Guide to the NIS 2 Directive

HIKVISION | THRIVE

Last updated July 2025

Contents

Understanding NIS2 and its Relevance to the Security Industry

Hikvision’s Practices in Response to the NIS2 Directive

Hikvision’s Commitment to Security

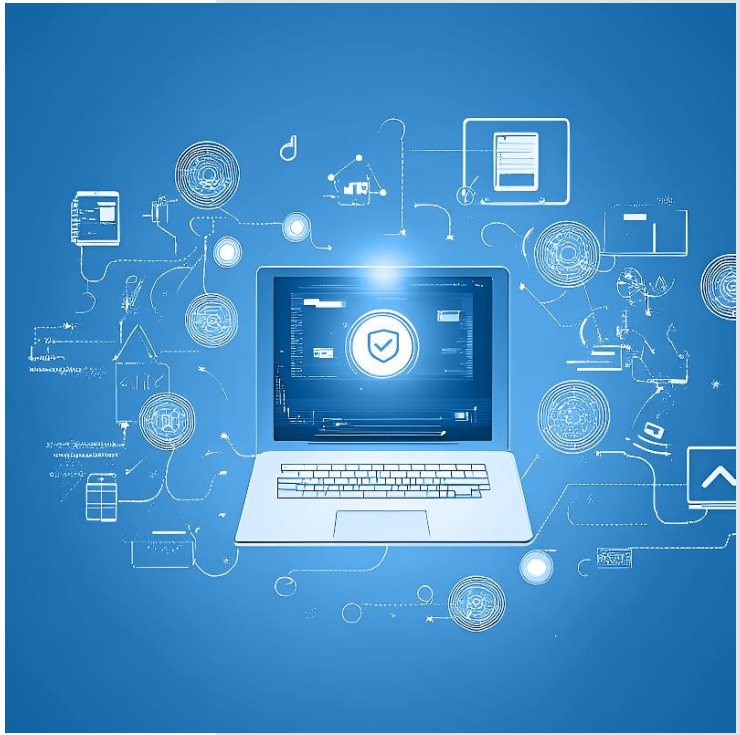
Understanding NIS2 and its Relevance to the Security Industry

What is NIS 2 directive?

The “Network and Information Security Directive” (NIS2 Directive), which came into effect in January 2023, updates and replaces the original European Union (EU) legislation on cybersecurity, the NIS1 Directive, adopted in 2016. The NIS2 Directive expands its scope, also the cybersecurity requirements and sanctions to harmonize and streamline the security level across all EU Member States to “improve the resilience and incident response capacities of both the public and private sector.” It requires that each EU member state transpose the NIS2 Directive into its national legislation.

The consequences of not complying with NIS2 can go beyond financial fines. Management teams within non-compliant entities could also be held legally accountable.

The transposition of the NIS2 into national law is still in progress. At Hikvision, we continue to closely monitor legislative and industry developments, and will make timely compliance adjustments as necessary.



Who is impacted by the NIS2?

The directive applies to both private and public entities, specifically, the directive applies to:Public or private entities of a type as described in Annex I or II to the directive; and

- Qualify (at least) as a medium-sized enterprise, meaning they have more than 50 employees, annual turnover/balance sheet total exceeding EUR 10 million (important entity); or
- Qualify as a large organization, having more than 250 employees, annual turnover exceeding EUR 50 million and a balance sheet total exceeding EUR 43 million (essential entity)

In addition, regardless of the size of the public or private entity, NIS2 applies to entities that are trust service providers, TLD-name registries, domain name registration service providers, providers of public communication networks and providers of publicly available electronic communications services.

What's more, the vendors that supply products and services to "essential" and "important" entities are indirectly affected. Those organizations need to ensure the security of their services and products.

What is the NIS2 requirement?

NIS2 compliance requires all relevant organizations to implement a number of minimum measures. Below is a general summary of the key requirement areas.

