

WHITE PAPER

DORA and Your Identity Infrastructure



TABLE OF Contents

1	Introduction
2	The emerging threat landscape
3	DORA
4		Identification and accountability
4		Access control
5		Resilience and business continuity
6		Monitoring and detection
6		Managing ICT third-party risk
7		Audits
8		Incident response and forensics
8		Threat-led penetration test
9		Continuous improvement
9		Tool specialisation
10	How can Semperis help?
13	Conclusion

Introduction

The advances of threat actors affecting our critical industries have significantly changed the expectations of regulators and the capabilities required to stay secure.

The European financial sector is feeling this with the introduction of the Digital Operational Resilience Act (DORA), which is coming into effect across the European Union (EU), and to an extent in the UK, and changing the game regarding required controls and financial services companies' cyber resilience.¹ The regulations, also known under the full name 'Regulations on digital operational resilience for the financial sector', were written into law in 2022.

The EU drove this initiative, recognising that the financial services sector is rapidly digitising, automating its service delivery, and increasingly leveraging cloud-based capabilities for business applications and underlying compute services. Digitisation means attacks can increasingly be scaled, something organised criminal groups and nation states are making the most of. In response to these developments, the EU drafted and issued DORA, which significantly elevates the obligations for a number of capabilities in financial services, such as incident reporting, preventive controls, penetration testing, third-party security, and the ability to recover and restore essential services after a breach.

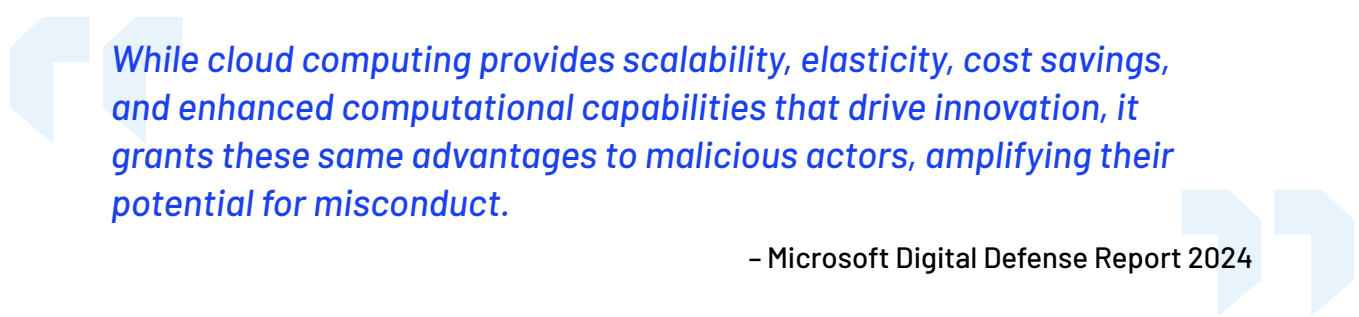
¹ DORA is an EU regulation, but because UK financial services organisations operate in the EU they will likely still be subject to the regulation.

The emerging threat landscape

The threats against the financial sectors in the EU and UK evolved rapidly over the preceding decade.

The **banking sector** remains one of the key sectors targeted by malicious actors, representing 9 percent of the attacks analysed according to ENISA, the EU's technical authority on cybersecurity and risk.²

The expanding use of **cloud computing services** is a major single point of failure and threat vector for the financial services industry across the continent. Whereas cloud vendors bring a strong set of security capabilities to their clients, they also represent a significant concentration risk. In 2023, more than 86 percent of companies reported an increase in cloud initiatives³ whilst 25 percent of banking executives had a strong focus on the cloud as a driver of resilience in 2024,⁴ and threat actors take advantage:



While cloud computing provides scalability, elasticity, cost savings, and enhanced computational capabilities that drive innovation, it grants these same advantages to malicious actors, amplifying their potential for misconduct.

– Microsoft Digital Defense Report 2024

Ransomware continues to cause high-profile, destructive attacks whilst increasingly exposing sensitive personal and business data from major organisations. Many of the groups likely use a different vector, such as social engineering or stolen credentials, to quickly pivot to the identity infrastructure, notably Active Directory (AD).

