
**NIS2 directive is implemented to enhance the security of network and information systems within the EU (European Union). These guidelines require operators of critical infrastructure and essential services to implement appropriate security measures and report any incidents to the relevant authorities. ARCON's highly mature Identity and Access Management (IAM) along with enterprise risk remediation solutions can help the EU-wide enterprises to comply with the NIS2 mandates and build a robust information security framework.**

## Table of Content

## Overview

The EU's Cybersecurity strategy aims to bolster the region's resilience against cyber threats and ensure that individuals, businesses, and enterprises benefit from secure digital technologies. It focuses on enhancing the security of essential services like hospitals, energy grids, and railways, and the increasing number of connected devices in residences and workplaces.

The EU emphasizes the need to be technologically sovereign, ensuring that all connected services and products are resilient. The strategy outlines a plan to work with international partners to ensure global cybersecurity and stability in cyberspace. It also ensures that the digital transformation respects fundamental rights, democracy, and the rule of law.

## What is NIS2?

The NIS2 (Network and Information Systems 2) Directive is a European Union directive aimed at enhancing cybersecurity across the EU and is an update to the original NIS Directive. The NIS2 Directive that came into effect on January 16, 2023, continues and expands the previous EU cybersecurity directive, NIS, introduced in 2020. NIS2 was proposed by the European Commission to build upon and rectify the deficiencies of the original NIS directive.

NIS2 expands its EU-wide security requirements and scope of covered organizations and sectors to improve the security of supply chains, simplify reporting obligations, and enforce more stringent measures and sanctions throughout Europe. It aims to enhance the security of network and information systems within the EU by requiring operators of critical infrastructure and essential services to implement appropriate security measures and report any incidents to the relevant authorities.

## Why NIS2?

The European Commission decided to revise the NIS Directive to clearly define the organizations covered and their specific requirements in the form of NIS2. The NIS2 directive expands the scope of the original NIS Directive to include a wider range of organizations, increasing the number of "entities" covered including public administration, digital providers, space, research, postal services, waste management, foods, manufacturing, and chemical products. The main goals of NIS2 are to:

- Strengthen cybersecurity requirements for a broader range of sectors and entities, including critical infrastructure.
- Improve cooperation between EU Member States on cybersecurity matters.
- Enhance incident reporting and response mechanisms.
- Introduce stricter enforcement and penalties for non-compliance.

## What are NIS2 requirements?

The NIS2 Directive introduces several key requirements to enhance the security of network and information systems within the EU. The principal areas it covers are:

- **Risk Management:** Organizations must implement measures to minimize cyber risks, including incident management, supply chain security, network security, access control, and encryption.
- **Corporate Accountability:** Management must oversee and approve cybersecurity measures, receive training on cyber risks, and may face penalties for breaches.

- **Reporting Obligations:** Essential and important entities must promptly report security incidents with significant impact, including a 24-hour "early warning" notification.
- **Business Continuity:** Organizations need plans for ensuring business continuity during major cyber incidents, including system recovery, emergency procedures, and crisis response teams.

Additionally, NIS2 mandates baseline security measures such as risk assessments, security policies, cryptography, incident handling, procurement security, cybersecurity training, and multi-factor authentication. These requirements aim to bolster Europe's resilience against cyber threats and improve overall cybersecurity standards.

## Who should follow NIS2 Directive?

The NIS2 Directive applies to a broad range of organizations within the EU, categorized into two main groups: essential entities and important entities. Here are the key types of organizations that must comply:

**Essential Entities**

- Energy: Electricity, oil, gas
- Transport: Air, rail, water, road
- Banking: Credit institutions
- Financial Market Infrastructures: Trading venues, central counterparties
- Health: Healthcare providers, hospitals
- Drinking Water Supply and Distribution
- Digital Infrastructure: Internet exchange points, domain name systems, cloud computing services

**Important Entities**

- Postal and Courier Services
- Waste Management
- Chemical Industry
- Food Production and Distribution
- Manufacturing: Critical products
- Digital Providers: Online marketplaces, search engines, social networks

Additionally, non-EU companies that operate within the EU or provide services to EU entities are also impacted by NIS2.

