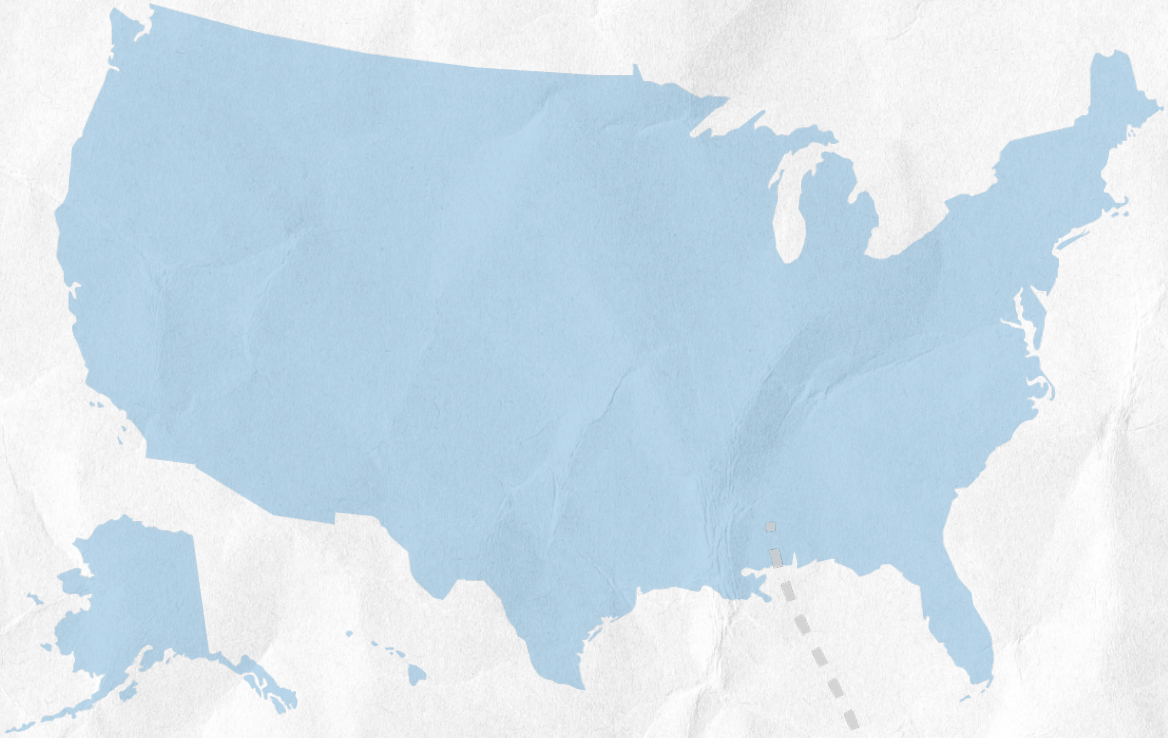


NIS2 & DORA:
Critical Compliance for U.S.

Prepare Your Company for the New Regulatory Landscape

Idera, Inc.

INDEX

Overview.....1

Introducing NIS2 and DORA.....2

What Is NIS2?.....2

What Is DORA?.....5

What are the Consequences of Non-Compliance?.....7

How Should U.S. Businesses Prepare for NIS2 and DORA?.....9

PreEmptive, Kiuwan, and Ranorex Equip U.S. Businesses for DORA and NIS2 Compliance.....10

Overview

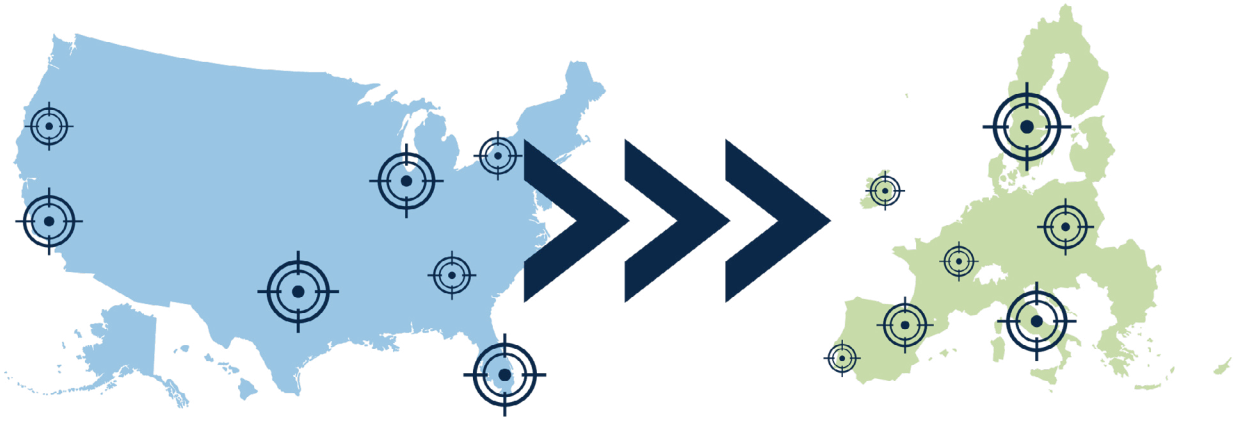
Two new significant regulations, Network and Information Security 2 (NIS2) and the Digital Operational Resilience Act (DORA), are set to take effect in early 2025. These regulations, although implemented by the European Union, will have implications for U.S. companies, especially those doing business in the EU or providing services to EU-based entities.

