A Reversec Whitepaper

Connecting the Dots: Shared Requirements of ISO 27001, NIS2, DORA and DFS

What do ISO 27001, NIS2, DORA and DFS have in common? A lot actually.

Authors:
Antti Laatikainen, Ondrej Doubek
Richard Suls and Jarkko Mattsson

REVERSEC

Contents

Connecting the Dots

What do ISO 27001, ISO 27001, NIS2, DORA and DFS have in common? A lot actually.
We've mapped out the shared requirements for you.

The big secret about regulations is that they are all essentially the same.

The cybersecurity landscape is facing a tsunami of regulations, as governments worldwide work to respond to increasingly complex and frequent cyber threats, data breaches, and national security worries. From sectors ranging from finance to critical infrastructure, CISOs across the globe now feel they must navigate an increasingly complex web of compliance requirements that vary by region and industry. But at the end of the day, the basic requirements are pretty much the same in all the main regulations, they're just formulated a bit differently.

This whitepaper is your guide to navigating the storm. In it, we will highlight how regional initiatives and regulatory packages might affect your business, how you can strategically meet these requirements, and how we can help.

We've selected the **ISO 27001 standard** along with three key regulations: the **Network and Information Security Directive 2** (NIS2), the **Digital Operational Resilience Act** (DORA), and the **NYDFS Cybersecurity Regulation** (DFS). We asked four of our top experts to weigh in on their practical implications and areas of application. In Chapter 2, we've mapped out the common security policies, controls, and activities into one comprehensive table to help you kick-start your security risk management journey.

