Unravelling European Regulations:

Everything You Need to Know about DORA and NIS2

getronics

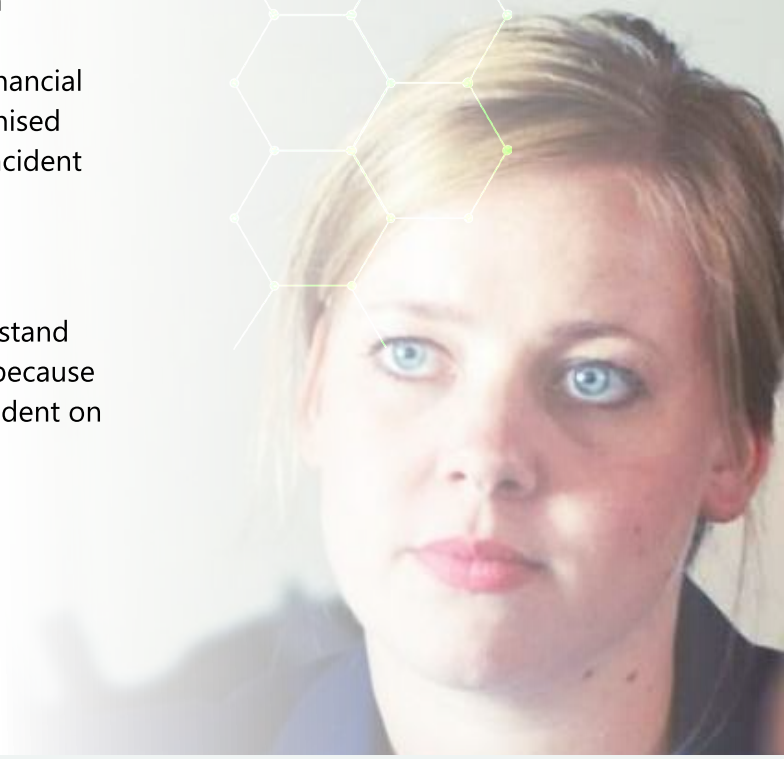
In today's digital age, operational resilience and cybersecurity are two fundamental pillars for any organisation. The Digital Operational Resilience Act (DORA) and the NIS2 Directive, relate to networks and information systems, addressing both issues within the European Union's cybersecurity strategy.

Adopting the European DORA and NIS2 regulations is not only a matter of legal compliance but also an opportunity to strengthen your company's market position, protect your assets, and build a relationship of trust with your customers.

What is the DORA Regulation?

The European Council adopted the DORA regulation in November 2022 with the aim of consolidating and standardising the digital operational resilience of EU financial entities against cyberattacks. DORA establishes harmonised and rigorous requirements for ICT risk management, incident reporting, digital operational resilience testing, and information-sharing agreements.

This regulation aims to strengthen the capacity to withstand and recover from operational disruptions, particularly because the financial sector is highly interconnected and dependent on ICT, making it more vulnerable to cyber risks.



What is the NIS2 Directive?

The NIS2 Directive, which succeeds the original NIS Directive, expands and strengthens security and incident reporting obligations for operators of essential services and digital service providers. NIS2 extends its coverage to more sectors and requires stricter technical and organisational measures to protect against cyberattacks.

This regulation aims to better defend essential entities against supply chain vulnerabilities, ransomware attacks, and other cyber threats.

getronics

Why Do I Have to Comply with DORA and NIS2?

Complying with these regulations is not only a legal obligation for affected entities in Europe but also protects critical infrastructures against disruptions and cyberattacks, minimising the risk of economic and reputational losses.

Which Sectors are Affected by DORA and NIS2?

DORA

- Financial institutions, companies offering consumers financial products or services such as loans, financial or investment advice, payment processing, or insurance.
- Their critical ICT service providers, such as cloud platforms or data analysis and protection services.

NIS2

The number of sectors affected has been expanded. Now, it not only applies to organisations operating within the new definition of 'critical' (and their employees), but also service providers and subcontractors offering the same services.

bold text > high criticality

Energy	Public administration
Transport	Space
Banking	Postal and courier services
Financial market infrastructures	Waste management
Healthcare	Manufacturing, production, and distribution of substances and chemical mixtures
Drinking water	Food production, processing, and distribution
Wastewater	Manufacturing
Digital infrastructure	Digital service providers
Business-to-business ICT service management	Research

When Do DORA and NIS2 Come Into Effect?

The **DORA** regulation will come into effect on **17th January 2025**, while **NIS2** came into effect on **27th December 2022**, following its publication in the Official Journal of the EU. However, member states have until **17th October 2024** to adopt it.

What Are the Implications for My Business?

DORA requires financial entities, investment firms, insurance companies and intermediaries, fintechs, cryptocurrency/crypto-asset management firms, and pension funds to do the following:

- Establish a process for managing ICT-related incidents to detect, manage, and report incidents.
- Classify ICT incidents and determine their impact using criteria such as the number of transactions or customers affected, reputational impact, incident duration, and more.
- Report incidents to relevant authorities.
- Be prepared to react quickly and effectively to these incidents.