NIS2 aims to ensure a high level of cybersecurity across the EU by requiring essential and important entities to implement robust security measures. This directive impacts sectors such as energy, transportation, health, finance, and digital infrastructure.

DORA focuses specifically on the financial sector, mandating comprehensive digital operational resilience to safeguard against ICT-related risks. Financial institutions, including banks, investment firms, and insurance companies, must adhere to stringent risk management and cybersecurity practices.

For U.S. companies, compliance with NIS2 and DORA is not optional if they operate within or offer services to the EU. Failure to comply can result in severe penalties, making it crucial for affected businesses to understand and prepare for these regulations.

This ebook provides detailed insights into NIS2 and DORA, outlining their purposes, requirements, and the steps U.S. companies need to take to ensure compliance. By understanding these regulations, businesses can better protect themselves from cyber threats and avoid substantial fines.



Introducing *NIS2* and *DORA*

NIS2 and DORA were introduced as part of the European Union's ongoing efforts to enhance cybersecurity and digital resilience across its member states. The increasing frequency and severity of cyberattacks prompted the EU to develop more robust frameworks to protect critical infrastructure and financial systems.

- NIS2 builds on the original Network and Information Systems Directive (NIS), expanding its scope and strengthening its requirements to address the evolving cybersecurity landscape. Its goal is to ensure a high common level of cybersecurity across the EU by harmonizing measures and procedures.

- DORA was conceived in response to the growing digitalization of the financial sector and the need for comprehensive regulation to manage ICT-related risks. It aims to create a unified approach to digital operational resilience, ensuring that financial entities can withstand, respond to, and recover from cyber threats.

These regulations represent a significant step forward in the EU's commitment to safeguarding its digital economy and ensuring the security and stability of its member states' infrastructures.

What Is *NIS2*?

NIS2, the Network and Information Security Directive 2, is a significant regulatory framework established by the European Union to enhance cybersecurity across its member states. It aims to ensure a high level of security for network and information systems critical to the EU's functioning. The directive builds on its predecessor, the original NIS Directive, by expanding its scope and strengthening its requirements.

What Do U.S. Businesses Need to Know About NIS2?

Given the global nature of today's digital economy, NIS2 has implications that extend beyond the borders of the EU. U.S. businesses offering services within the EU or interacting with EU-based entities must take note of NIS2 compliance requirements.

Understanding the Scope of NIS2

NIS2 aims to ensure a high level of cybersecurity across the EU by categorizing entities into two main groups: essential (critical) entities and important entities. These categories determine the level of supervision and requirements for cybersecurity measures.

To qualify as an essential entity, an institution must fall within one of two annexes outlined in the NIS2 directive. These annexes define the sectors that pose the most significant risk to the stability of the EU if they suffer a crippling cybersecurity incident.

Annex 1 (**Critical Entities**) Includes:

- Transportation
- Health
- Drinking Water
- Space
- Financial Services Market Infrastructure
- Banking
- Digital Infrastructure
- Waste Water
- ICT Service Management
- Digital Service Providers

Annex 2 (**Important Entities**) includes:

- Postal/Courier Services
- Food
- Waste Management
- Digital Providers
- Manufacturing
- Chemical Manufacturing

The EU categorizes businesses by size, influencing whether a business is labeled as essential. The classifications are:

Large Enterprises:

Businesses with ***€50m+ annual revenue*** and 250+ employees

Medium Enterprises:

Businesses with ***€10m+ annual revenue*** and 50+ employees

Member State Selection:

Any enterprise explicitly chosen in a ***given Member State's transposition*** of NIS2 guidelines (based on an entity's risk profile)

These classifications help businesses understand their obligations under NIS2.