Chapter 1:
ISO 27001 and the Big Three Regulations: DORA, NIS2, and DFS

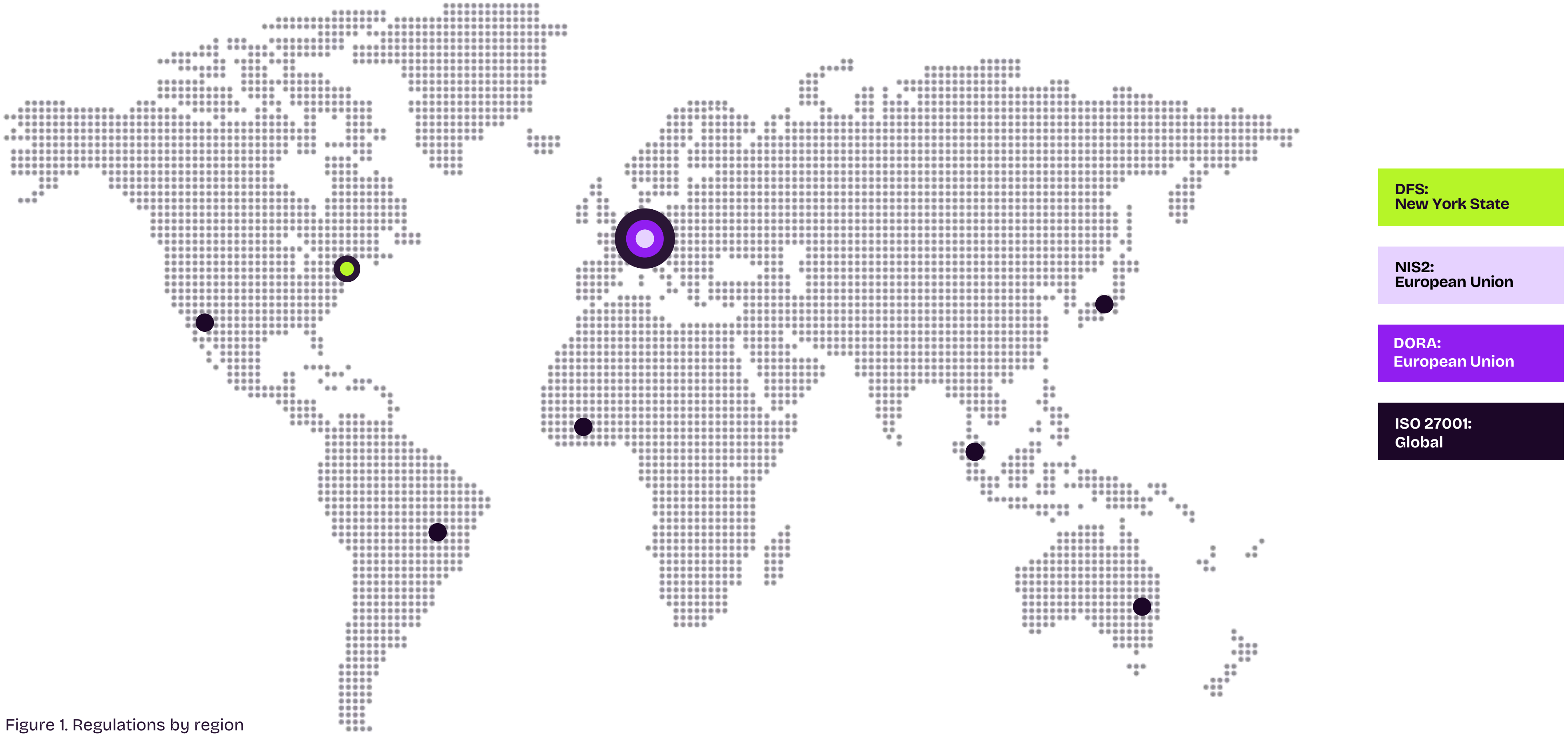


Figure 1. Regulations by region

What is DORA and to whom does it apply?

The Digital Operational Resilience Act (DORA) is a European Union cybersecurity regulation applicable to all financial organizations with operations in EU member states. Its goal is to ensure that financial entities within the EU can withstand and recover from all types of ICT-related disruptions and threats. It came into force in January 2023, and compliance with most of its provisions have been mandatory since January 2025. The consequences for non-compliance range from financial penalties and public reprimands to restrictions on business operations.

DORA's key focus areas include risk management, incident reporting and digital operational resilience testing. Financial institutions must conduct regular self-assessments and independent audits of their ICT risk management frameworks. So, what do these requirements mean in practice? Check out the chart in Chapter 2.

What is NIS2 and to whom does it apply?

NIS2 is the updated version of the original NIS Directive (NIS1), adopted 2016 as the first EU-wide cybersecurity law. NIS2 was updated in 2022 and enacted into law in 2024 to strengthen cybersecurity across member states. It's the regulation for all the critical infrastructure in EU countries.

Naturally, all those industries run on IT or at least need support from IT systems to function. NIS2 enforces a set of minimum-level cybersecurity and cyber hygiene regulations that these organizations need to consider in their operations.

For organizations that need to comply, requirements like regular risk assessments, encryption, audits and security reviews are now mandatory. NIS2 mandates that initial incident reports must be submitted within 24 hours, and a more comprehensive report within 72 hours. NIS2 significantly extends cybersecurity obligations to suppliers and third-party vendors, requiring measures to mitigate risks associated with third-party relationships and ensure a robust cybersecurity posture across the supply chain.

Authorities now have more oversight and can conduct audits, issue binding instructions and impose sanctions. Non-compliance can result in harsh penalties like fines of up to €10 million or 2% of a company's global turnover.

The European approach to NIS2 and other regulations emphasizes accountability and prevention. CEOs and senior management are held responsible for their organization's cybersecurity measures, requiring them to oversee, approve, and be trained on these measures to address cyber risks effectively. CISOs must implement best practices to achieve the same goals. The growing threat landscape and NIS2's focus on prevention place significant additional pressure on CISOs in organizations that need to comply.

Figure 2. NIS2 industries

What is DFS and to whom does it apply?