Leadership awareness
Leadership must be aware of and understand the requirements of the Directive and the risk management efforts.

Crisis Preparedness
Maintain backups and continuity plans for IT system post-incident.

Network Security
Use encryption, multi-factor authentication, and encrypted emergency communication, when appropriate.

Data encryption / Cryptography
Policies and procedures for the use of cryptography and, when relevant, encryption.

Security policies
Define protocols for incident handling, data access, asset management, etc.

Supply Chain Security
Assess and mitigate risks with direct suppliers and the broader supply chain.

Vulnerability Management
Establish policies and procedures for handling and reporting vulnerabilities when they happen.

Cybersecurity Training
Reinforce cybersecurity hygiene through regular training and drills.

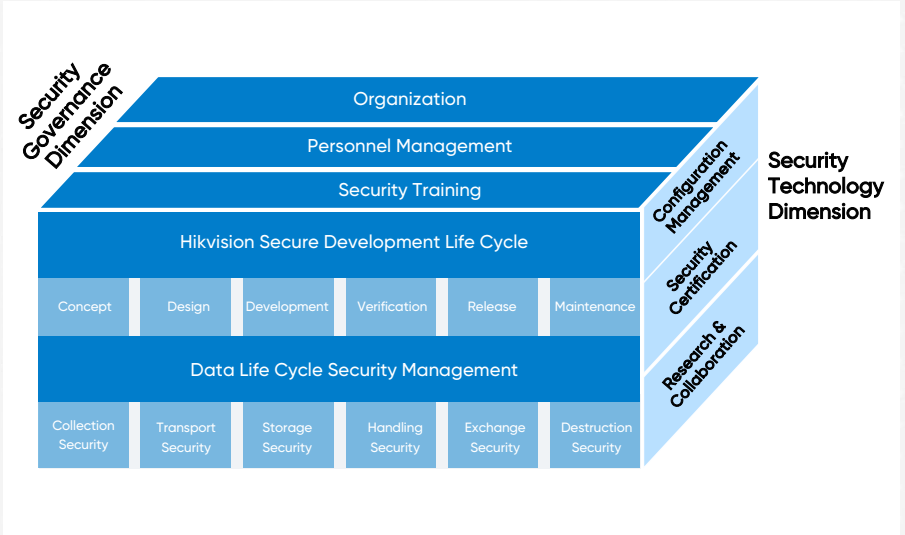
The above-mentioned requirements should not be considered fully comprehensive. To ensure that an organization fully complies with the NIS2 Directive, it is critical to consult with the appropriate compliance officer.

Hikvision's Practices in Response to the NIS2 Directive

Hikvision Security Development Maturity Model

Hikvision Security Development Maturity Model: Through extensive research and development efforts, along with insights from industry best practices such as OpenSAMM, BSIMM, CSDL, MSDL, and customer feedback, we have established the Hikvision Security Development Maturity Model (HSDMM). This model quantifies the security activities involved in product security development and integrates a comprehensive organizational structure, well-defined security development management processes, and robust technical measures to ensure the effective implementation of security activities. As a result, the HSDMM enhances product confidentiality, integrity, and availability while also strengthening personal data protection. Ultimately, this provides customers with safer products and solutions.

