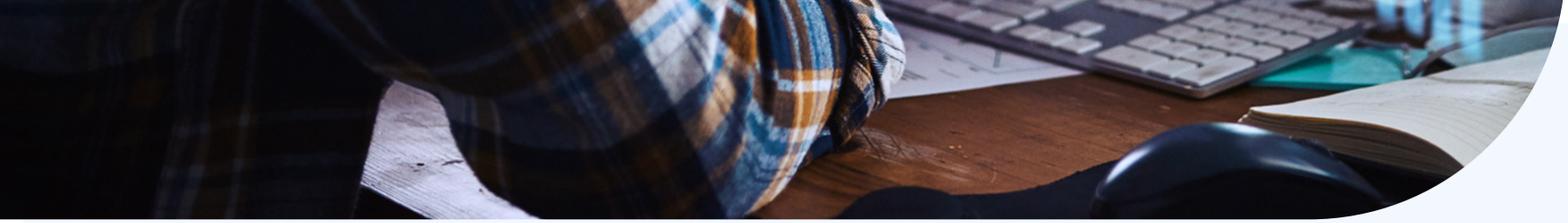
Is Your Physical Access Control System **Ready for NIS2?**

New EU Directive Closing the Gap on Physical and Digital Security

EBOOK



NIS2 Background and Basics

Cybersecurity affects companies, individuals and nations great and small — and it's a constantly moving target. To stay ahead of the rapidly evolving threat landscape, governments across the globe are implementing legislation to better protect data and consumers.

The European Union, a leader in this space, has passed the **Network and Information Security 2 (NIS2) Directive** to strengthen cybersecurity and protect critical infrastructure. Implementation for this wide-reaching measure (an update to 2016's NIS Directive) is **October 17, 2024**.

This date marks when NIS2 requirements will have been transposed into the national laws of EU Member States — and companies within those states must comply with its requirements or face steep fines.

NIS2 aims to raise the collective capacity to prevent, withstand, manage and recover from physical and digital threats to IT (information technology) and OT (operation technology) systems and infrastructure.

NIS2 Varies in Practice by Country

It's important to know that NIS2 outlines **minimum** requirements, which each member state will interpret differently. For example, critical entities "significant incidents" should notify competent authorities within 24 hours, but those authorities are defined by each country. Many of these requirements are yet to be solidified and could change over time.

What's New in NIS2:

Stricter Security, Higher Fines and Reporting Obligations — And an Eye on Supply Chains

The NIS2 Directive was designed to build upon and modernize the legal framework first articulated in the **original NIS Directive**. This legislation aims to increase the level of cybersecurity in Europe in the longer term, particularly when it comes to critical infrastructure and essential services.

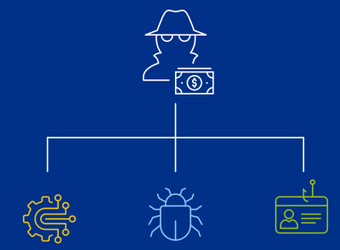
Here are some of the most notable additions:

- **More Industries Affected** — NIS2 covers a wider range of entities than the original directive. It now includes sectors like energy, transport, finance, healthcare, utilities, digital infrastructure and public administration. Size thresholds vary by industry, but organizations with as little as €10 million in gross annual revenue will have to comply. **See Annex 1 for full list of sectors, subsectors and entity categories.**
- **Scope Expanded to Suppliers** — NIS2 defines and distinguishes between "essential entities" (EEs) and "important entities" (IEs). Any company that is part of an EE or IE organization's supply chain must also comply with the regulation. Some HID manufacturing sites for electronic components may be classified as IEs under NIS2; Jump ahead to page 6 for the proactive steps we've taken ensure that these facilities exemplify cybersecurity excellence.
- **Stricter Controls** — The new directive applies stricter and more comprehensive security measures. It requires organizations to implement robust controls in order to mitigate risks and protect systems and data, including the prevention of unauthorized access, phishing, ransomware and other cyberthreats.
- **Stronger Reporting Requirements** — Organizations must report significant cybersecurity incidents within 24 hours of detection to the authority that their member state has designated. What's "significant"? According to the NIS2 Directive, it's any event that might cause severe damage, disruption or loss, either to your organization or to other people.
- **Harsher Penalties** — Fines for non-compliance are much higher than they were in the past. In fact, penalties can reach up to 10% of an entity's annual turnover.

Where to Start: The Risk Assessment

NIS2 is about building cybersecurity resilience. Resilience is not created overnight, which is why the legislation emphasizes company-specific assessments and processes — and not a “one-size-fits-all” approach.

For in scope entities, the first step towards NIS2 compliance is to perform and document an operational risk assessment in order to gain a comprehensive understanding of all relevant threats, in particular those that could disrupt their ability to provide essential services. Based on this assessment (which should be repeated “whenever necessary in light of their particular circumstances and the evolution of those risks, and [at least once] every four years”), management must decide on the measures to reduce those risks and follow up on their implementation — or face personal liability.



Are Risk Really on the Rise?

Undoubtably, yes. According to the European Union Agency for Cybersecurity (ENISA), 2023 saw a significant increase in both the variety and quantity of cyberattacks and their consequences, and there was no indication of a slowdown. Distributed Denial of Service (DDoS) and ransomware top the list, followed by social engineering, data related threats, information manipulation, supply chain and malware.

HID

NIS2 Addresses and Accounts for the Interconnection of Physical and Cybersecurity

Our physical and digital worlds are increasingly blurred and intertwined. According to the 2024 State of Physical Access Control report, published by HID in partnership with IFSEC Insider:

- Nearly half **(48%)** of all respondents confirm that the IT department is "fully consulted" when it comes to upgrading physical access control systems
- **58%** of security personnel work with the IT department to establish best security practices, while
- **55%** of security respondents said they collaborate with IT when looking for new technologies

Gartner echoes this convergence, reporting that 41% of enterprises plan to combine parts of cyber and physical security by 2025, a 10% increase over 2020.

