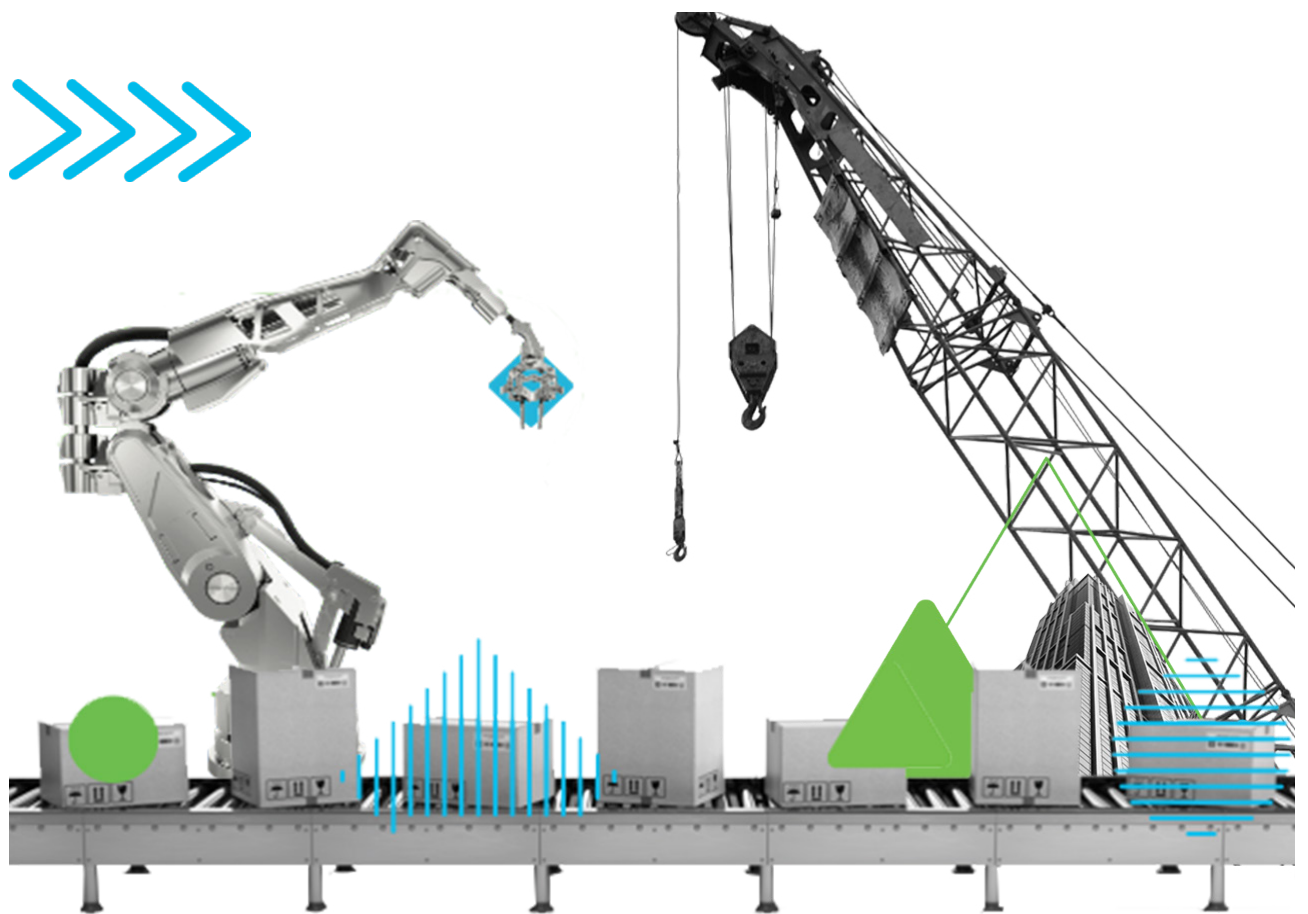


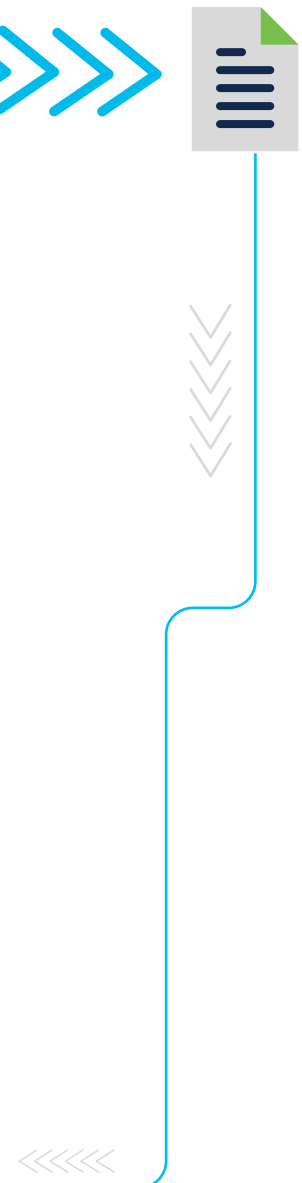
# NIS2 Compliance for Industries

Building industrial security capabilities to drive compliance



# Contents

<b>Executive summary</b>	<b>3</b>
<b>What is NIS2?</b>	<b>3</b>
Who must comply with NIS2?	4
Multinational organizations	5
What cybersecurity measures does NIS2 entail?	6
What are the reporting obligations?	7
Who controls compliance and how?	7
What are the penalties for noncompliance?	8
How does NIS2 differ from NIS1?	8
<b>Driving NIS2 compliance in industrial organizations</b>	<b>9</b>
How OT networks can address the 10 key NIS2 requirements	10
Benefiting from ISA/IEC 62443 to comply with NIS2	13
Cisco Validated Designs (CVDs)	14
Cisco services	14
Cisco Networking Academy	15
<b>Links and references</b>	<b>15</b>



## Executive summary

The European Network and Information Security (NIS2) directive outlines cybersecurity requirements for organizations operating in the European Union (EU) to ensure that there is a high, common level of protection across Member States. It addresses the limitations of the initial NIS directive established in 2016 with stricter requirements, an expanded scope of entities and sectors that must comply, and increased penalties for noncompliance.

An estimated 350,000 organizations<sup>1</sup> across the EU are affected by the NIS2 directive. Organizations, especially those engaging with NIS for the first time, will need to invest significant resources in understanding their responsibilities and ensuring compliance.

The directive applies to large and medium-sized organizations operating in critical industries such as energy, transportation, manufacturing, water, and healthcare, as well as banking, finance, digital services, and more. Depending on their size and the industry they operate in, organizations fall into the “Essential” or “Important” categories. Both must comply with the same security measures, but Essential Entities are proactively monitored and are subject to greater fines if they are found to be noncompliant.

Because NIS2 is a European directive, each EU Member State is responsible for transposing it into their local legislation and for enforcing it. Key requirements are the same, but local laws define specific procedures and implementation guidelines, driving toward the same objectives across the EU: ensuring that organizations that are part of the supply chain of critical infrastructures understand their exposure to cyber risks, implement cybersecurity best practices, and are able to detect, manage, and report incidents within a very short timeframe.