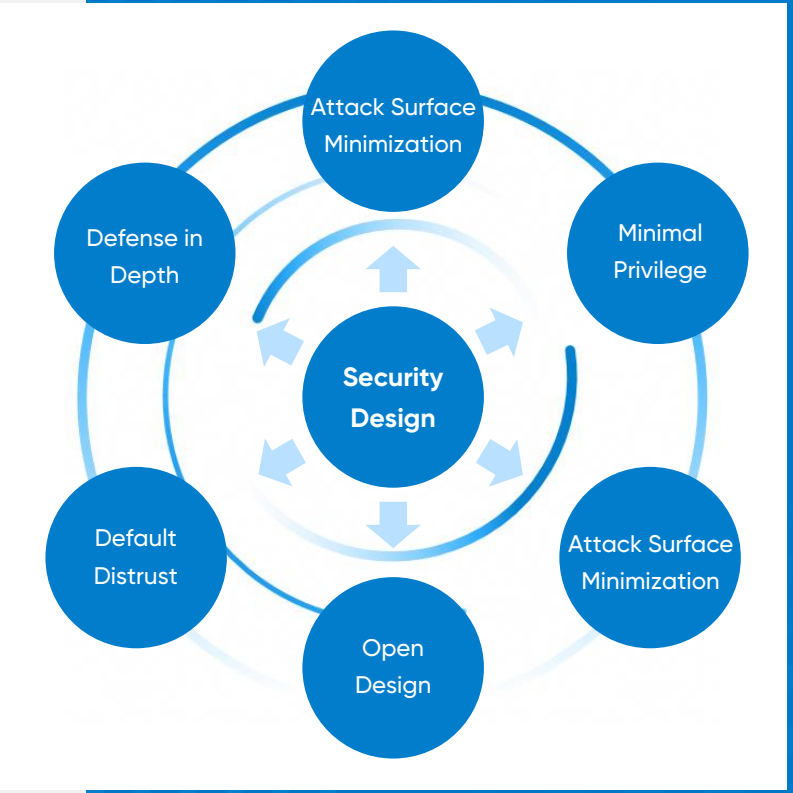
For more in the HSDMM, the Hikvision Cybersecurity White Paper explores it across three dimensions: security governance, security processes, and security technologies. We invite you to read the full Cybersecurity White Paper for further details.



Design stage

Integrating security measures at the earliest stages of product development is essential to ensure that security is a fundamental aspect of the design process rather than an afterthought. This approach involves implementing robust security principles, such as defense in depth, data encryption, access control, and regular security assessments throughout the product lifecycle. By embedding security into the design, Hikvision proactively addresses potential vulnerabilities and enhances the overall resilience of its products against cyber threats.

Hikvision devices follow the principle of security by default. Some security functions or configurations of the product are enabled by default. These security measures do not need to be configured by users. They provide basic security protection for the device and serve as the basis for other security reinforcement measures. Hikvision devices are pre-configured in factory default state with the following: insecure protocols, such as SSLv3.0, TLSv1.0/1.1, SNMPv2, etc. are turned off by default; management protocols are disabled by default and secure versions of these protocols are adopted to reduce exposure to attacks; products are open by default to ports only directly relevant to customers' demands, with all other ports closed.



Release stage

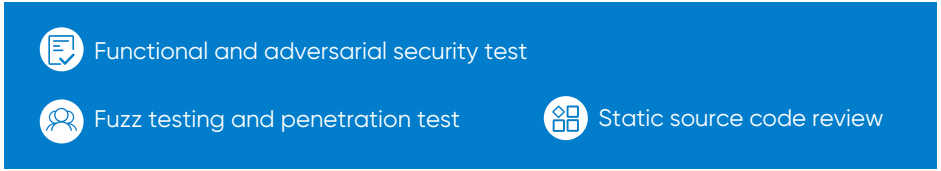
Before the product release, Hikvision follows a rigorous security test plan and strategy according to the product demand stage to complete the test. Our self-developed security testing platform enables a full range of testing methods, including:

- Functional and adversarial security test
- Fuzz testing and penetration test
- Static source code review
- Virus scanning

The product release packages of Hikvision are digitally signed by the product development management to ensure the source and integrity of the software release packages are verified, effectively avoiding illegal software packages.

Maintenance stage

To continuously protect customers after deployment, Hikvision has established the Hikvision Security Response Center (HSRC), which is responsible for receiving, addressing, disclosing, and resolving security-related vulnerability issues with Hikvision's products and solutions. Responsibilities include:



Hikvision is a member of the internationally renowned vulnerability information database Common Vulnerability & Exposures (CVE) as a CVE Partner. With this membership, Hikvision can obtain security vulnerabilities discovered by external organizations without delay, improve security emergency response speed, and provide customers with more secure products and solutions.