If a business falls under an Annex 1 sector and qualifies as a large enterprise, it is labeled as "Essential," meaning it's subject to proactive supervision, such as routine monitoring by representatives of an EU Member State. These representatives monitor activity to ensure the company meets the specific cybersecurity guidelines of the member state.

In contrast, a business may fall under Annex 1 but qualify as a medium enterprise, classifying it as "Important." In this case, the company must still follow the same guidelines but faces reactive monitoring. Authorities only get involved after an identified instance of non-compliance, rather than through routine or random checkups.

What Measures Must Essential and Important Entities Adhere to?

The specific measures that companies must implement to comply with NIS2 will be finalized after each EU Member State transposes the directive into national law. However, the directive outlines an "all-hazards approach" to cybersecurity, which encompasses the following areas:

- **Risk Analysis and Information System Security Policies:** Implementing thorough risk assessments and establishing robust security policies.
- **Incident Handling Policies:** Developing procedures for effective incident response and management.
- **Business Continuity Protection:** Ensuring backup management, disaster recovery, and crisis management plans are in place.
- **Supply Chain Security Policies:** Managing security between direct suppliers and service providers.
- **Network Security, Development, and Maintenance:** Ensuring the security and resilience of network infrastructure.
- **Cybersecurity Risk-Management Measures:** Conducting regular procedures, assessments, and training to manage cybersecurity risks.
- **Cryptology and Encryption Policies:** Implementing strong encryption practices to protect sensitive data.
- **Access Control Policies and Asset Management:** Ensuring secure access controls and effective management of digital assets.
- **Multi-Factor Authentication Solutions:** Utilizing multi-factor authentication to enhance security.

When Does NIS2 Go Into Effect?

The NIS2 directive mandates that EU Member States complete the transposition of NIS2 into national law by October 17th, 2024. These national laws will take effect in January 2025, requiring corporations to implement the specified policies outlined in their respective Member State's transposition of NIS2. Subsequently, each Member State is responsible for compiling a database of essential entities and conducting bi-annual updates to ensure ongoing compliance.

What Is *DORA*?

DORA, the Digital Operational Resilience Act, is a comprehensive piece of legislation enacted by the European Union to regulate ICT and cybersecurity practices within the financial sector. Unlike directives such as NIS2, which require transposition into national laws, DORA is a regulation that applies uniformly across all EU member states.

DORA serves two primary objectives:

1. **Strengthening Risk Management:** Equipping financial sector businesses with technologies and services to enhance risk management and mitigate vulnerabilities along the ICT supply chain.

2. **Standardizing Regulations:** Creating a unified set of regulations and rules that apply evenly throughout the European Union, ensuring consistency and clarity in the financial sector's cybersecurity practices.

The European Banking Authority (EBA) previously issued guidelines for ICT and security risk management. However, these guidelines led to inconsistent application across financial institutions and lacked specific technical solutions. DORA addresses these shortcomings by:

- Centralizing rules and establishing clear, enforceable guidelines.
- Outlining a framework for monitoring and holding financial institutions accountable.
- Mandating the creation of safety policies, holistic risk management plans, and mandatory ICT incident reports.
- Requiring disaster recovery planning, resilience testing, and risk management for ICT third parties.

What Do U.S. Businesses Need to Know about DORA?

Similar to GDPR and NIS2, DORA has extraterritorial implications. Any U.S. business interacting with or providing services to EU financial entities must comply with DORA's requirements or face significant penalties. This includes companies offering third-party services to EU financial institutions.

Additionally, if a business provides certain third-party services to EU financial institutions, it's also subject to the same regulations and penalties.

In terms of timing, just like EU institutions, all EU and EU-related institutions and ICT third parties must demonstrate their resilience capabilities for digital planning, testing, and disaster recovery on January 17th, 2025.

