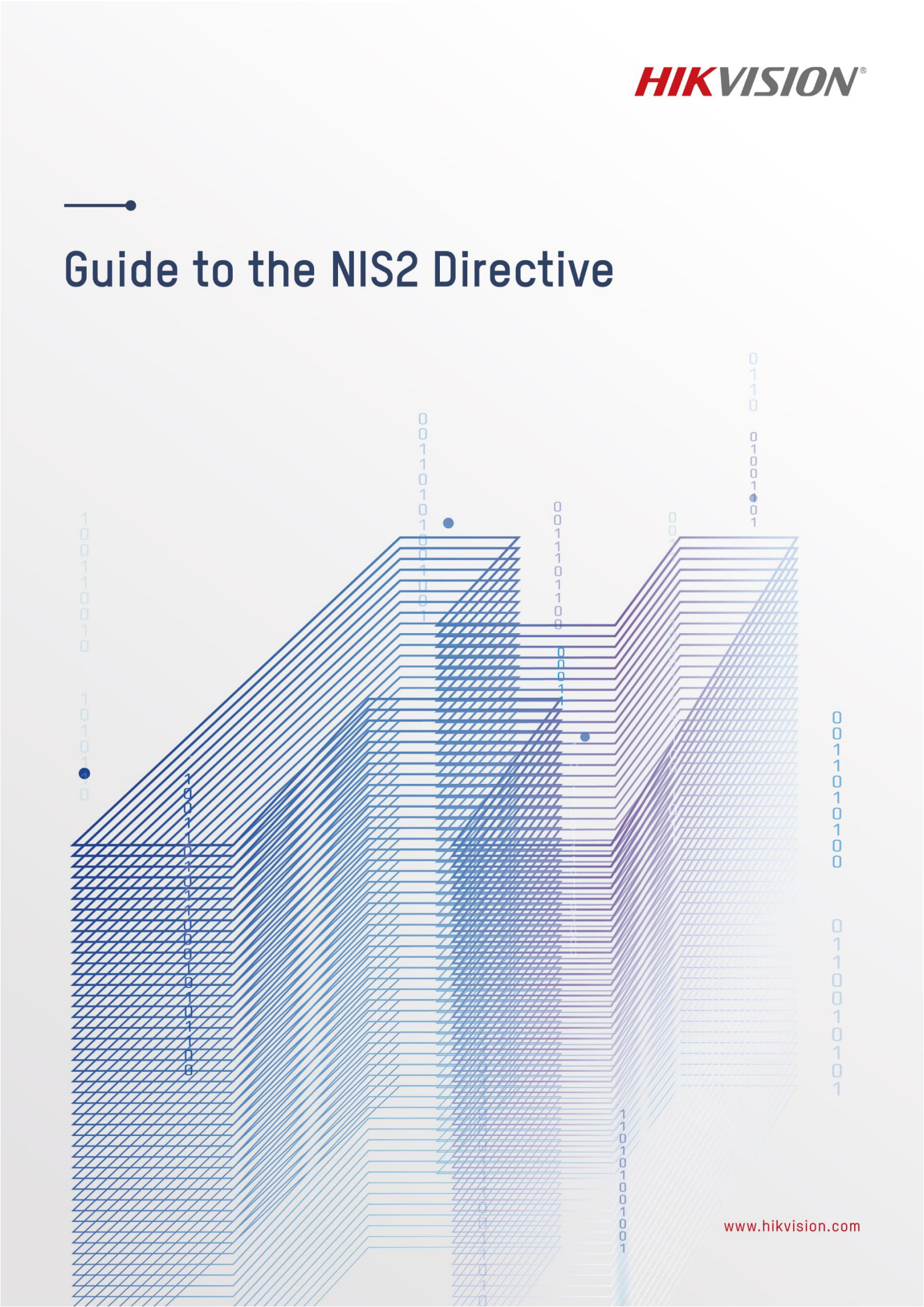
HIKVISION

Guide to the NIS2 Directive



www.hikvision.com

Copyright Disclaimer

Trademarks Acknowledgement

Legal Disclaimer

CONTENTS

Introduction

The "Network and Information Security Directive" (NIS2 Directive) has replaced and updated the first-ever European Union (EU) legislation on cybersecurity, the NIS1 Directive adopted in 2016. The aim of the NIS2 is to strengthen the collective cybersecurity level across EU Member States by increasing and harmonizing cybersecurity enforcement requirements for critical infrastructure sectors, strengthening cooperation among cybersecurity authorities, addressing the security of supply chains, and streamlining reporting obligations.