Hikvision promptly releases software updates to address emerging security issues. Users can see firmware update notifications on their devices and client software, and we encourage them to apply the latest firmware for security fixes as soon as possible. In addition, we recommend regular security hardening including updating configurations and installing security patches.

Device security

Device security is designed to ensure that all core components of each device provide security for both hardware and software. The tight coupling in Hikvision device hardware and software ensures each component of the system can be trusted and the whole system is verified. Security measures for each step, from the initial start to the software update, will be analyzed and examined.

Leadership awareness

The code for secure boot is embedded within the chip, ensuring that the device starts from a trusted foundation. The secure boot chain helps ensure that the software has not been tampered with. If any component fails verification, the boot process will halt, protecting the device from potential threats.

Password security

Hikvision devices incorporate robust account security measures to protect user access. These include strong password complexity requirements, activation mechanism and illegal login monitoring mechanisms.

Secure shell

To meet the requirements for debugging and maintenance, the devices support remote login through a secure SSH protocol. The devices utilize SSHv2, offering enhanced security to safeguard data in transit.

IP filtering

Hikvision devices support IP filtering technology to filter out unauthorized client objects, thus reducing the threat to the host. When devices are under attack, the IP filtering technology can complete specific defensive actions to enhance the device's ability to handle risks.

Authentication and authorization

To prevent unauthorized access and increase overall Hikvision device security, Hikvision supports:

Identity authentication

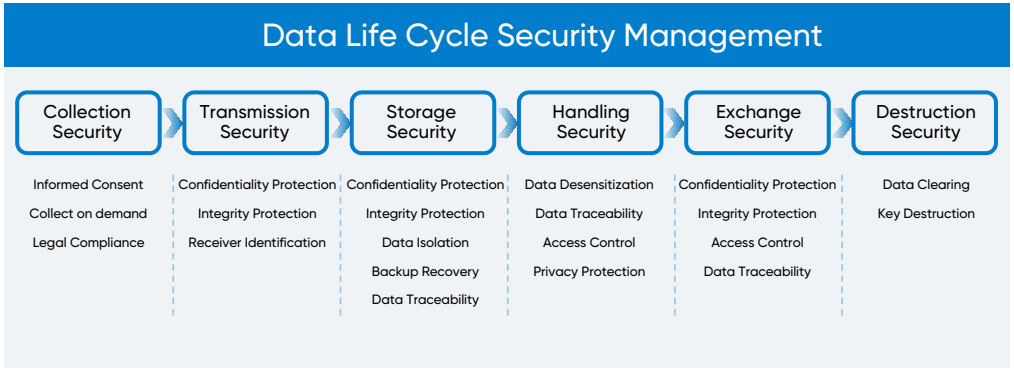
The identity management system defines and manages the access permissions of each user's identity role and required resources, and dynamically manages their required resource access permissions based on their identity role lifecycle, achieving functions such as unified identity management, unified identity authentication, unified access control, and permission compliance management.

Permission management

Hikvision limits the access permissions of applications, categorizes and grades permissions, and configures permissions based on business relevance and minimum authorization principles. Only authorized users can log in or access applications. Hikvision devices all support user permission and access control management, providing multi-dimensional security guarantees for user operations and device access control.

Data security

Protecting sensitive data during both transmission and storage is crucial. Hikvision employs advanced encryption algorithms to ensure the confidentiality and integrity of this data. The implementation of these encryption protocols is designed to safeguard data against unauthorized access and tampering.



Secure protocol

The network transmission of all Hikvision products supports secure transfer protocols such as HTTPS, TLS, and DTLS.

Digital watermark

Embedded or implicit watermarks, based on technologies such as information hiding and data encryption, help track and trace data usage and ensure copyright integrity.