Even a prolific ransomware actor like Akira, which is otherwise known for leveraging perimeter device vulnerabilities, makes good use of the AD infrastructure, including creation of new administrative accounts on domain controllers for persistence and lateral movement and Mimikatz and LaZagne to steal credentials.⁵

Identity remains one of the main threat vectors for organised crime. Password spray attacks, weak passwords,⁶ unhardened environments from an access point of view,⁷ and vulnerabilities in multifactor authentication configuration routinely give attackers the dreaded way in. In fact, Microsoft reported 7,000 identity-based attacks per second in 2024. Ninety-nine percent of them focused on passwords,⁸ up from 4,000 the year before.⁹

² [ENISA THREAT LANDSCAPE 2024](#)

³ [Cloud Value: Navigating the Cloud Adoption Journey | Accenture](#)

⁴ [Cloud banking: How banks are using the cloud: PwC 2024](#)

⁵ [#StopRansomware: Akira Ransomware | CISA](#)

⁶ No or weak credentials is the lead compromise factor with 47.8 percent, according to [Google Cybersecurity Action Team, Threat Horizon, Apr 2023](#)

⁷ [Palo Alto Unit 42 found that 99 percent of cloud users, roles, services, and resources are granted excessive permissions](#)

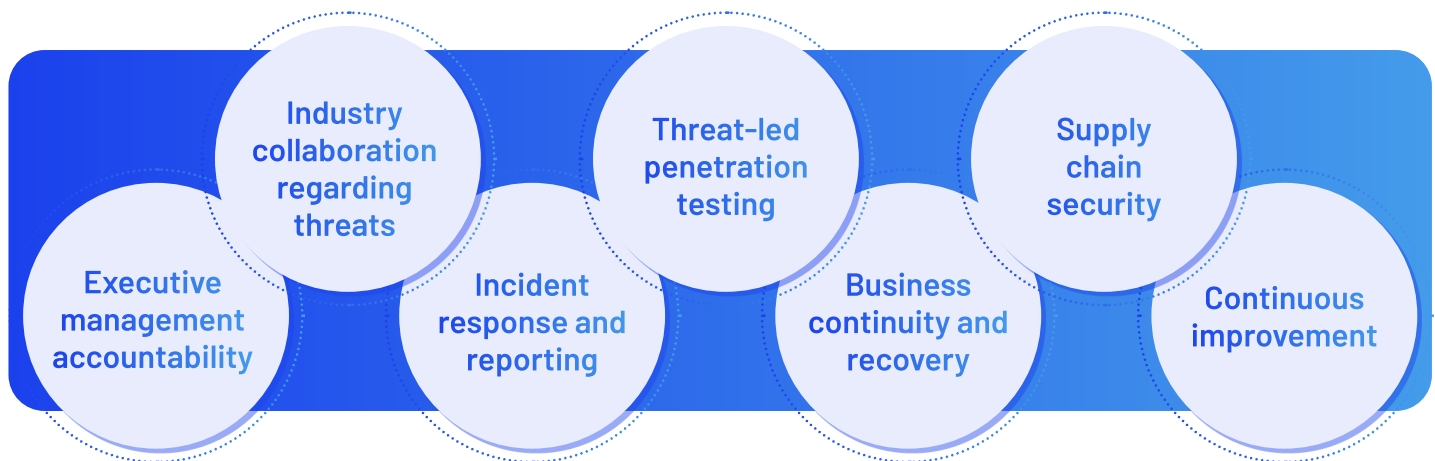
⁸ [Microsoft Digital Defense Report 2024](#)

⁹ Microsoft Digital Defense Report 2023

DORA

As a regulated entity subject to DORA, you will need to confirm a number of controls across the full spectrum of cyber resilience. Unfortunately, there's no silver bullet, unlike what some vendors might tell you. You need to ensure you have strong capabilities across the full regulation, but as you commence this journey (or wrap it up, for the lucky few), you'll do well to remember one of the core objectives of the regulation: building cyber resilience for your enterprise. This means ensuring resilient services are in place and they are resistant to destructive events, whether accidental or malicious, internal or external. You need to know that the key capabilities underlying your essential or important services can resist most attacks and be restored in good order if breached. Firms found to be violating DORA could face daily fines of up to 1% of daily average turnover for up to 6 months.

