NIS2 & DORA

Are You Prepared for The Two EU Legislative Instruments?

Two dynamic EU legislations are coming soon.
How can organizations be proactive and pragmatic in their adoption to become compliant?

Table of Content

Introduction

In 2024, the world has become increasingly polarized through geopolitical conflicts, wars in multiple regions and is faced with an ever-evolving cyber threat landscape turbocharged through the emergence of AI. In this complex digital world, cyberattacks have become a daily occurrence for most organizations, and protecting critical infrastructure has become ever more challenging.

According to the World Economic Forum (WEF) **Global Cybersecurity Outlook 2024**,

29%

of organizations reported that they had been materially affected by a cyber incident in the past 12 months.

54%

of organizations are unaware of the cyber vulnerabilities in their supply chain.

64%

of executives who believe their organization's cyber resilience is sufficient still lack an adequate understanding of their supply-chain cyber vulnerabilities.

In response to evolving cyber threats, the EU has issued two new directives that directly address cyber resilience in organizations. The NIS2 Directive and the DORA Regulation play significant roles, each bringing profound changes that will significantly alter the European cybersecurity landscape.

As cybersecurity leaders, understanding the nuances of the NIS2 Directive and DORA Regulation is essential to improving your organization's cybersecurity resilience and staying compliant.

Network and Information System 2 (NIS2)

The NIS2 Directive, an EU-wide cybersecurity legislation effective from 2023, aims to harmonize and strengthen ICT network and information security in critical sectors across EU member states. It broadens the scope of applicability to additional sectors such as public electronic communications networks, digital services, waste management, postal services, and the manufacturing of critical products like medical devices and chemicals. The directive mandates enhanced cybersecurity measures, such as risk analysis, incident response, encryption, vulnerability disclosure, threat detection, and training.

To whom does NIS2 apply?

NIS2 applies to all medium and large companies offering regulated services, including ICT system operators and organizations in the banking and financial services, energy, health, water, and transportation sectors.

NIS2 Pillars

- IT Governance & Risk Management
- Cybersecurity Policies & Procedures
- Technical & Operational Measures
- Compliance with Legal & Industry Standards
- Security Technologies & Solutions
- Technical Compliance & Certifications
- Reporting & Communication
- Human Resources & Training

NIS2 Pillars – Detailed Compliance Checklist

NIS2 mandates stricter requirements for risk management, incident reporting, and supply chain security. Use the checklist to ensure compliance, build resilience, and prevent disruptions.

1. IT Governance and Risk Management

Under the NIS2 directive, institutions are required to define organizational goals and risk management strategies to assess third-party risks, assign clear roles and responsibilities, and continuously monitor and review cybersecurity measures to ensure compliance.

2. Cybersecurity Policies and Procedures

Organizations need to ensure cybersecurity policies are properly documented, communicated, and evaluated and have policies for incident handling, asset management, and maintenance of IT infrastructure in place. They must also have incident response plans in place, ensure supply chain security, and establish backup management and recovery plans.

3. Technical and Operational Measures

NIS2 encourages organizations to implement basic cyber hygiene practices, conduct regular cybersecurity training, focus on robust vulnerability handling, encrypt data to protect sensitive information, and deploy robust endpoint protection and network and information security measures to prevent unauthorized access and attacks.

4. Compliance with Legal and Industry Standards

Align cybersecurity risk management measures with relevant European and international standards such as NIST, ISO 27001, CIS, & MITRE ATT&CK etc., to strengthen cybersecurity posture.

5. Security Technologies and Solutions

Organizations must have comprehensive security solutions like SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and UEBA (User and Entity Behavior Analytics) to ensure compliance with industry standards. They must also secure and continuously monitor cloud environments to prevent breaches or cyberattacks.

6. Technical Compliance and Certifications

NIS2 mandates the use of multi-factor authentication, secure communication systems, and ensure compliance with relevant European international standards such as ISO 15408 for technology security and ISO 27001 for information security management.

7. Reporting and Communication

Efficiently detect and report major incidents to authorities and stakeholders, following established protocols. Automate reporting wherever possible.

8. Human Resources and Training

Organizations will provide appropriate and proportional cybersecurity training, ensure effective human resources security, implement effective asset management and access control policies.

Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act, or DORA, is a European Union (EU) regulation that will become applicable from January 2025, to create a binding and comprehensive ICT risk management framework to establish and enforce technical standards on financial entities and their critical third parties.

