies and clean rooms

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, SnapLock Compliance software takes capability to a new level by logically air gapping your data without any need for physical separation.

Clean rooms build upon this with compute and networking available to **restore copies of data** to forensically examine it for corruptive and restore safely.

Governance and Organisation

Article 5

Article 5

Governance and Organisation

Article 5 **firmly places responsibility** on the management body (C-Suite).

They must be trained in the risks of Cyber Threats and make the business decisions such as deciding risk tolerance.

“ 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

”

- DORA, Article 5: 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](#)

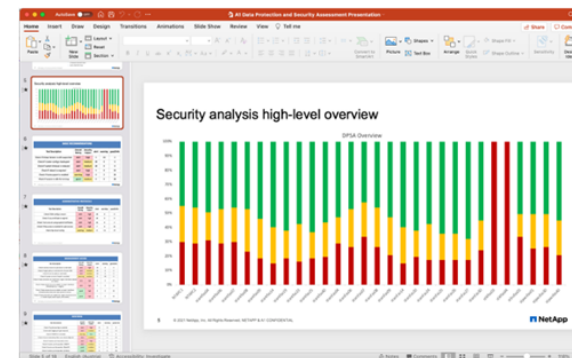
NetApp Data Protection & Security Assessment

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](#)



3.0 Snapshot Analysis

Customer utilizes NetApp Snapshot and SnapMirror technology to perform backups on most volumes to provide disaster recovery and business continuity. This study focuses solely on the NetApp backup and replication technology.

Snapshots are point-in-time copies to protect data without the requirement of purchasing an excessive amount of storage and without a performance impact, allowing data to be recovered quickly. When creating snapshots of data volumes, pointers are created to original data blocks and during normal use of the data the blocks are changed. If a volume or file needs to be restored to a prior version, it's a simple and easy process to change the active pointer to the blocks from the snapshot copy, restoring the file or volume to its prior state.

Following charts and tables reflect elements Rotterdam usage of snapshot technology for its volumes by data category. Volumes excluded from the analysis are Data Protection (DP) volumes, which have snapshots on the primary cluster volumes, and SVM root volumes.

Findings:

- all volumes of category 1 are meeting the sla of immediate recovery capability of 14 days
- 2 volumes, MOSAQ and RADT, have 195 local snapshots older than 60 days
- 3 volumes have one or two snapshots older than 60 days
- all volumes of ntapaff03 and ntapaff29 have no hourly snapshot of the last hour
- ...

Recommendations:

- add hourly schedule for all critical volumes to minimize data lost to 1 hour
- Review the list of snapshots older than 61 days and clean up to free space if no longer required
- ...

WHAT NEXT?

Get Ready For DORA : [DORA \(netapp.com\)](https://netapp.com)

The screenshot shows the NetApp website's landing page for DORA. At the top, there is a navigation bar with the NetApp logo, a search bar, and links for 'Solutions & Products', 'Explore NetApp', 'How to Buy', and 'Support & Training'. Below the navigation bar is a large hero section with a dark background and a woman looking at a screen. The text in the hero section reads: 'Financial Services', 'GET READY FOR DORA', and 'The Digital Operational Resilience Act (DORA) comes into effect in January 2025. How prepared are you?'. Below the hero section is a white section titled 'What is DORA?'. It contains a paragraph explaining DORA as a new set of regulatory standards for managing cyber resilience concerns in the European Union financial sector. Below the paragraph is a bulleted list: 'Financial entities operating in the EU' and 'Third-party ICT service providers'. At the bottom of this section are two buttons: 'Dive into our DORA E-Book' and 'DORA Infographic'. The footer of the page includes the NetApp logo, copyright information '© 2024 NetApp, Inc. All rights reserved.', and the text '— NETAPP CONFIDENTIAL —'.

NetApp

What are you looking for?

Solutions & Products ▾ Explore NetApp ▾ How to Buy ▾ Support & Training ▾

Financial Services

GET READY FOR DORA

The Digital Operational Resilience Act (DORA) comes into effect in January 2025. How prepared are you?

What is DORA?

The Digital Operational Resilience Act, or DORA, is a new set of regulatory standards for managing cyber resilience concerns in the European Union financial sector. DORA impacts:

- Financial entities operating in the EU
- Third-party ICT service providers

[Dive into our DORA E-Book](#)

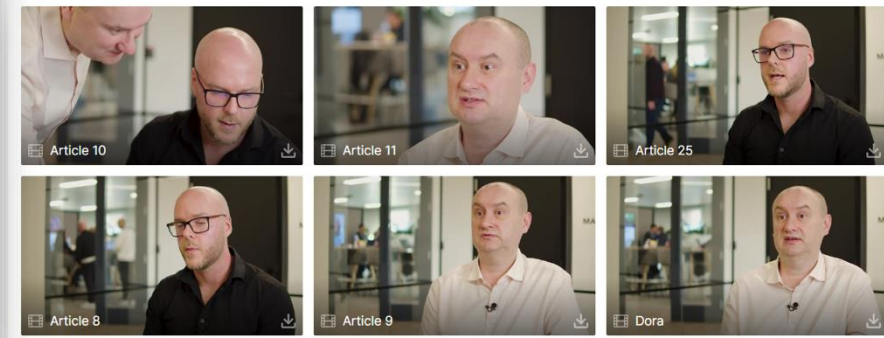
[DORA Infographic](#)

NetApp

© 2024 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —

Video content

1. DORA overview
2. Article 9
3. Article 10
4. Article 11
5. Article 12
6. Article 28



Webinar initiative DORA Series

The grace period for noncompliance ends in Jan 2025, which means the time to start building a DORA-compliant environment is now. NetApp will be hosting **a series of webinars every 8 weeks** to discover how NetApp can help meet five specific articles established in DORA guidelines.



NetApp.com DORA Website



Peter Dean

NetApp Industry Solutions – FSI Lead

LinkedIn – <https://www.linkedin.com/in/peterdean3/>



Adam Gale

NetApp Executive Architect

LinkedIn – <https://www.linkedin.com/in/adam-gale01/>



Steve Rackham

NetApp Industry Solutions – CTO for FSI

LinkedIn – <https://www.linkedin.com/in/strackham/>

ng-DORA-enquiry@netapp.com