The DFS Cybersecurity Regulation (23 NYCRR 500) is a set of cybersecurity requirements issued by the New York State Deparent of Financial Services (NYDFS). It applies to financial institutions, including banks, insurance companies, and other financial service providers operating under NYDFS supervision. This includes non-US organizations licensed in the state of New York. It is designed to protect consumers and ensure the safety and soundness of the institution, as well as New York State's financial services industry. To that end, supervised entities must assess their cybersecurity risk profiles and implement a comprehensive plan that recognizes and mitigates that risk.

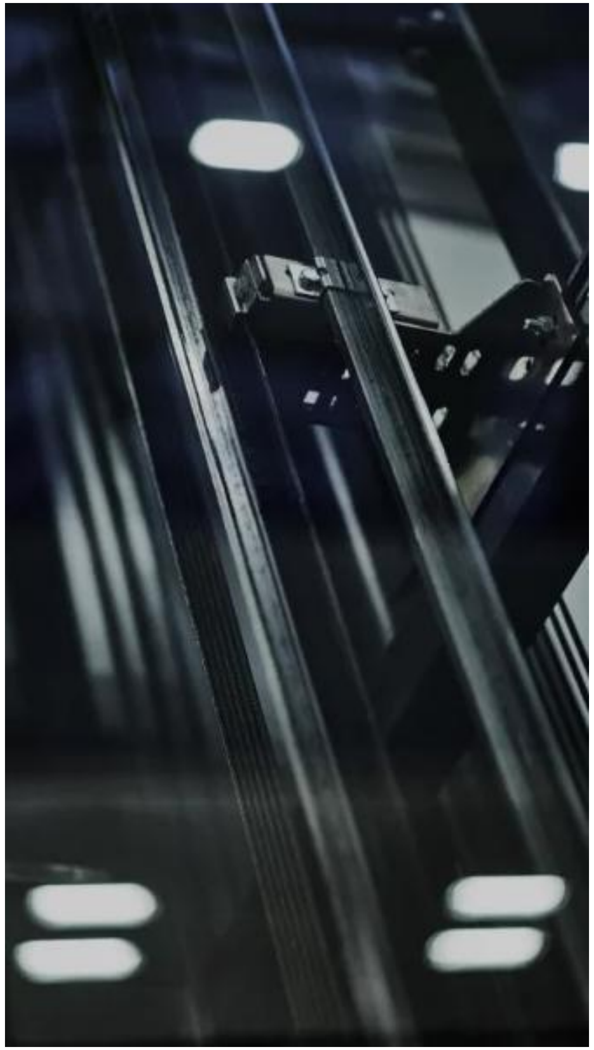
The DFS was one of the first U.S. regulations to mandate specific cybersecurity measures for financial institutions. It first came into force in 2017 and has been amended since then. **The final compliance deadline is November 2025**, and non-compliance can lead to regulatory fines, penalties, and reputational damage. This regulation has a tiered structure in its new amendment – the Cybersecurity Regulation 500. Some requirements apply to all firms, while others are specific to Class A companies with over one billion dollars in assets or a certain number of employees.