With the dramatic increase in cyberattacks against European organizations and the current geopolitical situation across the globe, NIS2 is a crucial step toward securing Europe’s critical infrastructures. This white paper details the main requirements of NIS2 and how organizations can benefit from the Cisco® security portfolio to drive compliance, safeguard their operations, and maintain a robust cybersecurity posture.

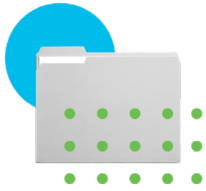
## What is NIS2?

In December 2022, the EU adopted an updated version of the NIS directive that was established in 2016. This NIS2 directive requires organizations operating in the EU to adopt a set of cybersecurity best practices and procedures to drive governance, risk management, and reporting.

It is designed to ensure the resilience of critical industries so as to safeguard European infrastructures and avoid a domino effect in case of major cyberattacks. NIS2 makes compliance mandatory by imposing significant financial penalties, establishing senior management’s liability, and reinforcing the role of local cybersecurity agencies to monitor and control organizations.

Because NIS2 is an EU directive, Member States must transpose it into applicable national law before October 17, 2024. NIS2 will be enforced as of October 18, 2024, although Member States have until April 17, 2025, to finalize the list of organizations that must comply.

<sup>1</sup>Source: radargrp.com



## Who must comply with NIS2?

In version 1 of the NIS directive, Member States were responsible for designating the organizations that were subject to the regulation. Not only does NIS2 apply to more industry sectors, but all organizations with more than 50 employees and annual revenues of over €10M now must comply, whether public or private. Member States can decide to add smaller entities to the list if they are considered to have a key role in the local economy or society.

The NIS2 scope is described in two annexes that list industry sectors to which the directive automatically applies. Annex I lists highly critical sectors. Annex II lists other critical sectors.