Understanding the Scope of DORA

DORA's scope is comprehensive, encompassing nearly all entities operating within the financial sector. These entities are required to adhere to the stringent cybersecurity and operational resilience measures outlined in the regulation, ensuring they are well-prepared to manage and mitigate ICT-related risks. Article 2 of DORA details the entities affected by the new regulations. Here is an abridged list of the 21 types of entities impacted:

- **Credit and Payment Institutions:** Including those exempted under Directive (EU) 2015/2366.
- **Account Information Service Providers**
- **Electronic Money Institutions:** Including those exempted under Directive 2009/110/EC.
- **Investment Firms**
- **Crypto-Asset Service Providers:** And issuers of asset-referenced tokens.
- **Central Securities Depositories and Counterparties**
- **Trading Venues and Repositories**
- **Managers of Alternative Investment Funds**
- **Management Companies**
- **Data Reporting Service Providers**
- **Insurance and Reinsurance Undertakings**
- **Insurance Intermediaries:** Including reinsurance intermediaries and ancillary insurance intermediaries.
- **Institutions for Occupational Retirement Provision**
- **Credit Rating Agencies**
- **Administrators of Critical Benchmarks**
- **Crowdfunding Service Providers**
- **Securitization Repositories**
- **ICT Third-Party Service Providers**

Ultimately, the list is comprehensive enough to assume that any legal financial entity is expected to adhere to these new laws.

When Does DORA Go Into Effect?

The Digital Operational Resilience Act (DORA) was officially published in October 2022. This publication provided financial institutions ample time to implement the necessary changes to achieve full compliance. The key dates to note are:

Publication Date:
October 2022

Full Compliance Deadline:
January 17, 2025

By January 17, 2025, all relevant entities must demonstrate their adherence to the regulations set forth by DORA, ensuring their digital operational resilience. One year after this deadline, the European Union will review the effectiveness of the implementation, assessing how well the regulations have met their intended goals and identifying areas for further improvement.

What Are the *Consequences* of Non-Compliance?

Failure to comply with DORA or NIS2 can result in severe penalties. EU Member States have dedicated regulators, known as “competent authorities,” to monitor compliance. Depending on the entity type, a company might be subject to proactive or reactive monitoring. These regulators are responsible for investigating infringements, issuing remedies for disaster relief, and imposing administrative and criminal penalties on non-compliant businesses.

Both NIS2 and DORA impose steeper penalties than previous regulations like the first iteration of NIS and GDPR. Companies should anticipate increased efforts from EU authorities to monitor and track violations.

Penalties for NIS2 Non-Compliance

For businesses failing to comply with NIS2, the following penalties may apply:

Essential Entities:

- Maximum fine of up to 10,000,000 Euros or 2% of annual turnover.

Important Entities:

- Maximum fine of up to 7,000,000 Euros or 1.4% of global annual turnover.

Additional punishments can include administrative fines and even criminal sanctions. The stringent penalties reflect the EU's commitment to ensuring robust cybersecurity measures across essential and important entities.

Penalties for DORA Non-Compliance

Similarly, non-compliance with DORA can lead to significant penalties:

Maximum Penalty:

- Up to 2% of global annual turnover.
- Potential criminal sanctions.

DORA's penalties are designed to enforce rigorous cybersecurity practices within the financial sector, emphasizing the importance of digital operational resilience.

Monitoring and Reporting Requirements

Specific laws under NIS2 and DORA allow authorities to conduct onsite visits, offsite checkups, and audits for companies within the scope of these regulations. The EU can now perform random or targeted security checks and request access to data records related to cybersecurity incidents.

In addition to stricter supervision, businesses face more stringent reporting thresholds. Both NIS2 and DORA require companies to report incidents within 24 hours and submit detailed reports within 72 hours of an incident. These reports must include a robust description and identification of the root cause, along with a plan for resolving the issue.

How Should U.S. Businesses *Prepare* for NIS2 and DORA?

By ***January 17, 2025***, any business within the scope of NIS2 or DORA must demonstrate efforts to adopt policies, technologies, and strategies that ensure resilience to cybersecurity threats outlined in these regulations. To avoid non-compliance penalties, relevant businesses must first understand their relation and classification to DORA or NIS2 and begin planning accordingly. Here is a general playbook to guide U.S. businesses in their preparation:

Education and Research

Research the specific guidelines of NIS2 and DORA to learn why they exist, why they're essential, and what they are meant to change. This step is important even for entities that might not fall directly into the scope of either law.

Understand the Scope

Identify the various categories and classifications and determine precisely where the business lands. For example, it may fall within one of the related categories or belong to the third-party ICT registry. Once that's clear, take a deep dive into learning the unique requirements that apply to the business.

Take Stock and Identify Vulnerabilities

Identify all current cybersecurity assets, processes, reporting tools, and services. Conduct a security assessment to pinpoint the most significant vulnerabilities and security gaps, especially concerning NIS2 and DORA requirements. This requires a full digital inventory audit and a future audit outlining where security measures may wear down and cause future problems.