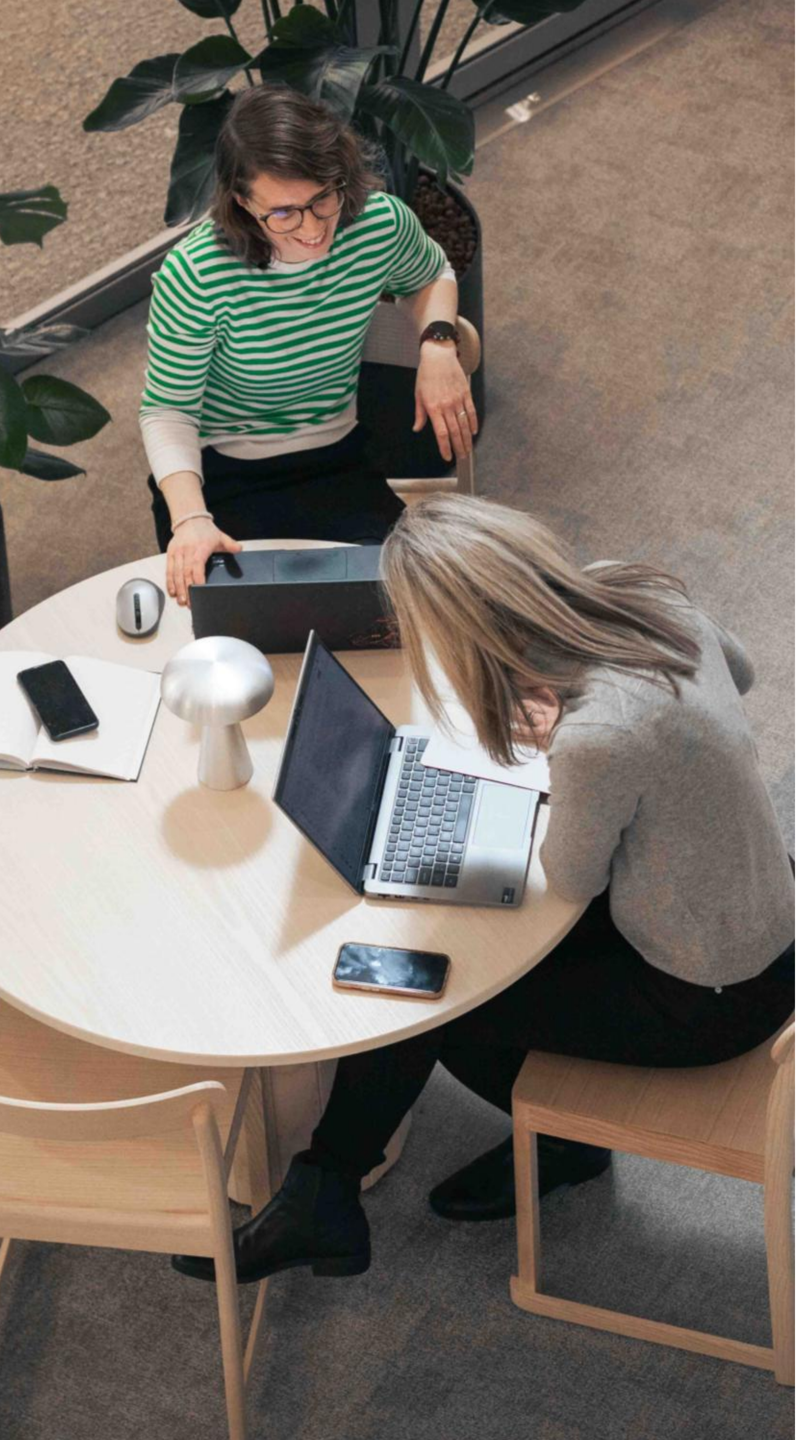
One key change is making the C-suite more accountable for security measures, ensuring they are signed off and tested. This addresses the previous lack of accountability. The DFS sets rules for incident reporting and emphasizes preparedness with measures like tabletop exercises and crisis management drills. These amendments show DFS' proactive approach to improving cybersecurity readiness.

THE CHALLENGES FOR CISOs

The DFS specifically mandates that CISOs report issues directly to them, necessitating new incident reporting mechanisms, including forming internal reporting bodies and new communication channels. CISOs also face the challenge of collaborating with their legal teams to determine what needs to be reported and what doesn't. This often requires an increase in staffing for CISOs and their teams.

The DFS requirements now mandate that CISOs understand their SaaS vendors' activities more deeply. Previously, it might have been sufficient to ask a vendor to complete their annual tabletop exercise or share security assessments of their products. However, the new requirements mean you must actively source this information, maintain it as part of your inventory, and demonstrate that you are effectively managing both your own cybersecurity measures and those of your vendors.





What is ISO 27001 and to whom does it apply?