Areas of Control for the European Financial Services Sector



We will not cover all of this comprehensive text, but will focus on selected sections depending on the security and resilience of your organisation's identity infrastructure, notably AD and Entra ID.

Identification and accountability

DORA places stringent demands on an organisation's governance and ability to report on relevant structures and outcomes.

Section	Selected Clauses
Chapter II, Section 1, Article 5 (2c)	DORA requires appropriate governance and mapping for all information communication technologies (ICT)-related functions.
Chapter II, Section 1, Article 7 (1 and 4)	The regulation requires that ‘...financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk...’ In addition, these must be reviewed at least annually.

It is important that you clearly define ownership of your identity infrastructure. For most critical business functions, the identity directory infrastructure is a key dependency. All roads may not lead to Rome anymore, but arguably they do for your key ICT. More often than not, your journey to resilience starts with a functional AD. A robust AD capability alone will not address this challenge, but your organisation should be able to manage a major source of uncertainty in your resilience programme with strong asset management practices and a good view of the inbound and outbound dependencies from AD and Entra ID.

Access control

Your directory infrastructure is a key component to all access control.

Section	Selected Clauses
Chapter II, Section 1, Article 9 (4c)	Underlying the DORA regulation is the use of a strong, comprehensive controls framework. Specifically, for identity and access management (IAM), the regulation requires organisations to ‘...limit the physical or logical access to information assets and ICT assets, ensure access rights, proper administration...’

Without control of your directory infrastructure, it likely will not be possible to comply with DORA requirements. Any misconfiguration or vulnerability could provide an attacker with the opportunity to compromise your IAM, thus providing them with a direct path to disrupt or hack critical or essential services. Identity-focused attacks are a significant threat vector in most major attacks. In their 2024 data breach report, IBM reported that “74% of data breaches start with privileged credential abuse”.¹⁰ Similarly, advanced threat actors—such as APT29, famous for the SolarWinds breach, which has historically leveraged supply chain vectors for initial compromise and persistence—are increasingly leveraging the state of hybrid identity in their weaponry.¹¹

¹⁰ <https://www.ibm.com/reports/data-breach>

¹¹ The regulation is clear on the need for robust IAM. An organisation should leverage supporting technical standards, such as ISO/IEC 27001 or the NIST Cybersecurity Framework, which provide comprehensive details on IAM controls.

Resilience and business continuity

DORA focuses on ensuring a resilient financial services industry for the EU. Your directory service infrastructure plays a crucial role in this.

Section	Selected Clauses
Chapter II, Section 1, Article 7(1)	Your key ICT services must be maintained for resilience.
Chapter II, Section 1, Article 11(1-4)	The regulation outlines that ' <i>Comprehensive Business Continuity Management (BCM), Disaster Recovery (DR) and auditable DR tests for critical systems are required</i> '.
Chapter II, Section 1, Article 11(5-6)	You need the ' <i>ability to evidence dependencies for critical information assets and annual testing of cyber-attack scenarios</i> '.
Chapter II, Section 1, Article 12	The regulation outlines a full set of requirements for backup policy and procedures, including scope, restore, backup, and security of the data in backups (integrity and confidentiality).

Your identity infrastructure is key for using most, if not all, digitally enabled services. Without a plan for AD and Entra ID, you might have a problem with a significant number of services covering general resilience through ICT services. Testing AD can be a significant challenge for large organisations, and this is even more pronounced with AD due to the various dependencies and challenges of full forest recovery.

Following a cyber-attack, your AD is likely to be critical in a restore situation, and regulators will likely expect this component to be included in an annual restore test. Microsoft's guidance for full AD forest restore has more than 29 steps and numerous pitfalls, including dependencies for other services such as the Domain Name System, and how to avoid restoration of malicious code in different volumes, such as SYSVOL.¹²

¹² <https://www.semperis.com/blog/manual-ad-forest-recovery-problems/>

Monitoring and detection

Because of the high number of methods focused on hacking AD, monitoring and detection are key to resilience and containment.