What makes DORA novel is that, until now, the EU has not regulated the ICT risk management of the financial sector but has general directives and guidelines such as European Banking Authority's on ICT and Cybersecurity risk management. With DORA, EU has harmonized the rules relating to ICT risk management and operational resilience for financial entities across all member states.

To whom does DORA apply?

DORA applies to all financial entities, including banks, insurance service providers, and their critical third-party ICT service providers.

Critical suppliers of banks will feel effects under DORA. But even if your company is not considered critical, you will most likely still be subject to DORA indirectly — the contractual terms that DORA imposes on financial institutions will trickle down toward most of the service providers of financial institutions.

DORA regulation also extends to suppliers outside the European Member States; for example, a North American technology provider will still be subject to DORA if it provides services to European banks.

DORA Pillars

ICT Risk Management

ICT Incident Reports

Digital Operational Resilience Test

ICT Third-party Risk Management

Information Sharing

DORA Pillars – Detailed Compliance Checklist

More than a standalone regulation, DORA is a holistic regulation set out to achieve a high common level of digital operational resilience that requires organizations to collaborate across multiple teams to set up an appropriate governance controls to managing the overall ICT risk. The below checklist will enable organizations to prepare for compliance –

1. ICT Risk Management and Governance

DORA focuses on implementing a well-structured system for ICT risk management and detection. Institutions are expected to take a proactive approach to their overall digital operational resilience strategy and develop comprehensive security policies. The pillar also mandates continuous testing and monitoring to ensure the effectiveness of the implemented measures.

2. Incident Response and Reporting

Institutions are expected to report all major incidents to better understand the ICT risk landscape across the union and to encourage a coordinated response. Organizations must maintain appropriate cybersecurity measures for cyber threat identification, protection, detection, response, and recovery, establish communication protocols, conduct proper post-incident analysis, and ensure compliance in incident reporting.

3. Digital Operational Resilience Testing

DORA mandates regular testing and risk assessments against various types of ICT disruptions to bolster ICT defenses. Organizations need to maintain detailed documentation and establish processes for continuous improvement.

4. Third-party Risk Management

DORA introduces a more streamlined approach to vendor assessments and third-party risks. Organizations are required to establish due diligence processes, including security obligations in contracts, monitoring and auditing third-party vendors, coordinating incident responses, and staying aligned with regulatory requirements.

5. Information and Intelligence Sharing Arrangements

DORA encourages institutions to collaborate and share cyber threat and vulnerabilities intelligence and develop data-sharing protocols to identify emerging threats. This will foster a collective defense strategy and boost sector-wide resilience.

Frequently Asked Questions

1. Why is the EU enacting NIS2 & DORA now?

NIS2 and DORA are the European Union's responses to the rising cyberattacks targeting the finance, electricity, oil, and gas sectors. Although NIS2 and DORA do not specify cybersecurity controls, they do define the governance framework that entities like banks and utility providers must implement.

These frameworks aim to enhance cyber-resilience by ensuring the presence of a robust management framework rather than prescribing specific information systems security measures such as encryption.

2. What does the regulatory impact of DORA and NIS2 look like for enterprises?

Larger enterprises must focus more on cybersecurity governance, ensuring they have policies and procedures to address cybersecurity risks. This includes defining security responsibilities and auditing their supply chain. Under NIS2 and DORA, enterprises must review their suppliers from a security perspective and mandate sanctions in case of non-compliance.

For NIS2, penalties can reach 10 million euros, while DORA penalties have yet to be defined by national governments. The financial regulators at the European level—the EBA—are involved in the actual administration of penalties.

3. What are the main differences between DORA and NIS2?

NIS2 is a directive that sets general rules and objectives for all EU countries, which must create laws to achieve these goals. Whereas DORA is a regulation directly applicable and enforceable in all EU member states, without needing individual country to enact specific laws.

Although DORA and NIS2 are designed to ensure cyber security resilience, they serve different purposes.

- The purpose of NIS2 is to harmonize more broadly the level of cyber security in the EU.
- The purpose of DORA is to protect the financial sector and ensure operational resilience, reliability of digital systems, and the availability and integrity of financial services.

According to DORA, NIS2 still applies to the subjects of DORA, but the overlap of NIS2 and DORA is prevented by the lex specialis provision in DORA, which means financial institutions need to be well informed about the requirements under both legal acts.

Both regulations prioritize the supply chain, requiring software suppliers to actively participate in risk management and the assessment of operational stability.

How does an organization prepare for these legislatives?