Figure 1. Industry sectors categorized as Annex I and Annex II under NIS2

Annex I sectors	Annex II sectors
 <p><b>Energy</b></p> <ul style="list-style-type: none"> <li>• Electricity*</li> <li>• Gas*</li> <li>• Oil*</li> <li>• Hydrogen</li> <li>• District heating and cooling</li> </ul>	 <p><b>Manufacturing</b></p> <ul style="list-style-type: none"> <li>• Medical devices</li> <li>• Compute, electronics, and optical products</li> <li>• Electrical equipment</li> <li>• Machinery</li> <li>• Motor vehicles, trailers, semi-trailers</li> <li>• Other transport equipment</li> </ul>
 <p><b>Transport</b></p> <ul style="list-style-type: none"> <li>• Air* · Rail* · Water* · Road*</li> </ul>	 <p><b>Digital providers</b></p> <ul style="list-style-type: none"> <li>• Providers of online marketplaces</li> <li>• Providers of online search engines</li> <li>• Providers of social networking services platforms</li> </ul>
 <p><b>Digital infrastructure*</b></p>	 <p><b>Postal and courier services</b></p>
 <p><b>Banking*</b></p>	 <p><b>Waste management</b></p>
 <p><b>Financial market infrastructure*</b></p>	 <p><b>Food production, processing, and distribution</b></p>
 <p><b>Health</b></p> <ul style="list-style-type: none"> <li>• Healthcare providers*</li> <li>• Pharmaceutical industry</li> </ul>	 <p><b>Production and distribution of chemicals</b></p>
 <p><b>Drinking water*</b></p>	
 <p><b>Wastewater</b></p>	
 <p><b>Public administration</b></p>	
 <p><b>Information and communication technology service management</b></p>	
 <p><b>Space</b></p>	

\*NIS1 scope

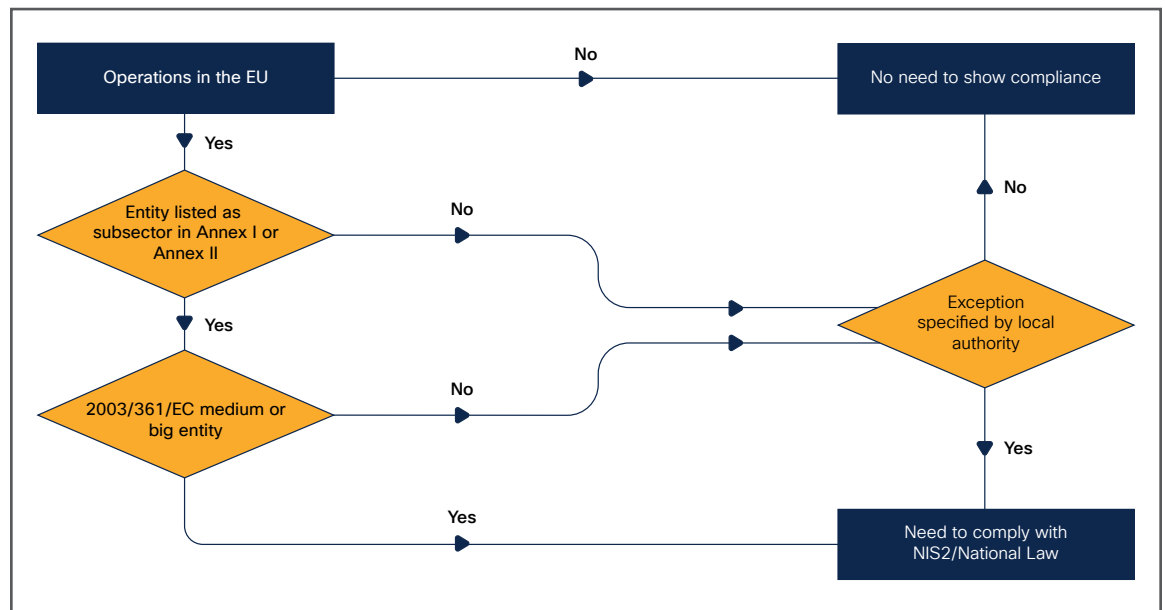
Under NIS2, the term “entity” describes any organization that must comply with the directive. It divides entities into two categories. Entities operating in sectors listed in Annex I can be categorized as “Essential” or “Important,” depending on their size and revenues. Entities in Annex II can only fall in the “Important” category.

Both categories must follow the same requirements and comply with the same security measures, but Essential Entities will be proactively monitored, whereas Important Entities will be audited only after a cybersecurity incident. Essential Entities face higher penalties, and their senior managers are held accountable for noncompliance. In other words, the control of Essential Entities is stricter due to the possible more dire consequences if that organization is found to be noncompliant.

Table 1. Categorization of Essential and Important Entities by size and revenues

Size of entity	Number of employees	Revenue (M€)	Annex I sector	Annex II sector
<b>Large</b>	$x \geq 250$	$y \geq 50$	Essential Entities	Important Entities
<b>Medium</b>	$50 \geq x > 250$	$10 \geq y > 50$	Important Entities	Important Entities
<b>Small</b>	$x < 50$	$y < 10$	Not concerned	Not concerned

Figure 2. Flowchart for determining the need to comply with NIS2



### Multinational organizations

Organizations based outside the EU but offering critical services within the EU must comply with NIS2. Verify whether your industry sector is listed in Annex I or Annex II and, if you qualify as an “Essential” or “Important” Entity, identify which local regulation you must comply with in each Member State you operate in.