Section	Selected Clauses
Chapter II, Section 1, Article 9 (1), as well as Chapter III, Article 17	'.. continuously monitor and control the security and functioning of ICT systems and tools...' and minimise impacts of any attacks

Threat actors gravitate to your directory infrastructure to elevate privileges, move laterally, and create persistence post-breach. This enables a number of stealthy attacks on AD, making your Security Operations Centre (SOC) unlikely to be able to address all indicators of compromise. Monitoring and detection are critical for organisations to identify emerging attacks; thus, the average time for a bad actor to gain access to AD is 16 hours,¹³ after which privilege escalation, persistence, and significant adverse effects can be very difficult to avoid. If the attacker manages to wipe out the AD forest, the organisation is looking at an average of 21 days to achieve full recovery, according to Forrester.¹⁴

Managing ICT third-party risk

A recurring theme in regulations around the world is how to manage supply chain risk. This is also a major component of the new DORA regulation.

Section	Selected Clauses
Chapter V, Section 1, Articles 28 & 30	Managing ICT third-party risk
Chapter V, Section 2, Article 31	Your lead overseer from the regulator is required to designate critical third-party service providers centrally.

You're still ultimately accountable for the availability and security of your organisation's directory services and the business functions it supports, even if your organisation leverages third-party suppliers to manage this capability. The 2024 Verizon Data Breach Investigations Report identified more than 15% of 10,000 confirmed data breaches that had a supply chain component. For the MOVEit attack alone, they were able to identify 1,567 breach notifications.¹⁵

¹³ <https://www.scworld.com/resource/ransomware-gangs-take-less-than-a-day-to-breach-microsoft-active-directory-heres-what-to-do>
¹⁴ <https://www.semperis.com/wp-content/uploads/resources-pdfs/resources-forrester-total-economic-impact-semperis.pdf>
¹⁵ [Verizon Data Breach Investigations Report \(DBIR\) 2024](#)

If we are correct in our assertion that you deem AD critical to your regulated services, you will need to address the many requirements in DORA via your supplier. This means having a contract and operating model where your supplier can provide evidence of both the security posture of AD and Entra ID (including hardening, vulnerability management and monitoring) and its resilience through measures such as backup, recovery, and restore testing. You may require the ability to audit the security posture of your directory services and have an effective means to report on this. You must also make sure your supplier of choice can support you in detecting and investigating security events as well as provide timely input to any incident response and recovery activities. Most suppliers will provide you with comforting language in their marketing about such capabilities, but what happens if your outsourcing provider has multiple big clients with simultaneously breached and encrypted ADs?

Lastly, it is very likely that Microsoft will be such a ‘designated’ supplier for financial services organisations in the EU. Are you ready to manage the fallout and questions from your audit committee, board, and senior leadership if the overseeing authority reports negative findings about AD or Entra ID?

Audits

Considering the criticality of the services within DORA’s scope, any required controls will be subject to auditing from the regulator (or proof of audit towards your suppliers).

Section	Selected Clauses
Section 1, Article 6 (6–7)	Both your services as a regulated financial sector organisation and your supplier’s will be subject to annual or regular audits. In addition, the regulation specifies that auditors should be skilled and experienced. Finally, a timely follow-up process on audit findings is a must.

Anyone working in security in highly regulated industries knows the disruptive potential of an adverse audit finding. It’s obvious that a red audit finding for a key service can impact your licence to operate and be a source of fines. When it comes to an audit of AD, many misconfigurations and weaknesses require a comprehensive approach to AD security to proactively control the conversation. If you don’t have this holistic view, your organisation will likely find itself constantly being reactive with auditors (and worse, with attackers).

Incident response and forensics

A big component of DORA pertains to visibility into threats and breaches. In cyber-attacks where the directory services are a main attack vector and means of disruption, such analysis and response become key.

Section	Selected Clauses
Chapter III, Article 19	Reporting of major ICT-related incidents and voluntary notification of significant cyberthreats

Forensics analysis on the AD is challenging. Attackers routinely use open-source tools, such as BloodHound, that quickly map attack paths by exploiting permissions and unintended configurations, allowing them to rapidly attain administrative access without alerting the defenders.

If an attacker achieves privileged access to the directory service, they have a broad array of opportunities to delete traces of their activity (or the whole log). A common method of attackers is to overwrite the logs of the infrastructure, and securing such data is difficult with native capabilities. The Cybersecurity and Infrastructure Agency recently noted that Ransomhub, Play, LockBit 3.0, and Ghost make use of this tactic.¹⁶

Threat-led penetration test

Active and advanced testing by red and blue teams invariably target an organisation's AD forest. DORA places significant emphasis on such advanced assurance processes for systems that support critical and essential services.

