Compliance Solutions for NIS2: The EU's Network and Information Systems Directive

Learn about the EU legislation affecting critical infrastructure and services and how Entrust can help.

Overview

As organizations embrace digital transformation, they face increased exposure to evolving cyberattacks and breaches. Threat actors pose significant risks to those providing critical infrastructure and services, whether motivated by financial gain or malicious state-sponsored agendas seeking to infiltrate organizations to harvest data or cause service disruptions.

In response, the European Union (EU) has introduced legislation focused on awareness, resilience, recovery, risk management, and incident reporting for essential and important industry sectors.

NIS2, the second iteration of the Network and Information Systems Directive, aims to enhance cyber resilience across the EU, particularly for operators of critical infrastructure and essential services.

ENTRUST'S COMPLIANCE SOLUTIONS

Our extensive portfolio secures identities, data, network applications, and workloads, integrating seamlessly with a broad partner ecosystem.

- **Mitigate Data Breach Risks**: Help protect your organization from potential breaches
- **Enable Regulatory Compliance**: Help meet data security regulations and stringent auditing and risk-reporting requirements
- **Enhance Data Visibility**: Maintain clear oversight of critical data assets

NIS2 Compliance Solutions

Goals of NIS2

NIS2 aims to enhance overall cybersecurity by:

- **Mandating Preparedness**: Each EU Member State must establish a Computer Security Incident Response Team (CSIRT) and a competent National Network and Information Systems Authority to address cyber threats
- **Increasing Collaboration**: Creating a cooperation group for information exchange among Member States
- **Promoting Cybersecurity Culture**: Fostering a cybersecurity culture across critical infrastructure sectors dependent on information and communication technology (ICT)

NIS2 Industries/Sectors

Essential Sectors

Essential sectors are required to comply with the NIS2 Directive regardless of their size.

- Health
- Transport
- Banking
- Financial Market Infrastructures
- Digital Infrastructure
- Water Supply
- Energy
- Public Administration
- Space Sector
- ICT Service Management
Managed Service Providers

Important Sectors

- Electronic Communications & Networks
- Digital Providers & Social Media
- Critical Product Manufacturing
- Postal & Courier Services
- Food & Beverage Industry
- Waste Management
- Chemicals
- Research

Learn more at entrust.com

NIS2 Compliance Solutions

Essential & Important Services

NIS2 impacts all organizations that provide "essential or important services" to the EU. Compared to the original directive, NIS2 increases the number of covered sectors from seven to 15, thereby protecting more vital aspects of EU society.

- **Essential Entities**: Large companies in critical sectors, defined as having at least 250 employees, an annual turnover of at least €50 million, or an annual balance sheet of at least €43 million.
- **Important Entities**: Medium-sized companies in high-criticality sectors that don't qualify as essential. These organizations typically have at least 50 employees, an annual turnover of at least €10 million, or a €10 million balance sheet.

Transposition Into National Law

All EU Member States were required to transpose the NIS2 directive into their national laws by October 17, 2024 – either updating existing cybersecurity laws or enacting new ones to meet the directive's requirement. This involves updating existing cybersecurity laws or enacting new ones to meet the directive's requirement.

Country-Specific Competent Bodies

Each EU Member State designates a national authority, or competent body, to oversee the implementation and enforcement of the NIS2 directive. For example, Germany's competent body is the Bundesamt für Sicherheit in der Informationstechnik (BSI), in France it's the National Cybersecurity Agency (ANSSI), and in Belgium it's Centre for Cybersecurity Belgium (CCB). Essential and important entities must consult their country's specific legislation for detailed requirements. In some cases, these laws often reference existing legislation and frameworks, such as the NIST Cybersecurity Framework (CSF), and certifications, such as ISO 27001/2.