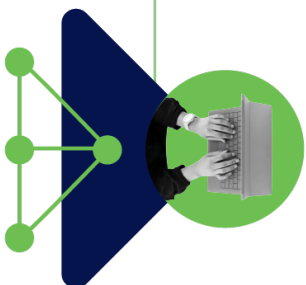
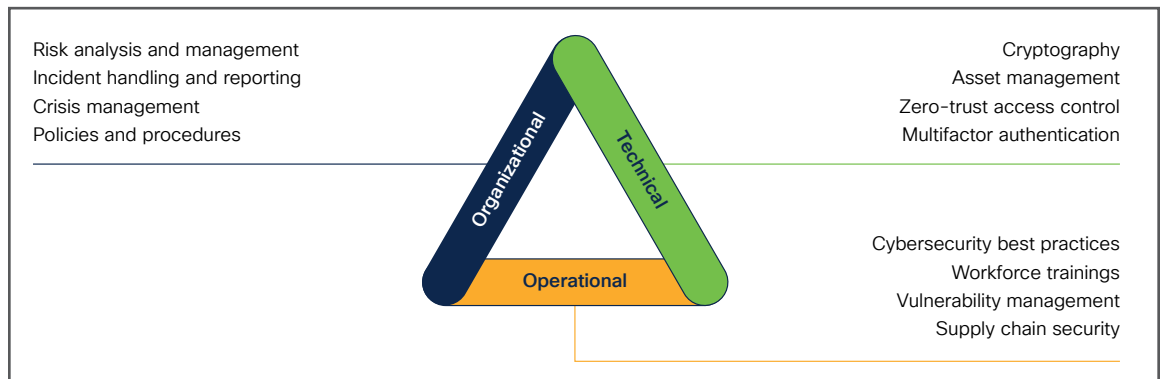


## What cybersecurity measures does NIS2 entail?

Cybersecurity measures that Essential and Important Entities must comply with are defined by each Member State in their national transposition of the directive. However, NIS2 imposes a risk management approach with a list of basic security measures to implement:

- Risk analysis and information system security policies.
- Incident handling, including prevention, detection, response, and recovery.
- Business continuity measures—such as backups and disaster recovery—and crisis management.
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.
- Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure.
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.
- Basic cyber hygiene practices and cybersecurity training.
- Policies and procedures regarding the use of cryptography and encryption.
- Human resources security, access control policies, and asset management.
- Use of multifactor authentication, secured voice, video, and text communications, and secured emergency communication systems within the entity.

Figure 3. Organizational, technical, and operational categories of NIS2 security measures








## What are the reporting obligations?

Although the NIS directive has always required organizations to report cybersecurity incidents, NIS2 makes it a legal obligation to report “significant” incidents and describes a clear and strict process for doing so.

To maintain compliance, entities must notify the local Computer Security Incident Response Team (CSIRT) or any other competent authority in their country according to the timeline below once an incident has occurred.

Figure 4. Timeline for required notifications of cybersecurity incidents

24 hours	72 hours	1 month
 <b>Early warning</b> Mandated to report any significant incident within 24 hours of becoming aware of it, regardless of whether it had any direct impact on operations.	 <b>Incident notification</b> Updated report within 72 hours of becoming aware of the incident, describing the nature of the incident and its severity, impacts, and indicators of compromise.	 <b>Final report</b> Detailed description of the incident must be submitted within 1 month, explaining its potential causes, ongoing mitigation measures, and cross-border impact.

The directive requires entities to implement incident detection and response mechanisms. They need to quickly identify incidents and assess their impact. Depending on the context, they may be required to inform their customers and the public.

## Who controls compliance and how?

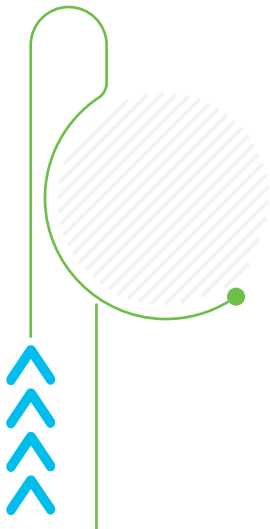
The NIS2 directive requires each Member State to designate at least one competent authority to drive the implementation of the directive in the country and monitor the compliance of entities within the directive’s scope. CSIRTs must also be established to monitor and analyze threats and incidents, collect forensic data, alert entities and other relevant stakeholders, and provide assistance when needed.

Authorities have the power to control entities in the manner listed in the table below.