## What are the penalties for NIS2 non-compliance?

The NIS2 Directive imposes significant penalties for non-compliance, which include:

**Administrative Fines**

- Essential Entities - It can reach up to €10 million or 2% of the global annual revenue, whichever is higher.
- Important Entities - It can be up to €7 million or 1.4% of the global annual revenue, whichever is higher.

**Non-Monetary Remedies**

- Compliance orders
- Binding instructions
- Security audit implementation orders
- Threat notification orders to entities' customers

**Criminal Sanctions**

- Top management can be held liable for gross negligence in a security incident.
- Public statements identifying responsible individuals and the nature of the violation.

These measures aim to ensure that organizations take cybersecurity seriously and implement the necessary measures to protect their network and information systems.

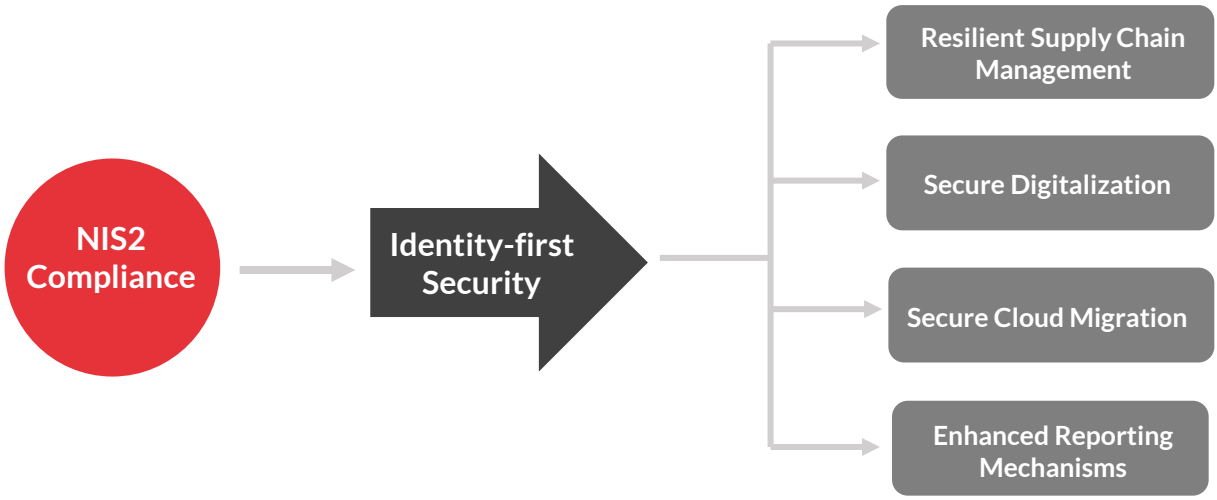
## Inherent IT Risks in Supply Chain Management

Cyber-attacks on supply chains have risen significantly, including security breaches stemming from compromised identity. It can happen in any industry, and it typically happens on a specific target, especially when the "target" has a lot of customer base. The hackers' objectives in such attacks are to infiltrate or affect as many suppliers as possible in the entire value chain of the "target." The incentive for the bad actors is that organizations have a lot of contracts with third-party vendors, especially in the manufacturing, pharmaceutical, healthcare, and government sectors.
Since NIS2 expands its requirements to improve the security of supply chains, it is highly imperative to figure out the risks and vulnerabilities of supply chains, especially those associated with access control and privileged identity management.

Some key points related to access control management are as follows:

- Typically, organizations do not have a systematic user verification process in place, such as multi-factor authentication (MFA) for every path that leads to a critical system. As a result, there is no detection of potential security gaps, and breach attempts can go unnoticed especially from an access management perspective.
- Normally, very few organizations give adequate importance to managing and secure passwords that are the prime targets of threat actors.
- In recent times, a lot is being discussed about digital-identity threat detection mechanisms. It secures the vendor with near real-time alerts on anything anomalous (if it happens). Without it, neither the organization, nor the vendor would know about the suspicious activity happening inside the IT ecosystem. ARCON leveraging AI and ML technologies, provides a robust stack of solutions that helps to identify threats and respond in real-time with the help of ITDR (Identity Threat Detection and Response) while ensuring robust user access governance, especially in an extremely critical PAM environment.