Competent bodies have three primary responsibilities:

1. **Supervision and Compliance**: Ensuring entities adhere to NIS2's cybersecurity requirements
2. **Incident Reporting**: Overseeing the reporting of significant cybersecurity incidents by essential and important entities
3. **Enforcement**: Imposing penalties for non-compliance, which can include substantial fines

NIS2 Compliance Solutions

Article 21: Cybersecurity Risk-Management Measures

Article 21 of the final NIS2 directive states that “Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services.”

Article 21 then states “Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity’s exposure to risks, the entity’s size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.”

Finally, Article 21 outlines “The measures referred to… shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following”:

The key measures outlined in Article 21 are summarized below, along with corresponding solutions from Entrust:

NIS2 Directive Measure	Entrust Solutions
1. Implement policies for risk analysis and information system security	**Entrust KeyControl** and **Certificate Hub**: Managing keys, secrets, and certificates; compliance and risk reporting
	Entrust Cryptographic Center of Excellence: Consulting services to establish a governance structure (certificate policies and practices) including incident and response around PKI
2. Incident handling: Each EU Member State must adopt a national large-scale cybersecurity incident and crisis response plan, and designate one or more Computer Security Incident Response Teams (CSIRTs)	**Entrust Cryptographic Center of Excellence**: Consulting services to establish a governance structure (certificate policies and practices) including incident and response around PKI
3. Business continuity, such as backup management and disaster recovery, and crisis management	**Entrust Identity as a Service**
	Entrust nShield HSMs/nShield as a Service: Cryptographic root of trust
	Entrust KeyControl: Key and secret backup and recovery. Integration with third-party backup and storage solutions to manage cryptographic keys

Learn more at entrust.com

NIS2 Compliance Solutions

NIS2 Directive Measure	Entrust Solutions
4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	**Code signing solutions**
	Entrust Identity as a Service: Control access of code and binary repositories for authorized users only
5. Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure	**Entrust Cryptographic Center of Excellence**: Consulting services to develop best practices around maintenance
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	**Entrust KeyControl**: Risk reporting of cryptographic assets (keys, secrets, and certificates)
	Entrust CloudControl: Compliance reporting across VMware- and Kubernetes-based frameworks
	Entrust Cryptographic Center of Excellence offers expert services that help customers identify and instill governance and policies to address crypto management best practices
7. Basic cyber hygiene practices and cybersecurity training	**Entrust Cryptographic Center of Excellence** offers the following packaged services to help customers identify and instill cyber hygiene processes and practices: • Crypto Health Check • Crypto Governance Consulting • PKI Governance Health Check • PKI System Health Check • PKI Governance Consulting
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption	**Entrust KeyControl**: Key and Secrets Lifecycle Management Managing the complete lifecycle of keys and secrets is critical for comprehensive security. Keys and secrets underpin the security of cryptographic processes
	Entrust KeyControl: Compliance and Risk Management Documenting how keys and secrets are used not only mitigates risks but also facilitates compliance
	Entrust nShield hardware security modules (HSMs) offer FIPS-certified hardware roots of trust, available on-premises or as a service, enabling organizations to implement and enforce best practices in the generation and protection of the cryptographic keys that underpin an organization's encryption strategy

Learn more at entrust.com

NIS2 Compliance Solutions

NIS2 Directive Measure	Entrust Solutions
9. Human resources security, access control policies, and asset management	**PKI as a Service / Managed PKI** **Entrust Identity as a Service** **Entrust KeyControl** for protection of database keys
10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems within the entity, where appropriate	**Phishing-resistant identities** **Entrust Identity as a Service** **ID Issuance** **AI-powered Identity verification** **PKI as a Service / Managed PKI**

The NIS2 directive primarily discusses process, responsibilities, and authorities and defines essential and critical entities. It also specifies the scope, timing, and potential fines for non-compliance. However, it is not prescriptive about implementation methods, and references to specific technologies are minimal.

As a directive, NIS2 requires each EU member state to transpose its provisions into national law in accordance with the NIS2 rules. For specific details, organizations should refer to their own EU country-specific competent body and legislation.