ISO 27001 is the leading international standard focused on information security. First developed in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), it helps organizations of any size and any industry protect their information in a systematic and cost-effective way through the adoption of an information security management system. The most recent update was in 2022.

Unlike the other regulations outlined here, ISO 27001 isn't legally mandatory. It is, however, considered one of the most highly-respected standards for information security management systems.

While all of the standards we've covered here have a lot in common when it comes to steps you need to take to be compliant, it's fair to say that ISO 27001 is one of the easiest to implement. Because it's so well-structured, knowing what you need to do to comply is less complicated than it can be with others.

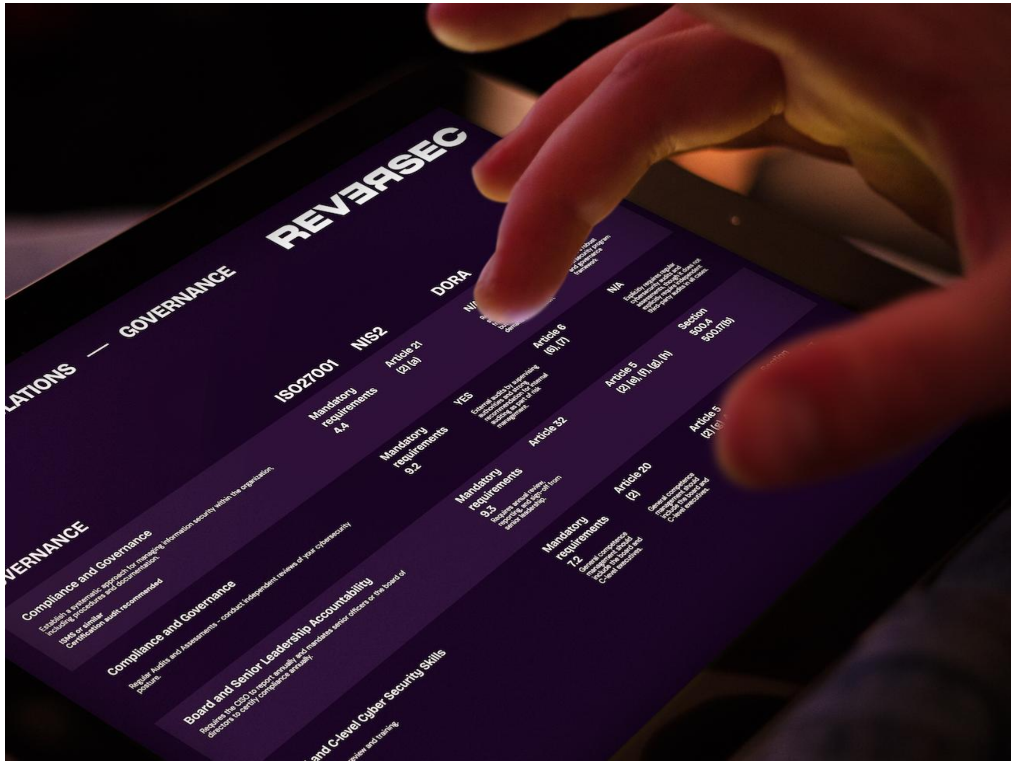
If you choose ISO 27001, the first challenge is to set the policies that will comply with the requirements. That means ensuring everyone across your organization knows how they need to behave to keep the company safe. And oftentimes, that's the easy part. Setting policies is one thing, but ensuring people in your organization stick to them is another. As a CISO, you must ensure that any policies work within your company culture while not disrupting your company's operations.

Another challenge is proving that your organization does what your policies say. If an auditor comes and asks to see your password policy, you'll also need to prove that you're able to detect if people within your organization aren't conforming. However, if you stick to the list of requirements, ensure that following them is something your organization understands and commits to, and if you stay on top of regular security checks, the challenges around ISO 27001 are easy to manage.

Chapter 2
Mapping the ISO27001 and the regulations

We've mapped out the common requirements of the three key regulations and the ISO 27001 standard to help you kick-start your security risk management journey.