NIS2 expands the obligations of the original NIS Directive, and although the specific details of NIS2 are still being developed, organisations are expected to:

- Maintain an ICT risk management framework.
- Develop security policies and backup and recovery procedures.
- Implement mechanisms to detect and respond to anomalous ICT activities.

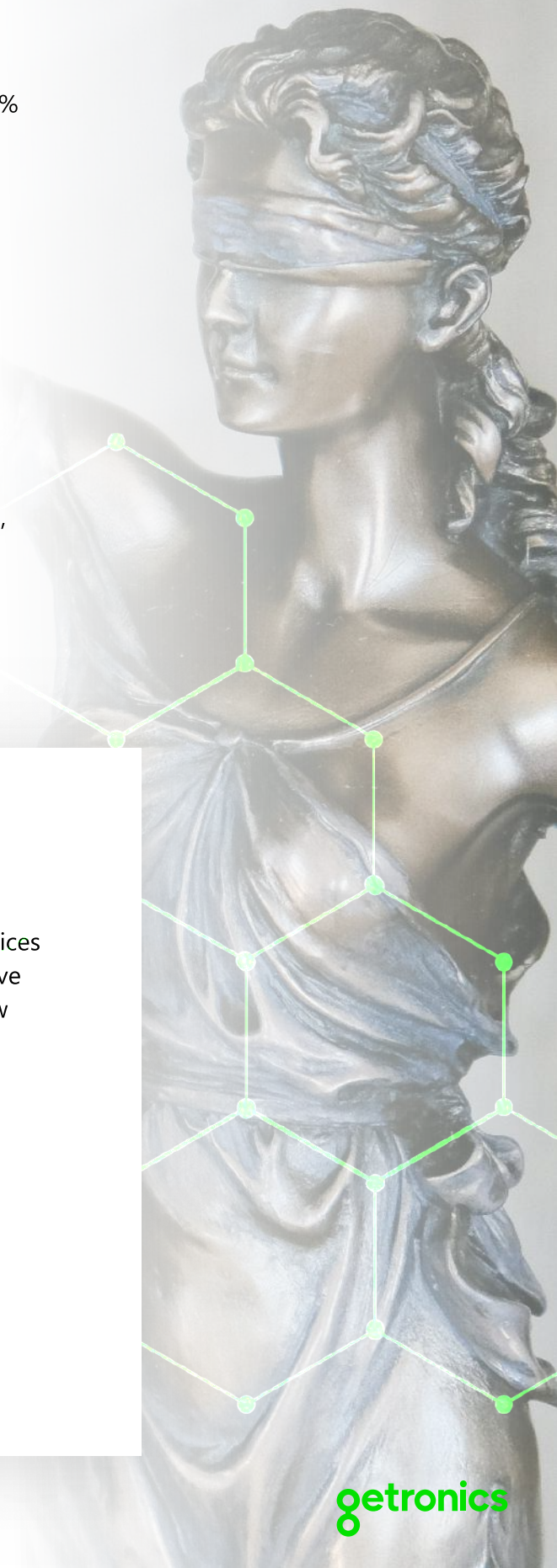
getronics

What Happens if I Don't Comply with the Regulation?

Non-compliance with DORA and NIS2 regulations can result in severe penalties.

Penalties for non-compliance can reach up to €10 million or 2% of the total annual global turnover. In very serious cases, authorities may order the suspension of operations until security requirements are met. Organisations may also be required to undergo security audits to ensure ongoing compliance with NIS2 requirements.

As for DORA, while it states that penalties for non-compliance should be effective, proportionate, and dissuasive, it does not specify the exact types of penalties or fine amounts. Sanctions can include corrective measures and in serious cases, the withdrawal of authorisation to operate. Additionally, management teams can be held personally liable for breaches, highlighting the importance of proper governance and effective ICT risk control.



But Where Do I Start?

The first step is to implement robust policies and best practices that cover all dimensions of cybersecurity. If you already have them defined, now is the time to conduct a thorough review and see if they comply with the standards.

The three-lines framework offers a clear structure for risk management and regulatory complianceDividing specific responsibilities among business areas, risk management & compliance, and internal audit.

getronics

INFOGRAFY:

Risk Analysis and Information Systems Security:

- Secure the supply chain
- Zero Trust Access: Who can be trusted to access my systems?
- Data protection and cryptography
- Backups - I've been attacked! What should I do now?
- Comprehensive incident and crisis management
- Basic cyber hygiene practices and cybersecurity training

Securing the Supply Chain

The first step is to identify and address the weakest link in the supply chain. This requires establishing continuous monitoring processes to identify and manage any issues that may arise with third-party services, as well as continuous improvement action plans.

It's important to have a multi-vendor and multi-platform partner that helps you find the technology that best suits your needs and core business.

By controlling all levels of the supply chain ,throughout the lifecycle of your systems you can avoid risks of business continuity disruption, and always ensure the best service to your end customers.