Section	Selected Clauses
Chapter IV, Articles 24 & 25	The regulation requires at least an annual Threat-led Penetration Test (TLPT) of all ICT systems supporting critical or important functions.

The TLPT can take many forms, but if the red team/attacker targets your AD, are you confident as a defender that you can detect the attack and respond through isolation? Post-breach, you also need to be able to clean and restore the system into a safe and trusted operational state. Whether it's a case of an actual attacker or a TLPT, you need to harden AD and patch vulnerabilities to stop or slow down their progress. On the other hand, if you are caught out by a penetration test, you need a rapid response to the regulator.

¹⁶ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>

Continuous improvement

A foundational aspect of DORA, like other regulations, is the need for continuous improvement.

Section	Selected Clauses
Chapter II, Section 1, Article 15	Evolution of the capability and introduction of new standards

Security is a bit like swimming against the current. On the surface, a duck looks calm, but under the water the duck is working hard. Staying on top of new guidance documentation from regulators can be a challenge. This is compounded by the continually changing nature of AD as users are onboarded, offboarded, or change roles and their settings change. Thus, standing behind a claim to your auditor or regulator that you are compliant and secure in your directory infrastructure is daunting if you're not constantly interrogating and adapting to new and evolving threats and new standards or continually monitoring AD for indicators of exposure.

Even having a person test and improve the AD forest restore can be a major undertaking. Automation is not just 'nice to have' for complex enterprises, it is a must.

Tool specialisation

DORA's guidance intentionally lacks specificity so it can cover many aspects of security across a breadth of information systems. This creates a unique challenge because you are responsible for understanding the intricate details required to secure each system and implement a programme to comply with DORA's standards. Specialised toolsets designed to secure these systems allow you and your organisation to shift focus from day-to-day security operations to a strategic focus to quickly and efficiently implement policies and procedures to keep your identity systems secure. Consider evaluating security solutions that are purpose-built for identity security such as Semperis, which offers community and paid tools that directly address the challenges of complying with DORA.

The tables on the following pages highlights the specialised capabilities that Semperis provides to address DORA's challenges.

How can Semperis help?

Challenge	How Semperis can help	Solution
<p>Identification and accountability</p> <p>In order to comply with DORA, it is vital that your organisation appoints someone responsible for ICT resilience.</p>	<ul style="list-style-type: none"> • Map dependencies to enable AD restore • Provide visibility into directory services security posture • Conduct risk identification and management, which are key for DORA compliance 	<ul style="list-style-type: none"> • Active Directory Forest Recovery (ADFR) automates forest recovery, including relevant dependencies. • Purple Knight provides point-in-time security assessment of AD or continuous threat and vulnerability detection and automatic backout of malicious changes. • Directory Services Protector (DSP) provides tamper-proof tracking by capturing every change made in AD and helps to identify malicious changes. • Migrator for AD streamlines AD modernisation by mapping dependencies and migrating objects to a greenfield AD environment.
<p>Access control</p> <p>You rely on the integrity, security, and resilience of AD and Entra ID to achieve privileged access and IAM objectives.</p>	<ul style="list-style-type: none"> • Identify and eradicate misconfigurations and vulnerabilities • Accelerate recovery in case of an outage to enable teams to continue working securely • Understand attack paths used to gain administrative access 	<ul style="list-style-type: none"> • DSP enables continuous monitoring of security posture of the AD and Entra ID • ADFR reduces AD forest recovery time by up to 90%. Forest Druid (a no-cost community tool) discovers attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit. • Forest Druid supports AD teams in mapping attack paths automatically.