> **Ransomware and other cyber threats have preyed on Europe for far too long. We need to act to make our businesses, governments and society more resilient to hostile cyber operations.**
>
> Lead Member of European Parliament, **Bart Groothuis** (Renew Europe, Netherlands).

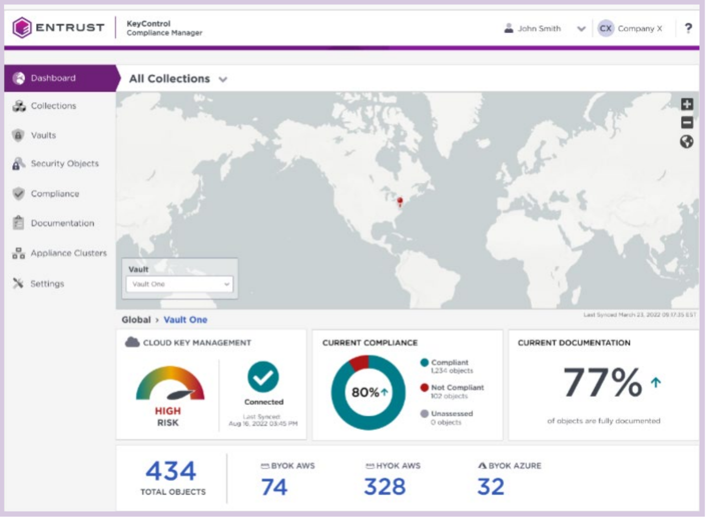
Learn more at entrust.com

NIS2 Compliance Solutions

1. Policies on risk analysis and information system security

Business continuity ensures that an organization's operations can continue smoothly, even in the face of disruptions. This involves a combination of strategic planning, technology, and processes to prepare for and respond to unexpected events.

Entrust KeyControl provides comprehensive risk reporting for cryptographic assets, such as keys, secrets, and certificates. It provides the ability to build a comprehensive inventory of cryptographic assets as well as categorize and assign level of risk, and it provides a unified dashboard with comprehensive risk reporting.



2. Incident handling

Member States' Computer Security Incident Response Teams (CSIRTs) are tasked with incident handling, which includes the prevention, detection, analysis, containment, response, and recovery from security incidents. This includes the processing of large volumes of sometimes sensitive data. Each EU Member State should ensure that their CSIRTs have an infrastructure for information sharing and processing, as well as well-equipped staff, which ensures the confidentiality and trustworthiness of their operations.

For essential or important entities establishing or refining their incident handling capabilities, one critical aspect is governance - specifically, documenting and detailing incident response procedures. In the case of public key infrastructure (PKI), as an example, Entrust provides consulting services to help establish governance structures, including certificate policies and practices, and incident response frameworks tailored to PKI environments.

3. Business continuity, such as backup management and disaster recovery, and crisis management

Business continuity, backup management, and disaster recovery are crucial components for maintaining the resilience of critical infrastructure.

All Entrust solutions support business continuity – whether as a service or on-premises. Entrust KeyControl and Entrust PKI maintain key archives to protect against key loss. In addition, Entrust KeyControl integrates with a range of enterprise backup and recovery solutions, providing key management to these applications on demand. The distributed architecture of KeyControl lends itself to scenario planning exercises such as cyber incidents where individual vaults can be readily switched offline and restored with minimal business impact.

4. Supply chain security, including supplier management/security

Most readers will be familiar with the SolarWinds Orion cyberattack where threat actors compromised the software build and update system of the SolarWinds network management software. Malicious Trojan code led to the compromise of multiple organizations' data and systems. The incident significantly raised awareness of the need to protect the integrity and security of the supply chain. The European Union Agency for Cybersecurity (ENISA) recommends several practical steps to enhance supply chain security;

- **Strategic Corporate Approach**: Develop a comprehensive strategy that integrates supply chain security into the overall corporate security framework.
- **Supply Chain Risk Management**: Identify and assess risks associated with suppliers and service providers. Implement measures to mitigate these risks.
- **Supplier Relationship Management**: Establish strong relationships with suppliers, ensuring they adhere to security standards and practices.
- **Vulnerability Handling**: Regularly monitor and address vulnerabilities within the supply chain. This includes patch management and incident response.
- **Quality of Products and Services**: Ensure that suppliers provide high-quality products and services that meet security requirements.