Lastly, don't forget to establish procedures for installation, patch management, regular security updates, and operational resilience testing. Security requires continuous work and updates, validated through independent company audits to ensure proper functioning.

Zero Trust Access: Who can be trusted to access my systems?

Adopting a Zero Trust access model, including multi-factor authentication and continuous verification, is vital to protect your information. Security policies and staff training, access control, and asset management will prevent attackers from accessing your information, but at what cost? It is important to have a provider that not only protects your business from unwanted visitors but does so without interfering with its performance and agility.

Data Protection and Cryptography

Data encryption is essential to ensure the confidentiality, integrity, and availability of sensitive information. It protects data against unauthorised access and security breaches, ensuring compliance with DORA and maintaining the trust of your customers and partners. With these Thales solutions, you can ensure that only authorised users can access the information and that it remains secure at all times:

- **CipherTrust Data Discovery and Classification:** identifies structured and unstructured sensitive data both on-premises and in the cloud. Uses built-in templates for quick identification of regulated data, highlights security risks, and helps discover compliance gaps.
- **CipherTrust Transparent Encryption:** offers data-at-rest encryption for files and folders, as well as access control for privileged users. Protects data on-premises, in the cloud, and in big data and container environments.
- **CipherTrust Tokenization:** enables the pseudonymisation of sensitive information in databases, maintaining the ability to analyse aggregated data without exposing sensitive information during analysis or in reports.
- **High-Speed Encryptor (HSE):** offers independent network data encryption, ensuring that data, videos, voices, and metadata are secure while transferring from site to site, or from on-premises to the cloud and vice versa.
- **OneWelcome Identity & Access Management:** limits internal and external user access based on their roles and context with granular access and authorisation policies that ensure the right user has access to the right resource at the right time.
- **OneWelcome Consent and Preference Management:** allows organisations to collect consumer consent, offering clear visibility of consented data and managing access to the data they are authorised to use.
- **SafeNet Trusted Access:** enables multi-factor authentication with a wide range of methods and forms, allowing customers to address numerous use cases, security levels, and threat vectors with unified policies.
- **Luna HSMs:** protects cryptographic keys and provides a hardened, tamper-resistant hardware security module for secure cryptographic processing, encryption, key protection, and generation, among others.
- **CipherTrust Enterprise Key Management:** optimises and strengthens key management in cloud and on-premises environments for internal encryption and third-party applications.
- **CipherTrust Cloud Key Management:** reduces third-party risks by keeping the keys that protect sensitive data hosted by external cloud providers under the financial institution's full control.

Backups - I've been attacked! What should I do now?

The question is not ***if*** I will be attacked, but ***when*** I will be attacked. We know that protecting ourselves is a basic part of our security policy, but what happens when my defences fall?

At this point it is crucial that properly encrypted information does not pose a threat. It is also important how quickly you can recover and return to business as usual.

Therefore, you must ensure that robust and certified backup systems are in place for disaster recovery. Consider using advanced backup solutions, such as those offered by Teradata or Infinidat. This can help ensure that backups are not only performed regularly but are also quickly recoverable and secure.

Comprehensive Incident and Crisis Management

Plan: Develop a crisis management plan covering the detection, response, and timely notification of any security event.

Analyse: After receiving and resolving an attack, focus on forensic analysis of the situation: What happened? How did they get in? What can we do to prevent it in the future? How can we improve recovery? etc.

Report: Creating a crisis management protocol will help you report your analyses of received attacks and responses as required by the regulations.

Basic Cyber Hygiene Practices and Cybersecurity Training:

Technology is key to preventing attacks, but it's important to remember that 95% of security breaches are due to human errors. Therefore, you should not underestimate good cyber hygiene practices, ensuring your employees are well-trained in cyber hygiene. This way they can recognize and avoid threats themselves.

How Can Getronics Help You?

As a provider of **ICT services** to companies affected by these two European regulations, **Getronics** is obliged to comply with them and have a contingency and business continuity plan.

This allows us, either with our own resources or through partners, to offer services and products focused on regulatory compliance and to have proven expertise in the area. Combined with our sectoral knowledge, we can help you adapt to the regulations, ensuring business continuity without loss of efficiency.

- **Audit:** We analyze risks both internally and in the software supply chain. We are vendor-agnostic for both hardware and software, seeking the greatest benefit for you (Dell, HP, SAP, Salesforce, etc.).
- **Training and Awareness:** We provide training and awareness for workers on security, and develop protocols and best practices.
- **Reporting:** Using machine learning and AI techniques, we can perform predictive analysis and create dashboards. In case of a real attack, we could perform forensic analysis and issue reports for the regulator.
- Implementation of **Zero Trust Tools** (Cloudflare), PAM...
- Backup Systems: Ensuring business continuity through our extensive partner network, always looking for the best fit for your business.
- **Secure Cloud Services:** Public, private, and hybrid cloud design, analysis, and auditing.
- Securing **Workplace Services**.

You can count on us as your primary cybersecurity partner. We have our own SOC in Barcelona, are CERT/CSIRT, and through our partners, we offer a comprehensive cybersecurity solution.