Table 2. Controls imposed on Essential and Important Entities

Essential Entities	Important Entities
Comprehensive controls in advance or when an incident is reported or if there are doubts about compliance (ex-ante and ex-post supervisory regime).	Light controls when an incident is reported or if there are doubts about compliance (ex-post supervisory regime).
Onsite inspections and offsite supervision.	Ex-post onsite inspections and offsite supervision.
Regular and targeted security audits.	Targeted security audits.
Security scans.	Security scans.
Information requests.	Information requests.
Requests for information to assess the cybersecurity policies and risk-management measures in place.	Requests for information to assess, ex-post, the cybersecurity policies and risk management measures in place.
Ad hoc audits, for example, after a significant incident.	





## What are the penalties for noncompliance?

The original version of the NIS directive let Member States define sanctions for noncompliance, leading to many disparities across the EU. NIS2 imposes a common sanctions regime designed to be effective, proportionate, and dissuasive.

Sanctions are imposed in addition to the audits, inspections, and controls listed above and can range from simple warnings to orders to cease conduct, orders to implement measures, orders to inform the public, administrative fines, and more.

In addition, Essential Entities can see their certification or authorization to operate suspended. The authority can also designate a monitoring officer to oversee the compliance. Senior managers can be personally held liable for infringements. They are required to approve the cybersecurity measures taken, oversee their implementation, attend trainings, and offer similar trainings to employees.

Last but not least, both Essential and Important Entities face significant financial fines when proven noncompliant.

Table 3. Sanctions for noncompliance with NIS2

Essential Entities	Important Entities
<ul style="list-style-type: none"> <li>• 2% of worldwide turnover with €10M minimum</li> <li>• Suspension of certification</li> <li>• Management liability</li> <li>• Monitoring officer designated</li> </ul>	<ul style="list-style-type: none"> <li>• 1.4% of worldwide turnover with €7M minimum</li> </ul>

### How does NIS2 differ from NIS1?

NIS2 was designed to address the limitations of the previous directive to better respond to the evolving cyberthreat landscape and ensure stronger resilience of critical infrastructures. It expands the NIS regulations with:

- More industry sectors and more organizations in its scope.
- Extra cybersecurity requirements.
- Shorter incident notification deadlines.
- Similar control procedures and penalties across all Member States.

The directive also has additional requirements for supply chain cybersecurity, stronger compliance supervision from the national authorities, and established guidelines for cybersecurity information that were not outlined in the previous directive.



## Driving NIS2 compliance in industrial organizations

Whereas the original NIS directive affected only a few highly critical organizations, NIS2 automatically applies to most organizations across many more industrial sectors. The objective is to strengthen Operational Technology (OT) security practices in the European Union.

Industrial networks used to be isolated from the rest of the enterprise and the internet. As organizations are digitizing operations and deploying Industry 4.0 technologies, seamless communications between IT, cloud, and operational networks are needed, exposing OT assets to grave cyberthreats and increasing the attack surface of critical industrial infrastructures.

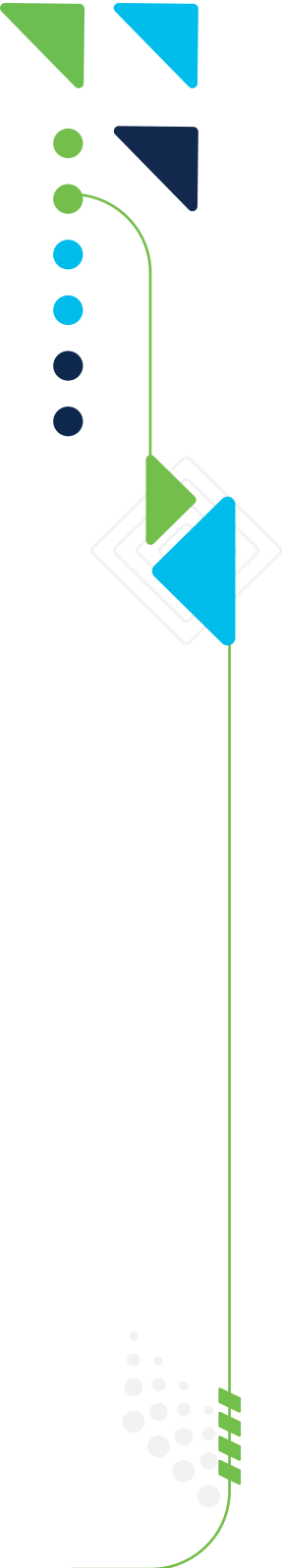
The NIS2 directive lists cybersecurity requirements that can help securely converge IT and OT networks, protect industrial operations, and improve critical infrastructure resilience while enabling their modernization. In addition to driving regulatory compliance, implementing these NIS2 requirements can help industrial organizations achieve great benefits, such as:

- Reducing operational costs by preventing or mitigating cyberattacks to maintain uptime and operational efficiency.
- Improving efficiency by streamlining processes, resulting in enhanced performance.
- Achieving innovation by adopting new technologies and developing new products or services, all with the highest level of security.