White box encryption

White box encryption offers a unique approach to key protection by embedding cryptographic logic directly within application code, making it difficult for attackers to analyze keys from intermediate data.

Key management

The keys are securely stored within a hardware-protected zone and employ a layered key architecture. This structured approach to key management enhances the security of encrypted data.

Privacy protection

Hikvision applies privacy-by-design principles, integrating privacy considerations from the start of the development process. Data anonymization techniques are used to protect sensitive information and reduce the risk of data breaches. Additionally, Hikvision publishes a privacy policy and notices online outlining the types of personal data collected and how it is used. Other key points include:

Data Lifecycle Security Management

This ensures that data is protected throughout its entire lifecycle, from creation to deletion.

Syslog Log Management Service

This service provides comprehensive logging and monitoring, ensuring that all activities are tracked and can be audited.

Security Emergency Response

This involves implementing procedures to respond promptly and effectively to security incidents.

Multi-level Data Security Assurance

This supports various levels of data security to ensure that sensitive information is well protected.

These capabilities are designed to enhance the privacy and security of Hikvision products by ensuring that personal data is continuously protected, while also informing users and giving them control over their data. For example, we introduced “face mask” technology to protect the individual’s privacy.

Supply chain security

Supplier security agreement

All suppliers are required to comply with Hikvision's security, privacy, confidentiality, and audit policies. Clear guidelines — such as Third-party Component and Source Code Management Specifications — ensure that third-party components comply with our requirements.

Supplier monitoring, review and change

Hikvision monitors suppliers throughout the entire contract cycle and ensures security during the cooperation process. We conduct regular reviews and security evaluations, and we manage incidents involving third-party cybersecurity risks in a timely and transparent manner.

Third-party component security

Hikvision takes a proactive approach to managing open-source and third-party software. Through integration with the software management platform, Hikvision applies various binary and source code analysis tools to automatically detect potential vulnerabilities, compliance issues, and licensing risks during the development process.

Third-party component lifecycle management

A unified version information structure and Software Bill of Material (SBOM) repository ensure we have full visibility into third-party component usage. In case a security issue arises with a specific component version, we can quickly identify impacted products and take swift action for updates and mitigation.

Cybersecurity training

Comprehensive training programs are essential for enhancing cybersecurity awareness and skills among employees and customers. Hikvision provides regular security awareness and training to allemployees.

Regular training sessions and workshops

Ongoing sessions keep staff updated on the latest security practices and threats. Hikvision employees are trained to avoid and mitigate security threats to the organization.

Simulated cyber attack exercises

Realistic exercises help employees recognize and effectively respond to potential security incidents.

Continuous education and certification programs

Hikvision encourages continuous learning through certification programs to ensure that employees maintain a high level of cybersecurity expertise.

Hikvision's Commitment to Security

The NIS2 Directive is a key step toward defending against both current and emerging cyber threats. It aims to strengthen the security and resilience of our shared digital ecosystem.

Hikvision strongly recommends consulting your legal counsel to ensure your business activities comply with the NIS2 Directive. Hikvision, as your valued partner, is here to help you understand and prepare for this regulatory framework, providing our support with Hikvision expertise and training capabilities.

Operating and providing service throughout Europe from our headquarters in the Netherlands, Hikvision, while implementing the aforementioned practices, will also pay particular attention to the requirements of the NIS2 Directive as it is implemented in the Netherlands. We'll closely track its progress and, once the NIS2 Directive is transposed into the Dutch national law, make timely compliance adjustments and promptly register with the national mechanism established there.

Beyond compliance with NIS2 requirements, Hikvision is always dedicated to adhering to internationally recognized cybersecurity standards such as ISO 27001, ISO 27701, and CSA STAR, ETSI EN 303645, Common Criteria (CC), and Cybersecurity Labeling Scheme (CLS).- This commitment extends to secure development lifecycle practices and secure-by-design principles.

For more details, please visit our Cybersecurity Webpage.

HIKVISION | THRIVE