Only a pragmatic approach that addresses digital risks and gaps can help organizations keep up with the new regulations and their likely impact. We've summarized a few key actions organizations must take to prepare for NIS2 and DORA:

Collaboration between small and large companies: Due to the current landscape of interconnectivity and interdependencies, collaboration is essential for organizations of any size to prepare for the upcoming changes. Large organizations impacted can support smaller organizations. Collaboration must occur not only among peers but also with partners and vendors.

Know your organization: Achieving and maintaining compliance can be expensive and time-consuming. So, organizations need to know their digital ecosystem and identify critical processes, services, and assets. Maintain a comprehensive asset inventory for security and compliance efforts, risk assessments, and security policies.

Perform compliance gap analysis: Organizations must perform a gap assessment on DORA and NIS2 to identify areas for improvement and risks and map the gaps against the risk landscape.

- **Have a robust vulnerability management process:** Perform continuous vulnerability scans to detect, prioritize, and respond to risks based on their criticality.
- **Make mindful investments:** Focus on investments that add value to Regulation and Directive requirements to achieve seamless compliance.

Both frameworks extend their reach to third-party ICT service providers, including cloud services, which are integral to financial entities' operations. As it pertains to the cloud, the dynamic instruments specify that financial entities should use multi-cloud approaches to improve resiliency.

Due to varied technology, multi-cloud strategies can indirectly create other security gaps. This approach necessitates that appropriate unified controls and monitoring are implemented to ensure that those security gaps aren't exploitable.

How letsbloom can help you ensure compliance?

With stricter compliance controls and breach disclosures, new regulations are transforming cyber risk management in Europe. If you're feeling overwhelmed, letsbloom can help. Designed to prepare enterprises against upcoming risks, rewards, and responsibilities, letsbloom's comprehensive platform can help you effortlessly align with the stringent standards of NIS2 and DORA.

1. Get instant visibility of your cloud environment, application, and workload communication.

Third-party risk assessment is critical to ICT risk management. Letsbloom offers comprehensive controls for Cloud environments (public, private and hybrid), Kubernetes, and compliance posture management. Our pre-built controls and multi-layer security ensure data availability, authenticity, integrity, and confidentiality, achieving high digital operational resilience. Any cloud, any workload, for any regulation – get comprehensive compliance observability in minutes and at scale. Letsbloom's unified cloud compliance platform enables cloud risk reduction and threat detection to ensure organizations meet all regulatory requirements efficiently.

2. Compliance gap analysis and implementation

Our platform analyses your existing processes, applications, and technical controls in the context of relevant rules, proposes an remediation roadmap that considers the context of your organization readiness, processes, and technology landscape for effective implementation.

3. Manage vulnerabilities with regular risk assessments.

Businesses must conduct regular risk assessments to identify and evaluate vulnerabilities in their cloud services to meet the relevant requirements. Letsbloom platform allows you to scan your clouds and workloads to uncover vulnerabilities and provides a detailed tactics breakdown against the MITRE ATT&CK framework that helps you conduct threat-led prioritization and perform a single click or automated remediation.

4. Implement strong preventive measures and tighter controls.

Our platform delivers context-specific-actionable-intelligence (CSAI) using pre-built patterns with infrastructure-as-code, policy-as-code, compliance-as-code, and controls-as-code. This can help you safeguard against prevalent risks in cloud applications, such as misconfigurations, exposed secrets, and vulnerabilities within cloud settings, containers, and Kubernetes clusters.

Continous Monitoring to identify and respond to incidents quickly

Identify, Priortize, Manage, Repond to risks based on criticaltiy

Instant Compliance Observability against DORA and NIS2 as well as CRA frameworks

Pre-built patterns with infrastructure-as-code, policy-as-code, compliance-as-code, controls-as-code.

Summary

DORA and **NIS2** mandate significant changes for organizations from an ICT risk management perspective and therefore organizations must start to prepare for these upcoming tasks on priority.

Like the GDPR, the provided penalties — particularly the fines — should encourage many players to pay special attention to how they apply and respect these new constraints.

Getting ready for DORA and NIS2 is a regulatory requirement and an opportunity for businesses to bolster stability and security, mitigate critical cyber risks, and improve operational resilience in an increasingly complex and interconnected digital world.

In a world drowning in data, changing regulations, and ever-increasing vulnerabilities, we make staying compliant and secure effortless!

Learn more about letsbloom compliance solutions and how we can prepare you for the upcoming changes.

Reach out to get a personalized demo.

Contact us at info@letsbloom.io

letsbloom