## How OT networks can address the 10 key NIS2 requirements

Table 4. Addressing NIS2 cybersecurity requirements in OT networks

NIS2 cybersecurity requirement	What should you look for?	Cisco solutions
<p><b>Risk analysis and information system security policies</b></p>	<p>Organizations should look to gain a security posture for the OT network. Your asset visibility tool should provide an inventory of all connected OT assets, determine the risk those devices pose to the network, and prioritize those risks to facilitate remediation.</p> <p>Cisco Cyber Vision, embedded in Cisco industrial network equipment, combines protocol analysis, intrusion detection, and vulnerability detection to help you inventory these OT assets and understand the security posture of your OT network.</p>	<p>Cisco Cyber Vision</p> <p>Cisco Vulnerability Management (formerly Kenna)</p> <p>Cisco Technical Security Assessment Service</p>
<p><b>Incident handling, including prevention, detection, response, recovery, and reporting.</b></p>	<p>Organizations should first organize one or more persons responsible for handling the response to and analysis of indicators of compromise, followed by the implementation of an incident response plan. A sufficient incident response plan offers a course of action for all significant incidents, such as having a structure in place to help IT staff stop, contain, and control the incident quickly.</p> <p>Cisco Cyber Vision provides a means of detecting activity within the industrial network while also integrating into response tools such as Cisco Identity Services Engine (ISE) for policy control and Cisco Extended Detection and Response (XDR) for incident investigation and response.</p>	<p>Cisco Cyber Vision</p> <p>Cisco Identity Services Engine</p> <p>Cisco Secure Firewall</p> <p>Cisco XDR</p> <p>Cisco Secure Network Analytics</p> <p>Cisco Secure Endpoint</p> <p>Cisco Talos® Threat Intelligence</p> <p>Cisco Talos Incident Response Services</p>
<p><b>Business continuity measures—such as backups and disaster recovery—and crisis management.</b></p>	<p>In addition to creating and storing backups for data and processes, organizations should architect their networks to allow critical networks to run in isolation. If one part of the network becomes compromised, the rest of the network should be able to run in a degraded state until the affected systems are fully restored.</p> <p>Cisco ISE enables IT administrators to isolate one or more devices while investigations are conducted. With ISE, compromised systems can continue to communicate on the network but with limited privileges, allowing the system to run in isolation, but disabling the ability for any potential compromise to spread throughout the environment.</p>	<p>Cisco Cyber Vision</p> <p>Cisco Identity Services Engine</p> <p>Cisco Catalyst™ Center</p> <p>Cisco XDR</p> <p>Cisco Talos Incident Response Services</p> <p>Network Segmentation Design and Implementation Services</p>

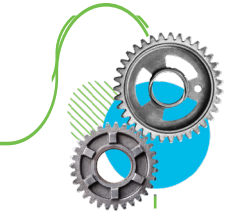


NIS2 cybersecurity requirement	What should you look for?	Cisco solutions
<p><b>Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.</b></p>	<p>Organizations should look to implement secure-by-design hardware and software. ISA/IEC 62443 is a globally recognized standard for securing critical infrastructures. Part 4-1 describes the requirements for a product security development lifecycle, which Cisco’s Secure Development Lifecycle (SDL) is certified to meet. Additionally, Part 4-2 describes the technical security requirements for Industrial Automation and Control Systems (IACS). Cisco Catalyst IE3100, IE3200, IE3300, IE3400, and IE9300 Series switches are certified to meet this standard.</p> <p>Cisco has a unique offering for NIS2 compliance that combines asset visibility, security posture, network segmentation, and Zero-Trust Network Access (ZTNA) within ISA/IEC 62443 certified networking hardware.</p> <p>To further address risks from suppliers or service providers, Cisco Secure Equipment Access (SEA) enables ZTNA to OT assets within the critical network. Unlike a VPN, which extends the network to remote clients and makes it difficult to control who can access what, Cisco SEA starts with a default deny posture and adaptively grants access only to specific resources at specific times based on identity and context policies. Sessions can be monitored, recorded, and terminated. Comprehensive audit trails are provided to help investigations and compliance.</p>	<p>Cisco Catalyst industrial networking portfolio</p> <p>Cisco Secure Development Lifecycle</p> <p>Cisco Secure Equipment Access</p> <p>Zero-Trust Infrastructures Design and Implementation Services</p>
<p><b>Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure.</b></p>	<p>Even when an organization deploys secure components, vulnerabilities will inevitably present themselves. Organizations should deploy tools that automatically inventory OT assets, identify their vulnerabilities, and ingest them into a vulnerability management solution for remediation and risk reduction.</p> <p>Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world and provides vulnerability information to Cisco Cyber Vision. Cisco Cyber Vision identifies the vulnerabilities within an OT network, detailing the Common Vulnerability Exposure (CVE) ID, Common Vulnerability Scoring System (CVSS), and a device risk score that provides guidance on which vulnerabilities should be prioritized.</p> <p>Cisco Vulnerability Management (formerly Kenna) adds a Cisco Security Risk Score to vulnerabilities found in the network. The system factors in both internal and external variables as potential risk indicators. Internal factors consider the frequency, severity, and criticality of each vulnerability. External factors consider the CVSS score, the Exploit Predication Scoring System (EPSS), and threat and exploit intelligence data from more than 19 different threat and exploit feeds to determine exploit kit availability, exploit volume and speed, and the vulnerability’s prevalence.</p>	<p>Cisco Cyber Vision</p> <p>Cisco Vulnerability Management (formerly Kenna)</p> <p>Cisco Talos Threat Intelligence</p>