In complex digital and supply chain environments, the foundation of a robust cybersecurity framework can be built by implementing an Identity-first security approach. To manage identity-centric controls in on-prem or on-cloud environments, organizations can count on an Identity-first security approach, that ensures context-wise controls and continuous monitoring of the identities, for both supply chain management, digitalization, or cloud migration. It plays a pivotal role in managing risks arising from any of the IT environments, especially those arising from compromise of privileged identity. Indeed, a privileged account often includes permissions that allow changes to be made to settings, such as security configurations. By nature, privileged accounts have the greatest potential for operational risk, reputational risk, loss of intellectual property, loss of regulated data or even, in the case of cyber-physical incidents, catastrophic loss.




## Role of IAM solutions in complying with NIS2 directive

ARCON, being one of the top vendors in IAM (Identity and Access Management) and GRC (Governance, Risks, and Controls) space, plays a crucial role in assisting organizations to comply with the NIS2 Directive. ARCON with its robust stack of IAM solutions can ensure the following:

- **Authorization:** Privileged Access Management (PAM) and other IAM solutions of ARCON authorizes every user before granting access to critical systems, applications, and databases by building a definite and stringent access control framework around people and policies.
- **Access Controls:** IAM solutions of ARCON enforce stringent access controls, ensuring that only authorized users can access sensitive data and systems. This includes implementing role-based access controls (RBAC), policy-based access controls (PBAC) and multi-factor authentication (MFA).
- **User Authentication:** ARCON solutions provide robust user authentication mechanisms to verify the identity of users before granting access. This helps to prevent unauthorized access and potential security breaches.
- **Continuous Monitoring/Audit Logs:** IAM systems continuously monitor user activities and details of access logs. This helps in detecting and responding to potential security threats in real-time.
- **Incident Reporting:** ARCON solutions can generate detailed reports on data access and user activities, which are essential for complying with NIS2's incident reporting requirements.
- **Privileged Access Management (PAM):** IAM includes PAM, which focuses on managing and securing access for users with elevated privileges. This is extremely critical as privileged accounts quite often targeted by cyber attackers for treasure trove of enterprise data.
- **Just-in-time (JIT) Privileges:** ARCON's JIT Privilege approach helps organizations to follow the principle of 'Least Privilege' and mitigates threats arising from 'always-on' privileges. It gives ample scope to the administrators to grant privilege rights to users to accomplish tasks in a secure manner without worrying about when to revoke the rights as it happens automatically after the designated timeline.
- **Password Vaulting:** ARCON's Password Vaulting feature ensures that the privileged credentials in an IT environment are stored and managed in a highly secure environment by providing a single point of control.
- **Identity Governance:** Governing identities, both human and non-human, is extremely critical for organizations to ensure that the right people have the right level of access to the right resources at the right time. ARCON offers identity governance that includes the entire identity lifecycle, including identity creation, management, and deletion.

## ARCON's products for Business Resilience and Risk Remediation

- **Drift Management:** ARCON Drift Management enables digital businesses to proactively eliminate threats that arise from application drifts before they become a challenge for the resilient IT posture and digital ecosystem.
- **Security Compliance Management (SCM):** ARCON's SCM is a robust centralized engine for IT controls, risk assessment, and risk mitigation to secure Information assets. It enables organizations to identify compliance irregularities by assessing the systems against the organization-specific information security and configuration baseline policies resulting in identifying the possible risks.