The Directive, which has been adopted by the European Parliament and the Council of the European Union (EU Member States) on 14 December 2022 and entered into force on 16 January 2023, expands its 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." The NIS2 seeks to correct the perceived shortcomings of the NIS1, eliminating the option to tailor adherence to the requirements and to modernize and strengthen the approach to cybersecurity across the EU. Each EU Member State now has until 17 October 2024 to transpose the NIS2 Directive into its national legislation.

The NIS2 Directive applies to all companies, suppliers, and organizations, including non-EU entities that deliver essential or important services in the EU. Entities that are under the scope of the Directive will face tougher cybersecurity regulation, with the possibility of administrative fines and/or withdrawal of license(s) to operate if organizations do not comply. Stricter requirements mean that concerned organizations now must lay out clear plans for how they perform risk management, control and oversight.

The Difference Between GDPR and NIS2

In simple terms, the NIS2 is for European cybersecurity what the GDPR has been for European personal data protection. Where the GDPR strengthened the requirements for how EU Member States manage personal data, the aim of the NIS2 is to ensure that all companies and organizations that are considered "essential" and "important" in these countries maintain an adequate level of cybersecurity to prevent and mitigate the impacts of cyber-attacks.

Who Will Be Impacted by NIS2

From a sector point of view, the goal of the NIS2 is to ensure that all organizations that maintain a critical position in society will be encompassed by the Directive to strengthen the overall level of Europe's cyber resilience. The broader scope of the NIS2 defines more sectors as "essential services,"

or sectors of "high criticality" that must implement cybersecurity risk management and prove that they are doing so. The Directive applies to all private and public entities which:

- Provide their services or carry out their activities in the EU
- Operate in at least one of the services listed below (Annex I and II of the NIS2 Directive) and meet or exceed the threshold to qualify as medium-sized or large enterprises:
    - 50 or more employees
    - Annual turnover exceeding €10 million

Essential (higher requirements) NIS1 originally covered	Important (lower requirements) NIS2 expands scope to include
Banking and Financial market infrastructure - credit, trade, market and infrastructure	*Digital providers (online marketplaces, search engines, social networking service platforms)*
Digital Infrastructure & ICT service providers - DNS(TLD), trust services, data center services, cloud computing, communication services, managed service providers and managed security providers, content delivery networks, providers of public electronic communications networks and providers of publicly available electronic communications services	*Foods - production and distribution*
Energy - supply, distribution, transmission and sales	*Manufacturers of certain critical products: computer electronic and optical products(**cameras**), electrical equipment, medical devices, machinery and equipment*
Healthcare - research, production, providers and manufacturers	*Motor vehicles, trailers and semi-trailers and other transport equipment*
Transport - aerial, rail, road and sea	*Postal & courier, parcel services*
Water supply - drinking and waste water	*Research*
Public administration, municipalities and regions	*Chemical products - production and distribution*
Space - software and services	*Waste management*

Member States have until 17 April 2025 to establish the list of essential and important entities, as well as entities providing domain name registration services. According to the estimates by the Belgian Center for Cybersecurity (CCB), there will be a twenty to fortyfold increase of entities in scope of the

NIS2 compared to the NIS1 Directive. It is expected that Member States will be able to adjust the methodology slightly.

How to Comply with NIS2

There are a number of minimum measures that the NIS2 compliance will require all relevant organizations to implement. Below is a general summary of the NIS2 requirement areas. These 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 internal/external compliance officer.

Required areas to be addressed (Art. 21):

- **Regular risk assessment and management**
  It is necessary for management to be aware of and understand the requirements of the Directive and the risk management efforts. They have a direct responsibility to identify and address cyber risks to comply with the requirements.
- **Cybersecurity training**
  Train and practice basic computer hygiene.
- **Security policies and procedures to manage cyber risks and incident handling such as incident resolution and reporting**
  Security procedures for employees with access to sensitive or important data, including policies for data access. The company must also have an overview of all relevant assets and ensure that they are properly utilized and handled.
- **Crisis management (business continuity, backup, recovery)**
  A plan for managing business operations during and after a security incident. This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.
- **Supply chain security (assessments)**
  Security around supply chains and the relationship between the company and direct suppliers. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.
- **Security of networks and information systems (development, maintenance)**
  The use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.
- **Vulnerability handling and reporting**
  Security around the procurement of systems and the development and operation of systems. This means having policies for handling and reporting vulnerabilities.