Challenge	How Semperis can help	Solution
Resilience and business continuity To comply with DORA, you need to be able to restore your directory infrastructure rapidly and have tests to validate you can accomplish this.	<ul style="list-style-type: none"> • Early detection or avoidance of a security breach of your directory infrastructure and dependent ICT services • Proven, clean-state restore with validated recovery point objectives and recovery time objectives • Well-maintained ICT services 	<ul style="list-style-type: none"> • ADFR automates the complicated recovery process for AD and recovers AD up to 90% faster. • ADFR also allows post-breach forensics to remove persistence and recover AD to a trusted state. • Disaster Recovery for Entra Tenant (DRET) recovers Entra ID objects and principles to a known good state.
Monitoring and detection Your directory infrastructure is a rich source of vulnerabilities and misconfigurations, requiring skill and dedication for meaningful detection.	<ul style="list-style-type: none"> • Monitoring AD and Entra ID is a strong DORA requirement to detect attacks and be able to accurately report on incidents. • Comprehensive control of the constantly changing AD environment with its rich attack surface • Visibility into the many AD-focused attacks and changing vulnerabilities 	<ul style="list-style-type: none"> • DSP enables continuous assessment of indicators of exposure in AD, automated rollback of malicious changes, and detection of machine learning (ML)-based attacks on AD • DSP provides tamper-proof logs and highly specialised AD/Entra ID threat analysis, enabling up-to-date, industry-leading insights and automation for directory security and enrichment of SOC visibility through security information and event management (SIEM) integration • Semperis products are enhanced by deep research from the AD-focused threat team.
Managing of ICT third-party risk If you outsource your AD operations you will need a strong focus on third-party risk, but if you leverage Entra ID, Microsoft will be such a supplier to your organisation regardless.	<ul style="list-style-type: none"> • A strong view of the security posture of outsourced directory infrastructure services • Evidence of resilience and restorability of your directory infrastructure services 	<ul style="list-style-type: none"> • DSP enables vulnerability management and exposure and threat detection. • ADFR provides automated, clean restore to any hardware or cloud solution.

Challenge	How Semperis can help	Solution
Threat-led penetration test The ability to avoid adverse findings in testing or rapidly address ones already found	<ul style="list-style-type: none"> • Remediation of critical vulnerabilities in your directory infrastructure prior to the penetration test • Ability to address such test findings after the event • Provision of realistic test environment to avoid the need to test live 	<ul style="list-style-type: none"> • DSP provides comprehensive analysis of indicators of exposure and step-by-step analysis on closing security gaps • ADFR enables post-breach forensics investigations, which can be used during disaster recovery or penetration testing exercises to ensure a clean restore of AD services.
Incident response and forensics DORA imposes strict incident reporting requirements on organisations.	<ul style="list-style-type: none"> • Secure your logs for forensic analysis • Enhance ability to detect actions of malicious actors and rapid incident reporting of attacks impacting AD and Entra ID 	<ul style="list-style-type: none"> • DSP's tamper-proof change tracking enables you to track changes even if security logging is turned off, logs are deleted, agents are disabled or not working, or changes are injected directly into AD or Entra ID. • DSP Identity Runtime Protection uses ML-based learning to detect ongoing attacks on AD, which are traditionally buried in logs and difficult to detect.
Continuous improvement Auditors and regulators will seek evidence of your dedication towards continuous improvement.	<ul style="list-style-type: none"> • Drive continuous improvement and automation through Semperis' industry leading threat intelligence and automation. 	<ul style="list-style-type: none"> • DSP and ADFR all drive best-of-breed resilience and risk reduction for your directory infrastructure services. They are essential tools that can integrate with your organisation's overall security program.

Conclusion

DORA regulations apply to the EU financial services sector and require significant measures to achieve compliance. To comply with the regulation, we recommend that you establish eight major capabilities for the resilience of your AD and Entra ID services:

1. Establish governance and ownership for your directory services.
2. Build visibility into risks and dependencies.
3. Establish comprehensive and automated exposure, threat, and vulnerability monitoring and integrate this capability into your SOC.
4. Reduce your directory vulnerabilities to reduce the attack surface for penetration testers and hackers alike.
5. Ensure you have the appropriate requirements and means of managing directory services risk in your supply chain.
6. Build robust response capabilities for your directory services to enable rapid incident response, reporting, and forensic capabilities.
7. Have an automated and tested recovery process to enable rapid restoration in case of a destructive incident.
8. Establish a project of continuous improvement, including adopting best practices from the cybersecurity industry.

In our experience, achieving the above is not sustainable over time without significant automation. Semperis' market-leading products can provide you with this threat-led, automated capability.