Saviynt

Unlocking NIS2 Compliance

How Identity Security Ensures Regulatory Readiness

Contents

How Identity Security Ensures Regulatory Readiness

A prominent economic principle suggests that **20% of effort drives 80% of outcomes.** When it comes to compliance readiness, the idea proves true.

By prioritizing Identity Security on the path toward NIS2 Directive readiness, enterprises learn: a little work goes a long way.

NIS2 Directive Overview

In January 2023, EU member states formally enacted a revision of the 2016 Network and Information Systems (NIS) Directive. Created in response to various well-publicized and damaging cyberattacks, the NIS2 Directive aims to bolster cybersecurity across the Union, including mitigating threats to network and information systems, and ensuring the continuity of services when incidents occur.

NIS2 also streamlines reporting obligations, and introduces more stringent supervisory measures and stricter enforcement requirements.

As of today, EU member states must incorporate the NIS2 Directive into their national laws by 17 October 2024.

NIS2 Emphasis Points

To address deficiencies and the fragmented application of earlier regulation, the NIS2 Directive **focuses on**:

Increasing the accountability of C-level leaders (by imposing direct obligations on the management in respect of compliance obligations, in particular to approve the cybersecurity risk-assessment);

Increasing the level of cyber resilience for entities operating in the EU across all relevant sectors (Notably, the NIS2 Directive provides a list of mandatory measures on business continuity, cybersecurity training, policies on risk analysis and information system security, etc);

Adding notification obligations to relevant authorities (in case of any incident having a significant impact on the provision of the services) and the recipients of the services (if such an incident is likely to adversely affect the provisioning of those services) within strict timeframes;

Creating GDPR-like fines (up to €10,000,000 EUR or 2% of the total annual worldwide turnover –whichever is higher);

Establishing better cooperation and information sharing between member states and competent authorities (to improve the awareness and the collective capability to prepare and respond to the cyber threats).

What organisations does NIS2 apply to?

The EU architected NIS2 to apply to **any entity** that provides essential or important services to the EU economy and society–including companies and suppliers.

Importantly, if an entity is not established in the EU, but offers services within the EU, it must designate a representative in the EU.

Essential Entities (EE)

Size threshold: varies by sector, but generally 250 employees, annual turnover of €50 million or a balance sheet of €43 million.

Your organization must manage risks and implement both damage prevention and mitigation measures that reduce risks and impacts. Adequate measures are expected, for example, around incident management, cyber security in supply chains, network security, access control and encryption.

– Bram van Tiel, PwC - Partner Cybersecurity and Privacy

Important Entities (IE)

Size threshold: varies by sector, but generally 50 employees, annual turnover of €10 million or a balance sheet of €10 million.

NIS2: Minimum Measures

NIS2 mandates that essential and important entities implement basic security measures to address vulnerabilities and likely cyberthreat forms across four key domains: risk management, corporate accountability, reporting obligations, and business continuity.

Within these, EU regulators **highlight fundamental measures** that entities focus on to protect network and information systems and the physical environment of those systems from potential cyber incidents.

Highlighted in Chapter IV, Article 21, the ten minimum measures include:

Risk assessments and security policies for information systems	**A plan for** handling **security incidents.**	Plans for **business continuity** such as backup management and disaster recovery; and other crisis management.	**Supply chain security** including relationships between the company and direct suppliers. Includes assessment of security levels and measures to address vulnerabilities.	Security around the **procurement, development, and operation** of systems. Includes, having policies for handling and reporting vulnerabilities.
Policies and **procedures for evaluating the effectiveness** of cybersecurity and risk-management measures.	**Cybersecurity training** and a practice for basic cyber hygiene.	Policies and **procedures for the use of cryptography** and, when relevant, encryption.	**Human resources security, access control policies and asset management.**	The **use of multi-factor authentication,** continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication.

How Saviynt Enables NIS2 Compliance

A capable NIS2 Directive response requires a unified identity security approach–one built on a foundation of Zero Trust.

Saviynt's Identity Cloud is a fully-integrated, converged identity platform that unites core identity governance and security capabilities to protect people, data, and infrastructure.

The multiple identity governance capabilities that the Identity Cloud offers–including Identity Governance and Administration (IGA), privileged access management (PAM), third-party access governance (TPAG), application access governance (AAG), and others helps organisations address NIS2 Article 21 requirements.

In particular, the platform supports preparatory efforts related to incident handling and reporting, supply chain security, cryptography and encryption, access control policies, and Zero Trust security.