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

Impact of Not Complying with NIS2

The NIS2 increases the penalties in case of non-compliance. Member states can implement administrative fines and non-compliant entities can also face legal consequences.

Financial impact (fines)

- Essential companies: Companies categorized as "essential" risk fines up to €10 million or 2% of their global annual revenue.
- Important companies: Companies categorized as "important" risk fines up to €7 million or 1.4% of their global annual revenue.

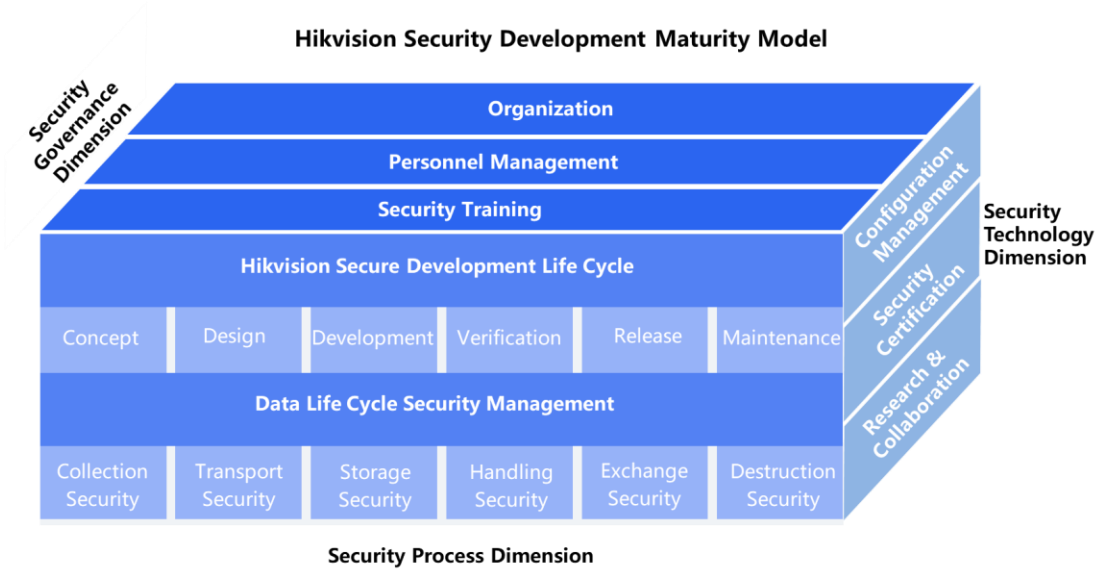
Legal impact

The consequences of not complying with NIS2 can go beyond financial fines. Management teams within non-compliant entities could be held legally accountable. In other words, the Directive now emphasizes that management can face legal ramifications if an entity fails to adhere to the new rules. Additionally, management needs to take courses to improve their ability to assess cybersecurity risks and encourage their organization to offer similar courses for all employees on a regular basis.

Hikvision Security Development Maturity Model (HSDMM)

With our extensive research and development efforts, and drawing on industry best security practices such as OpenSAMM, BSIMM, CSDL, MSDL, and customer feedback, we have established the Hikvision Security Development Maturity Model (HSDMM). Quantifying the security activities in product security development, this model integrates a comprehensive organizational structure, well-defined security development management processes, and robust technical measures to ensure the effective implementation of security activities. This, in turn, enhances product confidentiality, integrity, and availability, while strengthening personal data protection, ultimately providing customers with safer products and solutions.

The Hikvision Cybersecurity White Paper provides more information on the HSDMM from three dimensions: security governance, security processes, and security technologies. For more details, we invite you to read our Cybersecurity White Paper.



Hikvision Security Development Maturity Model (HSDMM)

Conclusion

The NIS2 Directive serves as an opportunity to better protect against the cyber-attacks of today and the future. It will make our collective digital ecosystem more safe and secure. When planning improvements, it will be imperative for impacted businesses to align with the NIS2 requirements to save time and reduce potential financial losses.

Hikvision is here to help companies prepare for this new regulatory framework, offering our partners support with Hikvision expertise and training capabilities. Hikvision is prepared to enact the changes needed to comply with the NIS2. Beyond compliance with NIS2 requirements, Hikvision adheres to internationally recognized cybersecurity standards such as ISO 27001, ISO 27701, and CSA STAR, in addition to secure development lifecycle and secure-by-design principles.

Guide to the NIS2 Directive

See Far, Go Further

HIKVISION®

Hangzhou Hikvision Digital Technology Co., Ltd.
No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China