As cybersecurity regulations proliferate, organizations now must navigate a maze of new proactive and reactive cybersecurity requirements and guidance. The good news is that many of them overlap, and there are several common security policies, controls and activities that all of them require you to fix to be compliant.



GOVERNANCE

GOVERNANCE	ISO27001	NIS2	DORA	DFS
Compliance and Governance Establish a systematic approach for managing information security within the organization, including procedures and documentation. **ISMS or similar** **Certification audit recommended**	**Mandatory requirements 4.4**	**Article 21 (2) (a)**	**N/A** Requires adoption of a strong security framework or standard but doesn't explicitly demand a certification.	**N/A** Mandates a robust cybersecurity program and governance framework
Compliance and Governance Regular Audits and Assessments - conduct independent reviews of your cybersecurity posture.	**Mandatory requirements 9.2**	**YES** External audits by supervising authorities and strong recommendation for internal auditing as part of risk management.	**Article 6 (6), (7)**	**N/A** Explicitly requires regular cybersecurity audits and assessments, though it does not explicitly require independent third-party audits in all cases.
Board and Senior Leadership Accountability Requires the CISO to report annually and mandates senior officers or the board of directors to certify compliance annually.	**Mandatory requirements 9.3** Requires annual review, reporting, and sign-off from senior leadership.	**Article 32**	**Article 5 (2) (e), (f), (g), (h)**	**Section 500.4 500.17(b)**
Board and C-level Cyber Security Skills Mandatory skills review and training.	**Mandatory requirements 7.2** General competence management should include the board and C-level executives.	**Article 20 (2)** General competence management should include the board and C-level executives.	**Article 5 (2) (g) 4**	**Section 500.4 500.13 500.14(a) 500.17(b)** Explicitly mandate training, though not skills review or specific certification.

REVERSEC

GOVERNANCE

GOVERNANCE	ISO27001	NIS2	DORA	DFS
Leadership is accountable for managing Information Security Risks	Mandatory requirements 9.3.2 (f)	Article 32	Article 5	Section 500.04 & 500.17(b)
A role responsible for Information Security must be assigned CISO or equivalent	Mandatory requirements 5.3	Article 32 Does not explicitly name CISO but someone needs to be named responsible.	Article 5	Section 500.04
Periodic Review & Continuous Improvement Requires covered entities to periodically update their cybersecurity program based on: • Emerging threats • Changes in business processes • Results of security testing and risk assessments	Mandatory requirements 10.1	YES Not explicitly required but included in general risk analysis.	Article 5 (2) (i) Article 6 (8) (d) Article 9 (4) (e)	Section 500.2(c)
Asset Inventory & IT Management Track Critical infrastructure & endpoints. Requires covered entities to maintain an accurate inventory of information systems, including assets, data, and privileged accounts.	Annex A 5.9	Article 21 (2)	Article 8	Section 500.13
Threat Intelligence Leverage threat intelligence to stay ahead of emerging threats.	Annex A 8.23 Not required but recommended.	YES Risk management and risk mitigation control selection should include evaluating emerging threats and risks.	Article 13 (1)	N/A Doesn't explicitly mandate using "threat intelligence," though regular risk assessments and monitoring are required.