It makes sense, right? As companies on the receiving end of these attacks can attest, you're only as secure as your weakest link — and that link might be physical or digital. The interconnection of physical and digital systems provides numerous benefits, but also additional vulnerabilities. For example, a compromised access control system might allow criminals to access restricted areas, disable alarms, alter permissions and steal proprietary information.

Legacy access control systems, which are still very prevalent, provide significantly less security and introduce more risk. Again, according to the 2024 State of Physical Access Control:

- **42%** reported their organization's access control was less than three years old
- **14%** said their access control system was more than six years old
- **54%** planned to upgrade access control system software
- **53%** planned to upgrade readers and credentials
- **50%** intend to upgrade controllers

Unifying IT and OT is the only way to achieve a holistic view of your entire operation and mitigate the growing threats that come with interconnected systems and devices, which is why NIS2 addresses both fronts.

Addressing Physical Access Control Areas of Focus

How can you fortify the cybersecurity of your organization's physical access control systems? As you've probably guessed, it involves more than simply evaluating the integrity of individual components. Part of your NIS2 risk assessment should examine how information travels from component to component — and where risk might be introduced. For example, how is sensitive information about employee identities and authorization privileges provisioned onto credentials? How is it stored and managed?

We recommend using a "good, better, best" type of framework that starts by establishing a baseline before making further upgrades and improvements. We've included some details on how to go about that below (sorted by product area), or you can **watch our on-demand webinar** for a deeper dive on the topic.

Area of Focus: Credentials

- **Purpose:** Securely store access control data
- **Set a baseline** with smart cards or virtual cards. Data stored on the card should be protected with encryption (AES 128 is best practice). So should data that's communicated from card or smartphone to reader during the authentication process.
- **Improve security** by deploying key management policies. Also, look for solutions that have been penetration tested and certified by a third party.

Area of Focus: Readers

- **Purpose:** Process credentials and send them to a controller
- **Set a baseline** with readers that support encrypted cards and are equipped with a secure element to store encryption keys
- **Improve security** by selecting a solution that offers a secure communication channel between reader and controller using IEC 60839-11-5:2020 standard OSDP v2. Manage updates and upgrades via authorized maintenance applications, not configuration cards.

Area of Focus: Controllers

- **Purpose:** Interface with readers and cards to determine whether user permissions are sufficient to grant access to an area
- **Set a baseline** by installing controllers in a secure, tamper-proof enclosure. Connect them to a secure, dedicated VLAN and deactivate all other interfaces (like USB and SD). Remove all default configurations and ensure that firmware and patches are always up-to-date.
- **Improve security** by allowing only approved IP addresses to connect to the controller — and ensure that encryption is used to protect data at rest and in transit

Area of Focus: Access Control Servers and Clients

- **Purpose:** Serve as the system's main database and management console, recording activity and enabling organizations to make changes and adjust settings
- **Set a baseline** by hosting servers and clients on a secure, dedicated VLAN. Select a solution that offers transparent Common Vulnerabilities and Exposures (CVE) reporting and complies with Secure Software Development Lifecycle (SDLC) standards like ISA/IEC 62443-4-1— and make sure to keep software and operating system patches up-to-date.
- **Improve security** by encrypting data at rest and in transit and deploying custom TLS certificates

Did You Know?
HID Can Also Help With Your Digital Preparedness

While this eBook is focused on the physical access aspects of NIS2, it's worth mentioning that HID is a global leader in identity management and authentication of all kinds — including multi-factor authentication (MFA), which is specifically called out by NIS2 as a recommended preventative measure.

We’re Ready To Help You Comply With NIS2

HID is a supplier of “essential” and “important” entities. Moreover, according to NIS2, some HID manufacturing sites can be classified as important entities. Consequently we’ve taken proactive steps to ensure that HID and its facilities exemplify cybersecurity excellence. Here’s how:

- **Certifications That Go Above and Beyond NIS2** — Our factories and product development operate with an Information Security Management System (ISMS) that surpasses the basic hygiene requirements currently outlined by NIS2. This positions us well above NIS2’s minimum standards and allows us to adapt to any enhanced requirements imposed by Member States promptly. Check out our full list of certifications, including SOC2 Type 2, ISO 27001, ISO 27018, CSA Star Level 2 and SEAL-5 TÜV Security Certification.
- **Continuous Monitoring and Improvement** — We are committed to continuously monitoring the evolving cybersecurity landscape and adjusting our practices to meet or exceed new standards as they develop
- **End-to-End, Interoperable Protection** — We are one of the few companies to power end-to-end protection, from PACS and identity and access management (IAMS) to digital certificates and biometrics
- **Tested and Trusted Global Leadership** — For over 30 years, HID has been trusted by the world’s most secure and regulated industries, including government, banking and healthcare

Every day, millions of people in more than 100 countries rely on HID to securely access physical and digital places, and many of those very same products and services can assist you in achieving NIS2 compliance.

Thank you for downloading this eBook as you embark (or continue) on your security journey. We will keep you posted as this regulation develops. Keeping your organization, data and people safe is what we do.

Certifications

AICPA SOC

ISO 27001 CERTIFIED by schellman

ISO 27018 CERTIFIED by schellman

CSA cloud security alliance®

TÜVIT 2020 Trusted Product

© TÜVIT – TÜV NORD GROUP – www.tuvit.de

HID

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171-1108

For more global phone numbers click here

2024-10-03-hid-pacs-nis2-eb-en
PLT-08041

Part of ASSA ABLOY