One area where Entrust can help in the supply chain is with code signing, which is the process of digitally signing executable files, libraries, and scripts using a signing tool and a digital certificate based on PKI technology. Code signing protects your company, partners, and end-users from software tampering when downloading executable program files – especially those from unsecured channels like the internet. As a code signing solutions provider, Entrust can help you and your suppliers implement efficient, high assurance code signing solutions that protect your business and your customers from attacks that forge or modify applications.

NIS2 Compliance Solutions

Entrust Identity as a Service (IDaaS) is a cloud-based identity and access management (IAM) solution designed to provide secure and seamless access for workforces, consumers, and citizens. It can be used to control access into code and binary repositories so that only authorized users are able to modify artifacts and code.

5. Security in connection with the acquisition, development, and maintenance of network and information systems, including the handling and publication of vulnerabilities

The NIS2 Directive states, "Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying such vulnerabilities is an important factor in reducing risk. Entities that develop or administer network and information systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered."

6. Policies and procedures (testing and auditing) for assessing the effectiveness of measures to manage cybersecurity risks

Entrust KeyControl's distributed architecture simplifies maintenance tasks, reducing the complexity of operations such as upgrades and backup/restore, and readily supporting scenario planning activities such as disaster recovery. Key vaults can be isolated without facing the scheduling challenge, risk, and unpredictability of taking your entire organization's KMS offline and then back online, thereby lowering the risk of service disruptions.

Another advantage of the KeyControl vault-based architecture is the ability to manage keys in segmented environments, preventing data transfer between network segments. This makes the vault architecture attractive to organizations that perform critical infrastructure operations or process sensitive data, such as via payment systems.

Entrust CloudControl delivers automated audit and compliance reporting based on various standards including NIST 800-53, and other control frameworks. It enables organizations to assess and identify cybersecurity gaps across cloud and orchestration platforms such as VMware, OpenShift, and Amazon EKS.

NIS2 Compliance Solutions

7. Basic cyber hygiene practices and cyber security training

Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software, and online application security, and business or end-user data upon which entities rely. Entrust's portfolio supports the application of strong security principles, from authenticating identities to PKI, digital signing, cryptography, and key management.

The Entrust Cryptographic Center of Excellence (CryptoCoE) comprises five building blocks that solve for specific gaps in your crypto and/or PKI environments. These may be summarized as:

- Entrust Crypto Health Check
- Crypto Governance Consulting
- PKI Governance Health Check
- PKI System Health Check
- PKI Governance Consulting

8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption

A barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization. As reported in the 2022 Ponemon Global Encryption Trends Study sponsored by Entrust, "Fifty-five percent of respondents say discovering where sensitive data resides in the organization is the number one challenge."

Best practices emphasize the protection of data, which relies on encryption as a fundamental means to secure sensitive assets. Effective data encryption requires the use of cryptographic keys that need to be managed securely over their lifecycle while complying with an enterprise's security policies and regulatory controls. Entrust nShield HSMs can be deployed as a high assurance root of trust and seamlessly integrate with KeyControl to provide an enterprise key, secret, and certificate management solution with a comprehensive, unified compliance and risk management dashboard.

In addition to helping assess crypto assets and security strategy, the Entrust Cryptographic Center of Excellence can also help define security policies and implement best practices.