ORGANIZATIONAL CONTROLS	ISO27001	NIS2	DORA	DFS
Policy and Compliance Define acceptable use policies for employees' use of company devices, networks, and data.	Annex A 5.10	Article 21 (2) (g)	Article 10 (3)	Section 500.3, 9, 11, 14, 17
Policy and Compliance Identify laws, standards, regulations (e.g. NIS2) and contractual agreements to which you must adhere.	Annex A 5.31	N/A References many additional regulations. Legal obligations are assumed to be part of the overall risk management framework but are not explicitly covered.	N/A References many additional regulations. Legal obligations are assumed to be part of the overall risk management framework but are not explicitly covered.	Section 500.3, 500.9
Supply Chain Security Identify key suppliers and third-party vendors in your supply chain, assess cyber security risks in the supply chain, and develop mitigation strategies for supply chain risks to ensure business continuity.	Annex A 5.19	Article 21 (2) (d)	Article 5, (2) (h), (I) Article 8 (5) Article 11 (4), (5)	Section 500.11
Threat Detection, Monitoring and Response: Detection Capabilities • System breaches • Network breaches • Other security incidents	Annex A 5.24 A 8.16 A 8.21	Article 21 (2) (b), (e)	Article 10 Article 11 Article 17 (2)	Section 500.5 , 500.16, 500.22 Doesn't explicitly require conducting purple team exercises but mandates periodic testing and validation of security controls.

REVERSEC

ORGANIZATIONAL CONTROLS	ISO27001	NIS2	DORA	DFS
Threat Detection, Monitoring and Response: Response Capabilities Incident response plans and playbooks	Annex A 5.24	Article 21 (2) (b)	Article 5 (2) (e) Article 11 Article 12	Section 500.16
Threat Detection, Monitoring and Response: Testing Incident response testing, disaster recovery exercises and Crisis Exercises Penetration Tests and Red Teaming	Annex A 8.13	Article 21 (2) (c), (g)	Article 11 (6) (a)	Section 500.16
Data Classification Information should be classified according to the organization's information security needs based on confidentiality, integrity, availability and relevant interested party requirements.	Annex A 5.12	N/A NIS2 does not specifically require data classification to be implemented. Effective risk management in practice needs it - to some extent.	Article 8 (1) Article 9 (4) (d)	Section 500.13, 500.15, 500.9, 500.3 Doesn't explicitly require formal data classification by confidentiality, integrity, and availability (CIA triad) but mandates controls that imply the need for data classification.

PEOPLE CONTROLS	ISO27001	NIS2	DORA	DFS
Security Awareness and Training Train employees on cyber security hygiene and recognizing and responding to cyber threats.	Annex A 6.3	Article 21 (2) (g)	Article 16 (1) (h) Article 30 (2) (i) Article 13 (6)	Section 500.14(b)
Security Awareness and Training Implement regular phishing exercises for employees to enhance awareness.	N/A	Article 21 (2) (g)	N/A	Section 500.14(b)
Reporting of Cybersecurity Events to Competent Authorities Ombudsmen CERT Regulatory bodies	Annex A 6.8	Article 12, Article 23 “to the supervising authorities” Article 24 “volunteered to peers”	Article 19	Section 500.17(a) 72 hours

TECHNICAL CONTROLS	ISO27001	NIS2	DORA	DFS
Asset Management Gain a thorough listing of your IT systems, like servers and computers, and their role in business processes and value chains.	Annex A 8	Article 21 (2) (i)	Article 6 Article 8 Article 9	Section 500.13
Data Encryption Encrypt sensitive data both at rest and in transit.	Annex A 8.1	Article 21 (2) (h)	Article 9 (4) (d)	Section 500.15
Deploy strong Identity and Access Management (IAM) to prevent misuse of systems and data. Enabling Multi-Factor Authentication (MFA) Connect to the company's infrastructure through VPN Strong authentication and encryption methods SSO Zero Trust Privileged Access Management	Annex A 8.5 A 5.15 A 8.27 Recommended.	Article 21 (2) (i), (j), (g)	Article 9 (4) (c), (d)	N/A Doesn't explicitly require remote session timeouts or passwordless authentication, but these practices align with the regulation's security intent of access control measures (Section 500.7, 12, 13).
Patch Management Plan and implement an effective process for installing critical security updates to all technologies (OS, infrastructure devices, and software updates). Prioritize internet-facing assets.	Annex A 8.8	Article 21 (2) (e)	Article 9 (4) (f)	YES Section not specified.