NIS2 cybersecurity requirement	What should you look for?	Cisco solutions
<p><b>Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.</b></p>	<p>There are often more vulnerabilities than an organization has the capacity to fix. That is why prioritization of vulnerabilities is so important.</p> <p>Cisco Cyber Vision applies a risk score to all devices and device groups discovered in the OT network. Using a combination of vulnerabilities, activities, and impact, risk scores provide guidance as to which devices should be addressed first when implementing risk-management measures.</p>	<p>Cisco Cyber Vision</p> <p>Cisco Vulnerability Management (formerly Kenna)</p> <p>Post-Deployment Assessment and Continuous Improvement Services</p>
<p><b>Basic cyber hygiene practices and cybersecurity training.</b></p>	<p>It is critical that organizations continuously train their workforce so that all employees understand the critical role they have in securing the organization. They should receive information about social engineering and learn how to identify phishing attempts, for instance.</p> <p>The Cisco Networking Academy® offers both free self-paced cybersecurity training and paid instructor-led training. Introductory courses offer guidance on how to be more cyber-aware, while advanced courses develop the skills needed to protect networks and prevent intrusions.</p> <p>By analyzing data flowing through the network, Cisco Cyber Vision provides a view of the cyber hygiene within the OT environment. Are passwords being sent in cleartext protocols? Are the vulnerabilities in the network being taken care of? Are any devices speaking to public IP addresses that should not be? By having a view of the activity in the network, network administrators can actively monitor whether best practices are being followed and act when bad practices appear.</p>	<p>Cisco Cyber Vision</p> <p>Cisco Secure Network Analytics</p> <p>Cisco Networking Academy</p> <p>Talos Cyber Range Training</p>
<p><b>Policies and procedures regarding the use of cryptography and encryption.</b></p>	<p>By using encryption on data in motion, organizations protect themselves from network sniffing attacks. Additionally, organizations should encrypt data at rest, to prevent malicious users from stealing data in the event of an access control breach.</p> <p>In an OT environment, it is not always possible to encrypt data as it flows through the network, as many legacy protocols still use unencrypted communication channels. However, there are some protocols that can be avoided, and by passively listening to the network, Cisco Cyber Vision provides a list of all devices on the network using unencrypted communication, which can be used to determine if any devices are violating policy.</p>	<p>Cisco Cyber Vision</p> <p>Cisco Secure Network Analytics</p> <p>Cisco Encrypted Traffic Analysis</p>





NIS2 cybersecurity requirement	What should you look for?	Cisco solutions
<p><b>Human resources security, access control policies, and asset management.</b></p>	<p>Often referred to as zero trust, this identity-driven approach to security allows access to resources only on the principle of least privilege. This requires maintaining a detailed inventory of all connected assets and defining policies to ensure that users and machines have access only to the resources required to perform their role.</p> <p>Using Security Group Tags (SGTs), Cisco ISE unifies access control policies across user and device groups, enabling granular control of the systems that any given user group can gain access to.</p> <p>When accessing OT assets remotely, Cisco Secure Equipment Access (SEA) enables ZTNA control, granting access only to specific resources at specific times, using specific protocols based on identity and context policies.</p>	<p>Cisco Cyber Vision Cisco Identity Services Engine Cisco Secure Equipment Access Cisco Duo Cisco Secure Access Security Strategy, Risk, and Compliance Services Network Segmentation Design and Implementation Services</p>
<p><b>Use of multifactor authentication, secured voice, video, and text communications, and secured emergency communication systems within the entity.</b></p>	<p>The threat of stolen credentials is still one of the largest attack vectors to any organization, and critical networks are no different. Organizations should secure user accounts by implementing Multifactor Authentication (MFA) for all password-protected applications and remote access services.</p> <p>Adopting MFA is relatively simple with Cisco Duo, as it doesn't require any hardware or software. Duo also checks that user devices comply with your security policy before allowing them to connect.</p> <p>To secure remote access to OT assets, Cisco SEA integrates with your existing identity provider through Security Assertion Markup Language (SAML) if an MFA solution has already been implemented. In other cases, native MFA can be enabled.</p>	<p>Cisco Secure Equipment Access Cisco Duo Cisco Secure Access</p>

### Benefiting from ISA/IEC 62443 to comply with NIS2

NIS2 stresses the use of international standards to ensure that entities within its scope implement effective cyber risk-management measures.