Create a Task Force

Initiate the right people by introducing them to the identified flaws. This team could include security professionals, risk managers, and auditors. This team must then build a cohesive plan to address current and future needs as the business works to close security gaps and minimize the threat footprint.

During this stage, it's critical to include and inform top management from the beginning and throughout the rest of the process. Executive management must communicate the process and developments to lower-level employees to build a culture of continuous improvement, accountability, and protection that aligns with the unfolding regulations.

Implement Legal Requirements

After fashioning a plan and bringing aboard the right people, begin rolling out the plan in phases, first with the most significant vulnerabilities. Document and report on all changes, and run audits that verify changes comply with DORA and NIS2.

Create a Structured and Lasting Process

Meeting the requirements laid out by DORA and NIS2 once isn't enough. Businesses must initiate a proactive stance towards compliance, which frequently audits existing processes to ensure that they satisfy the guidelines of existing regulations and implement tactics to future-proof processes in anticipation of new rules. A forward-thinking mindset chooses the best technologies, detailed strategies, and in-depth policies using data-driven methodologies for securing websites, mobile apps, APIs, networks, and servers.

PreEmptive, *Kiuwan*, and *Ranorex* Equip U.S. Businesses for DORA and NIS2 Compliance

The burden of cybersecurity is only getting more critical, regardless of the industry. However, following DORA and NIS2 isn't just about avoiding penalties; prioritizing security can have significant financial benefits and help prevent major economic fallout. For example, the average cost of a data breach in 2023 was **$4.45 million**, a number that doesn't even include the damage to a business's reputation. That cost can be avoided with even the most straightforward digital security plan.

As businesses navigate the brave new world of cybersecurity, it's pivotal to remember that NIS2 and DORA are merely baseline initiatives focused on helping companies fortify their digital defenses to keep hackers at bay. Yes, companies must adhere to these regulations, but they also must go above and beyond to guard every last piece of digital infrastructure.

PreEmptive stands as the standard defense against cybersecurity threats. For the best digital defense, use PreEmptive for application hardening. PreEmptive is an industry-leading, professional-grade digital protection service trusted by over 5,000 companies worldwide. Its multi-layered plans address root causes of vulnerabilities through constant runtime checks, extensive obfuscation updates, real-time attack detection, and more. With these tools, businesses can prevent tampering, reverse engineering, unauthorized debugging, and SQL injections.

Kiuwan can assist with several crucial elements, such as risk management, information and intelligence sharing in relation to cyber threats and vulnerabilities, and ICT third-party risk. Kiuwan's comprehensive solutions ensure that businesses are equipped to identify, assess, and mitigate cybersecurity risks effectively.

Ranorex plays a vital role in digital operational resilience testing. With Ranorex's robust testing framework, businesses can ensure their digital operations are resilient and can withstand cyber threats. Ranorex provides automated testing solutions that enhance the stability and security of digital infrastructures.

To make it easier, please see tables below:

NIS2 Directive	Product Offerings
Risk & Vulnerability Management (Identify, assess and understand security risks to the network and information systems supporting them)	**SAST & SCA**
Incident Reporting & Handling (Establishing plans for dealing with security breaches, Including how to detect, report, analyze and fix security breaches)	**SCA**
Supply Chain Security (Securing relationships with third-party suppliers checking and auditing security practices)	**SCA**
Cryptography & Encryption (Protecting sensitive data and communications to keep data secure)	**&**

DORA Directive	Product Offerings
Incident Reporting (Incident classification based on severity & timely reporting of details, and incident analysis)	**SAST, SCA & QA**
Operational Resilience Testing (Conduct regular testing ensuring adequate resilience against potential disruptions)	**&**
Third-Party Risk Management (Perform continuous monitoring, and implement strong governance practices for third parties)	**SAST, SCA & QA**
Information & Intelligence Sharing (Financial entities to share information regarding cyber threats & vulnerabilities in confidential, trusted networks)	**SAST, SCA & QA**

There isn't much time before companies must comply with DORA and NIS2. That's why now is the time to invest in the proper digital defense arsenal.

Explore our offerings and industry-specific solutions or request a free demo to see how PreEmptive, Kiuwan, and Ranorex can fortify your digital defenses and ensure compliance with NIS2 and DORA.

***Smart App Protection** for an Unsafe World!*

GET IN TOUCH:

www.kiuwan.com

www.preemptive.com

www.ranorex.com