Enterprises that position identity as the new security perimeter–and embrace autonomous, adaptive identity security for employees, third parties, and machines–may meet compliance directives in six key ways:

1 Bolstering risk management procedures, plans, and execution

NIS2 requires organizations to implement appropriate technical and organizational measures to manage risks to their network and information systems. Saviynt's IGA provides visibility into who has access to what resources across the entire organization, helping to identify and manage risks associated with excessive or inappropriate access rights.

Enterprises also simplify access right-sizing with automated provisioning and deprovisioning for any human or machine identity to any application or cloud.

With PAM, enterprises support Just-In-Time access and grant elevated privilege on a time-bound basis. By starting from a place of Zero-Standing privilege, security leaders can employ least privilege policies, including privilege clipping using usage and outlier analysis.

Saviynt's role-engineering capabilities help secure data and mitigate threat risks by creating a single user identity that encompasses entitlements across all accounts to standardize role definitions that limit access according to the principle of least privilege. Saviynt's solution employs both bottom-up and top-down role analysis, as well as usage-log analysis, providing visibility into access granted but not being used, mitigating excess access risk.

2 Improving incident detection and response

Saviynt's identity platform continuously monitors for new risks and identifies unusual behavior so organizations can prove continuous control effectiveness.

If control violations occur, the platform sends alerts and suggests remediation actions.

Platform analytics can detect high-risk activity based on various data risk scoring parameters including volume spike, ingress/egress traffic, event rarity, outlier access, policy/control violations, and threat intelligence. Saviynt then enables enterprises to perform signature-less analysis for rapid detection, effective investigation, and closed-loop security response. Leveraging techniques such as quarantine, access lockdown, or security team alerts, security teams guard against insecure data sharing.

In addition, audit trails and session recordings add robust documentation of cyber incidents.

3 Strengthening escalation and reporting capabilities

To support adherence to escalation, reporting, and related incident handling requirements, Saviynt's Risk Exchange consumes and exchanges risk data across key GRC and risk platforms, including SIEM, UEBA, and vulnerability management tools.

With risk signals contained in a single dashboard, IT departments increase their effectiveness, reduce risk-monitoring fatigue, and decrease operational cost.

4 Reinforcing software supply chain security

Through NIS2, EU regulators put software supply chains in the crosshairs. With Saviynt, enterprises can incorporate least privilege **within DevOps and CI/CD processes**.

Using PAM, enterprises have the ability to tightly scope secret distribution and limited lifespans of credentials to limit the period where attacks can take place. An API integration lets developers call the Saviynt vault to request access and check out a key at the time of code execution.

This results in less key exfiltration and compromise.

5 Enlarging board and management involvement

NIS2 places **renewed responsibility** on "management bodies" in ensuring compliance with elements of NIS2. Regulators want to emphasize corporate leadership's role to:

- Approve the cybersecurity risk management measures taken by the entity–for instance, the risk man-agement measures surrounding supply chain security diligence;
- Supervise the implementation of the risk management measures;
- Follow specific, regular training to gain the requisite knowledge and skills to apprehend and assess the cybersecurity risks;
- Maintain accountability for entity non-compliance.

More responsibility for management around non-compliance should move enterprises to embrace easier ways leaders to lead cybersecurity initiatives.

Saviynt's dashboards offer easy-to-read visualizations that can be used to present high-level control and risk data to the Board or Senior Management. Organizations can also download

complete audit trail logging infor-mation such as keystroke logs for more detailed information about controls' weaknesses.

6 Preventing cyber incidents

Through better identity and access rights management, (including across applications, data, and third-par-ties), enterprises can limit security incidents such as unauthorized access or data breaches.

This aligns with the NIS2 Directive's requirement for organizations to take "necessary measures" to prevent incidents that could disrupt essential services.

Furthermore, entities can elevate their own cybersecurity capabilities by, where appropriate, pursuing the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems.

Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness

– EU NIS2 Directive, Preamble 89

Next Steps for NIS2

Eligible enterprises must form a plan to implement NIS2 Directive measures soon. To start, assess whether your organization falls within the scope of the regulation. If confirmed, review your existing processes, policies, and cybersecurity measures to identify relevant gaps.

For more information about how Saviynt can support your organization's NIS2 Directive readiness effort, learn more about the Identity Cloud or meet our team.

- **Tour Identity Cloud**, provides intelligent access & governance for any app, any identity, any cloud. Modernize your identity program and build a zero trust foundation designed to take on new challenges as they emerge.
- **Explore** compliance readiness customer stories.
- **Connect** with a Saviynt security professional.

ABOUT SAVIYNT

The Saviynt Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution.

Saviynt PAM solution is delivered via an agentless, zero-touch cloud-architecture so you can quickly deploy privileged access capabilities. Achieve zero-standing privileges with just-in-time (JIT) access and intelligent risk insights to power your PAM program.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suit e D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com