## NIS2 Directive Checklist and Role of ARCON solutions

In this compliance mapping paper, we have discussed the requirements of NIS2 Directive in the below table and how ARCON's IAM solutions such as Privileged Access Management (PAM), Security Compliance Management (SCM), Endpoint Privilege Management (EPM), ARCON My Vault, and Drift Management can help the business enterprises of the EU to comply with all the requirements.

| NIS2 Directive Requirements | Does ARCON help? | Which ARCON solution and its feature addresses it? |
|---|---|---|
| Organizations must implement measures to minimize cyber risks, including incident management, supply chain security, network security, access control, and encryption. | ✔ | ARCON's Privileged Access Management (PAM) solution helps EU organizations to minimize cyber risks by providing network security and data encryption through robust access control mechanism.<br><br>A robust access control module that ARCON offers ensures the deepest level of granular control. It includes –<br>i. Fine-grained access control (Admins can control exactly which users have access to which services and resources);<br>ii. Process and Command Restriction (Admins can restrict or elevate specific processes or commands that can be executed);<br>iii. Critical Command Approval (Privileged user requires that certain commands be approved by the admin before they can be executed)<br>iv. Reporting (Admins can generate reports on the privileged user activities and access control events). |

| | | |
|---|---|---|
| | | With the Data Intellect feature of ARCON's Endpoint Privilege Management (EPM) solution, one can classify the data based on importance such as PII, sensitive information and gain complete visibility over confidential data.<br><br>ARCON's My Vault solution offers a centralized repository to store, access and share all sorts of critical business information in a secure manner. This stored information remains encrypted and can be deleted easily after a preset time to avoid any unauthorized access. It also controls the end-users' activities based on the pre-configured permissions even at a granular level. This tool has a solid integration with ARCON \| PAM. |
| NIS2 requires corporate management to oversee, approve, and be trained on the entity's cybersecurity measures and to address cyber risks. Breaches may result in penalties for management, including liability and a potential temporary ban from management roles. |  | ARCON's Security Compliance Management (SCM) solution enables organizations to identify compliance irregularities by assessing the systems against the organization-specific information security and configuration baseline policies resulting in identifying the possible risks.<br><br>It is a robust technology that enables enterprises to adhere to various IT security standards for compliance purposes and enhances visibility towards the information security posture of an organization. This way possibilities of non-compliance penalties or potential temporary ban from management roles are also prevented. |
| Essential and important entities must promptly report security incidents with significant impact, including a 24-hour "early warning" notification. |  | ARCON Privileged Access Management (PAM) solution provides real-time alerts for suspicious activity, enabling security teams to respond to potential threats quickly by freezing or terminating the session. This "early warning notification" adds an extra layer of security to privileged accounts and helps to protect sensitive data. |
| Organizations must plan for how they intend to ensure business continuity in the case of major cyber incidents. This plan should include considerations about system recovery, emergency procedures, and setting up a crisis response team. |  | ARCON's Drift Management effectively identifies discrepancies, non-compliances, or any variances happening in an IT environment and thus allows security pros to expeditiously investigate and rectify them to ensure business continuity. |

| | | |
|---|---|---|
| | | It enables digital businesses to proactively eliminate threats that arise from application drifts due to unauthorized alterations or deviations before they become a challenge for the resilient IT posture and digital ecosystem. This way it helps the GRC (Governance, Risks, and Controls) leaders to preserve the desired state of all security controls by continuously comparing the current configuration of systems against the standard baseline policy. |
| The use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate. |  | ARCON's PAM solution offers Multi-Factor Authentication (MFA) that acts as a strategic, relevant, and essential engine to provide multiple forms of identity verification steps before the users are allowed access to the desired network, system, or application. Along with the traditional verification methods such as SMS and Email OTP mechanisms and hardware tokens, ARCON's MFA provides integration with various third-party authentication apps, including disparate biometric and facial recognition technologies. |

## Conclusion

All organizations from the EU need to take steps to improve their cyber resilience and the NIS2 directive provides the necessary framework.

- The NIS2 directive places obligations for cyber resilience
- The compliance team must ensure that any organization's resilience to cyber-attacks is adequate
- It enhances the security of network and information systems within the EU by implementing appropriate security measures and reporting any IT incident to the relevant authorities
- ARCON provides the necessary safeguards to comply with the NIS 2 Cybersecurity framework

## about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

**ARCON Privileged Access Management (PAM)** is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us