TECHNICAL CONTROLS	ISO27001	NIS2	DORA	DFS
Business Continuity and Disaster Recovery (BC/DR) Formulate a Business Continuity Plan. Formulate a Disaster Recovery Plan. Set up regular backups to ensure data recovery.	Annex A 8.13	Article 21 (2) (c)	Article 5 (2) (e) Article 11 Article 6 (8)	YES Section not specified.
Business Continuity and Disaster Recovery (BC/DR) Set up immutable backups for critical systems.	Annex A 8.13	Article 21 (2) (c)	Article 5 (2) (e) Article 11 Article 12	N/A
Logging and Monitoring Set up centralized logging, prioritizing critical systems.	Annex A 8.15	Article 21 (2) (e)	Article 16 (2) Article 17 (2) Doesn't talk about logging at all- only about detecting incidents in general.	Section 500.22, 500.06 Audit Trail
Network and Endpoint Security Apply proper network security controls such as service, network, and endpoint firewalls, and implement endpoint protection software to safeguard devices (Workstation, Server and Mobile devices).	Annex A 8.20	Article 21 (2) (g)	Article 9	YES Section not specified.

REVERSEC

TECHNICAL CONTROLS

TECHNICAL CONTROLS	ISO27001	NIS2	DORA	DFS
Network Security Deploy network segmentation based on asset purpose and criticality (e.g. accounting systems, sensitive data).	Annex A 8.20	Article 21 (2) (e)	Article 9 (4) (b)	N/A Doesn't explicitly mandate network segmentation. Aligns with DFS's secure network design and access control. Entities can choose different strategies to meet the requirements.
Secure Development Life Cycle Establish and apply rules for the secure development of software and systems. This should include live testing during development and any third parties involved should be considered.	Annex A 8.25 A 8.28 A 8.29 A 8.30	Article 21 (2) (e), (d)	CHAPTER IV Places significant emphasis on vendor management, encompassing this aspect as well.	Section 500.8, 500.5, 500.11
System Hardening Remove all unnecessary services and features from all used technologies, especially if they are remotely accessible. Restrict and harden the remaining services on a technical level to be as restrictive as possible (service hardening, attack surface minimization).	Annex A 8.27 A 8.20 A 8.9	Article 21 (2) (e)	N/A	Section 500.18

TECHNICAL CONTROLS	ISO27001	NIS2	DORA	DFS
Deploy Technical Solutions to Protect Systems, Data and Communication Email and messaging Shared and cloud storage Network and Internet traffic	N/A	Article 21 (2) (j)	N/A	Section 500.7 500.12
Software Asset Management Develop a comprehensive understanding of software applications and licenses and their impact on business operations and compliance requirements.	N/A	Article 21 (2) (e)	Article 5 (2) (h), (i)	N/A Doesn't explicitly require comprehensive software asset management or detailed license compliance tracking; elements of software application management, especially regarding their security and associated risks, are implicitly required by the regulation.

Chapter 3
How Reversec can help

Let's meet all your compliance requirements together.

Our security and risk management experts are experienced in assessing and implementing a wide range of security standards and regulations. We provide hands-on support to organizations of all sizes, helping you meet regulatory requirements through:

- **Regulatory Assessment and Current state analysis**: Evaluate your current security posture and identify areas needing improvement.
- **Customized Compliance Roadmap**: Develop a tailored plan to achieve compliance based on your specific needs.
- **Implementation Support**: Assist in executing necessary security controls and IT improvements.
- **Risk Management and Cybersecurity Strategy**: Create a robust strategy to manage cyber risks and align with regulatory demands.
- **Employee Training**: Educate your staff on regulatory requirements and best practices.
- **Continuous Testing, Monitoring, and Improvement**: Ensure ongoing compliance and adapt to new threats and regulations.
- **Audit Preparation and Support**: Help you prepare for audits and provide support during the process.

> Regulations can mandate that policies be built. But there's no regulation on Earth that can mandate that teams actually read and understand them.

REVERSEC

Reversec.com