ISA/IEC 62443 is a key cybersecurity standard for designing secured IACS infrastructures. It is widely used in many sectors where NIS2 applies, such as power utilities, manufacturing, oil and gas, and more. Organizations that have experience with ISA/IEC 62443 are in a good position to achieve compliance with NIS2.

Deploying certified components helps drive compliance by ensuring a secured supply chain. Cisco's industrial networking portfolio comprises various products that are certified against ISA/IEC 62443-4-1 (secure product development lifecycle) and ISA/IEC 62443-4-2 (technical security requirements for IACS components).

[Implementing the ISA/IEC 62443 cybersecurity framework](#)—especially parts 2-1, 3-2, and 3-3—goes a long way toward NIS2 compliance, as it includes most of its key requirements such as risk analysis, access control, strong authentication, use of cryptography, continuous monitoring, business continuity and disaster recovery, and more.

It is important to note that the NIS2 directive envisions a European certification scheme that is currently under development for cloud services, 5G, and consumer IoT, as well as for industrial infrastructures. The industrial infrastructure certification scheme will likely be based on or derived from ISA/IEC 62443. Any experience with or certification for these standards will help entities within the NIS2 scope achieve certification.

### Cisco Validated Designs (CVDs)

For more than 20 years, Cisco has been helping industrial organizations around the globe digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more. Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. It is a rare combination.

By designing, developing, and testing products together, Cisco enables IT and OT teams to achieve advanced outcomes while reducing the complexity, time, and gaps incurred by the need to make point products work together. Our solutions come with comprehensive design and implementation guides that will help you reduce risk, accelerate implementation, and make the most of your technology stack.

[Cisco's OT security reference design](#) is a blueprint for a secured, robust, and reliable industrial network. It leverages Cisco's comprehensive networking and security technologies to provide industrial asset visibility, macro/zone segmentation, zone access control, threat detection, and response. It extends IT security technologies to the operational world for consistent access policy management and aggregation of industrial security events in the Security Operations Center (SOC), so organizations have global visibility into both their IT and OT domains to manage risks and drive governance and compliance effectively.

### Cisco services

More than just deploying technical solutions, NIS2 compliance is about requiring entities to assess their existing cybersecurity practices, understand risks, identify gaps, and drive change. Cisco is an acknowledged industry thought leader in cybersecurity, with an [extensive service offering](#) that will support customers across the globe and in all industry sectors to achieve compliance. Cisco can assist with expertise, insights, recommendations, advisory capacity, and services in addition to products.

With broad expertise in specific NIS2 requirements, Cisco and its partner network can help entities assess, design, implement, and maintain a future-ready security architecture and advise them on organizing security incident management and implementing tools, processes, and procedures, as well as designing and implementing critical incident report capabilities.

Table 5. Sample Cisco services related to NIS2 compliance

Product type
<b>Operational Maturity Assessment</b>
<b>Security Architecture Framework</b>
<b>Security Strategy, Risk, and Compliance Services</b>
<b>Technical Security Assessment Services</b>
<b>Incident Response Services</b>
<b>Network Segmentation Design and Implementation Services</b>
<b>Zero-Trust Infrastructures Design and Implementation Services</b>
<b>Security Solution Planning, Design, and Implementation Services</b>
<b>Post-Deployment Assessment and Continuous Improvement Services</b>

## Cisco Networking Academy

As all organizations are strengthening their cybersecurity practices and hiring more talent, there are currently more than 3.5 million vacancies in the cybersecurity field worldwide, including 350,000 in Europe. Training more experts is key to filling the skills shortage gap and protecting critical infrastructures.

The [Cisco Networking Academy](#) is the world's largest and longest-running corporate social responsibility education program. It is dedicated to helping develop the workforce of the future through an unmatched ecosystem of partnerships, including governments, academic institutions, and nonprofits. In 2023, Cisco announced its [goal to train 250,000 people](#) with cybersecurity skills across the EU over the next three years.

In addition, the Cisco Networking Academy's [Skills for All](#) platform provides best-in-class content that is accessible to as many learners as possible. It offers free self-paced cybersecurity training to anyone looking for introductory content, and even advanced courses to develop the skills needed to protect networks and prevent intrusions.

## Links and references

- [Official text of the NIS2 directive.](#)
- [European Commission's web portal on NIS2.](#)
- [ENISA's NIS website.](#)
- [ISA/IEC 62443-3-3: What is it and how to comply?](#)
- [Cisco OT security solution.](#)
- [Cisco Secure portfolio.](#)
- [Cisco Technical Security Assessment Services.](#)
- [Cisco Networking Academy.](#)
- [Contact Cisco](#) to discuss your needs for NIS2 compliance.