NIS2 Compliance Solutions

Digital Certificates

Entrust security solutions allow you to issue digital certificate-based identities to corporate assets, while also including best practices, governance, and security controls via your PKI, including:

- Strong issuance and revocation controls
- Up-to-date certificate policy
- Operational procedures
- Change controls

Our private TLS/SSL certificates offer best practices, governance, and security controls, from how they were architected to strong issuance and revocation controls.

Our digital certificates deliver three key outcomes:

- Strong device identities – from IoT and mobile devices to servers and virtual machines
- Encryption for web servers, networks, and other systems
- Enforced access control to micro-segmented networks, applications, and systems

Certificate Lifecycle Management (CLM)

The more digital certificates an organization has, the greater the need for management and automation tools. CLM is an important component of your overall strategy by making sure you have strong issuance protection for your certificates.

Entrust's CLM solutions:

- Provide full visibility into your full certificate estate across environments
- Centralize control of digital certificates
- Provide the automation layer required to mitigate the risks that come with a high volume of certificates across multiple distributed environments

CLM ensures you have strong issuance protection for your certificates and mitigates common risks such as a rogue certificate being issued that gives too much access or privilege. Entrust's CLM solutions deliver the visibility, control, and automation you need to have a strong security practice today but also to prepare for a post-quantum future.

9. Human resources security, access control policies, and asset management

Compromised identities play a crucial role at different stages of the attack lifecycle – be it at the entry point, for privilege escalation, lateral movement, or even for data exfiltration. Stolen user credentials, expired digital certificates that secure devices, phishing, misuse of privileges, and social engineering are some of the tactics, techniques, and procedures that cyber adversaries use, all related to enterprise-wide identities including user identities and machine identities.

Digital transformation has expanded the attack surface beyond the network perimeter. Identity has become the new perimeter as organizations embrace remote and hybrid work arrangements, deploy cloud-based applications extensively, and use multiple devices, critical infrastructure, and assets. Entrust Identity as a Service provides a centralized approach to managing and aligning access control policies with secured assets, ensuring that only authorized users are granted access.

Entrust KeyControl offers management of cryptographic assets, namely cryptographic keys and secrets, such as API credentials.

Entrust PKI as a Service (PKIaaS) provides rapid provisioning of pre-configured certificate authorities (CAs) tailored to your use cases. Each customer receives a dedicated root CA and any necessary subordinate CAs. We ensure that configurations, such as certificate extensions and key usage, are pre-selected to match your requirements, creating turnkey solutions ready for immediate use. Configuration specifics, including supported certificate formats, are outlined in the published Certificate Practice Statement (CPS). The number of certificates that organizations are issuing and managing continues to grow at a rapid rate. Some of this can be attributed to the continued growth of traditional use cases and the need to secure remote and distributed workforces. But much of it has to do with the continuing rise in machine identities.

Centralized machine identity lifecycle management through Entrust Certificate Hub provides a unified view of all machine identities across your organization, along with a simple and intuitive ”single pane of glass” view. Available on-premises or managed, Certificate Hub helps resolve some complexities that can come with machine identities by providing one of the most critical components of machine identity management: automation.

10. Multi-factor authentication, continuous authentication, and secure voice, video, text, and emergency communications (as appropriate)

Entrust's identity and access management solutions support a wide range of authentication methods including:

- Passwordless
- Single Sign-On
- Phishing-Resistant MFA
- Adaptive Risk-Based Access and Authentication: Added security via contextual authentication driven by adaptive risk-based policy engine to verify users and devices before granting access
- Certificate-Based Authentication
- Non-intrusive detection of users' behavioral and environmental anomalies while protecting consumers from credential-stealing attacks, impersonation attacks, and computer/session takeover attacks
- AI-powered identity vesrification: Remote Identity Verification (IDV) blending award-winning document and biometric verification, trusted data sources, and fraud detection signals to seamlessly onboard customers for fraud prevention, KYC, and AML

Entrust is a trusted security adviser with decades of experience and a broad portfolio of solutions designed to help organizations meet NIS2 requirements and enhance their security posture.

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223