NIS2 Services

Does NIS2 apply to your organization? Then you are required to comply with this EU directive from October 2024. This will involve effort. We can help you with this - from the start of your compliance process to full NIS2 compliance.

These NIS2 Services give you:

Insight into gaps
You gain insight into your current security controls and any gaps with NIS2 requirements.

A clear road map
You receive concrete recommendations for improvement, so that you can take action.

Help with implementation
You receive expert help with implementing measures needed for NIS2 compliance.

Why NIS2 Services?

To raise the cyber resilience of its member states, the EU has adopted the the **Network and Information Security (NIS2)** directive. This directive applies to around 160.000 European organizations in important sectors such as transport, government, energy and healthcare. If NIS2 applies to your organization, your organization faces a number of obligations.

For instance, the directive requires that you adopt a risk-based approach and implement appropriate security measures. It also expects you to report significant cyber incidents to the relevant competent authority. From October 2024 onwards, you are subject to audits from local supervisors. We can help you prepare for compliance to NIS2.

Which NIS2 Services do we offer?

NIS2 Boardroom Training	NIS2 Gap Assessment	NIS2 Implementation Support	Risk Management	Supply Chain Security

NIS2 Boardroom Training

The **NIS2 Boardroom Training** empowers your executives to make informed decisions about NIS2. This is important because NIS2 explicitly holds board and senior management accountable for compliance with the directive. You will receive relevant legal insights from our partner **De Clercq Lawyers and Notary**. After this one-day training:

- Your board will have sufficient knowledge to judge which measures are needed to protect your organization from cyber threats.
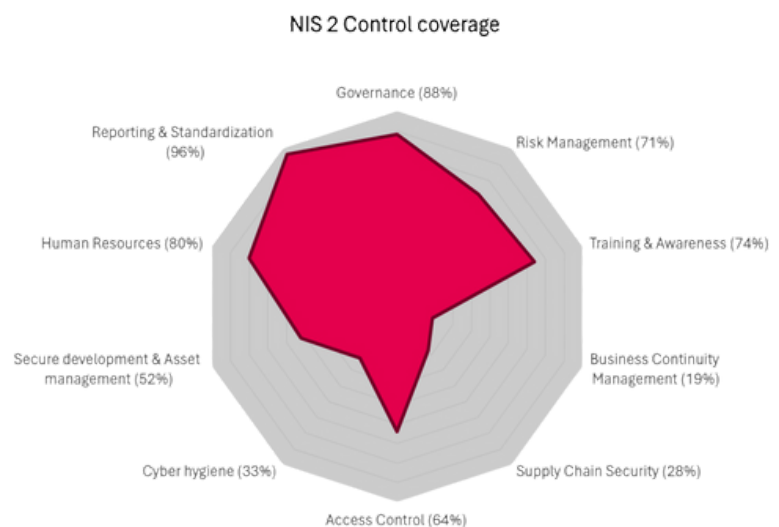
- You will meet the boardroom training requirements of NIS2.

NIS2 Gap Assessment

You can also conduct a **NIS2 Gap Assessment.** What is the security maturity level of your organization? Which gaps are there when it comes to NIS2 compliance and which steps are needed to bridge these?

To assess this, we use a selection of the ISO 27001 standard, expanded to incorporate all additional NIS2 requirements not yet covered by default. You will see the outcome in a graphic like this:

NIS 2 Control coverage

- Governance (88%)
- Risk Management (71%)
- Training & Awareness (74%)
- Business Continuity Management (19%)
- Supply Chain Security (28%)
- Access Control (64%)
- Cyber hygiene (33%)
- Secure development & Asset management (52%)
- Human Resources (80%)
- Reporting & Standardization (96%)

The results of the Gap Assessment give you insight into your maturity and the identified gaps. You will receive concrete recommendations for improvement.

NIS2 Implementation Support

Depending on the gaps revealed by the NIS2 Gap Assessment, we offer assistance with implementation. You may need specific cybersecurity services to close certain gaps. We can help you with this.

Maybe you want to invest in awareness: we offer a **SAFE Awareness Program.** This program is designed to achieve actual behavioral change.

Do you need an incident response plan? The **Incident Response PRO** service helps you prepare for potential incidents and guarantees help in case of one.

The complete security service **CyberCare** helps you plan and implement necessary cybersecurity measures. We can act as your independent, trusted advisor.

Risk Management

Article 21 of NIS2 requires organizations to manage network and information system security risks. We can help you do this. For example, by reviewing existing security risk methodology, defining the methodology for the organization and performing risk assessments.

Supply Chain Security

NIS2 requires you to manage the security risks around your suppliers and service providers. Are you looking to identify potential weaknesses in your supply chain? We can help you with a Vendor Assessment.

What our customers say

"We're glad we started on time"

"We thought we had NIS2 covered, since we are ISO 27001 certified. However, Secura's Gap Assessment showed us that some of our critical processes were not covered by our ISO certification."

More information on NIS2

Does NIS2 apply to you?
NIS2 applies to important and critical sectors in Europe. In most cases it is quite easy to determine whether the directive applies to your organization. You can find out if NIS2 applies to you using our flowchart: **secura.com/nis2**

Practical Guide to NIS2
What are the main requirements of NIS2? What do they mean in practice? Read more in this Practical Guide to NIS2, written by NIS2 experts: **secura.com/nis2**

Webinars and events
Do you want to know more about NIS2 and what it means for your organization? Our consultants regularly share their expertise during webinars and events. You can find upcoming webinars and events on **secura.com/events**

About Secura / Bureau Veritas

Secura is a leading cybersecurity company. We help customers all over Europe to raise their cyber resilience. Our customers range from government and healthcare to finance and industry. We offer technical services, such as vulnerability assessments, penetration testing and red teaming, but also provide audits, forensic services and awareness training.

Secura is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80.000 employees and is active in 140 countries.

Example case | NIS2 Services

Which problem did the customer have?
A multinational product manufacturer in the transport sector, with sites all over Europe, wanted to reach NIS2 compliance. Due to the size, complexity and required expertise, they asked us to assist them end-to-end.

Result
We helped this customer to identify the scope and applicability of NIS2, together with their legal department. We also identified gaps in regard to NIS2 compliance, created a global risk assessment methodology and finally supported the implementation of our recommendations.

Interested?

Contact us today to start raising your cyber resilience.

✉ **info@secura.com**

☎ **+31 (0) 88 888 3100**

🌐 **secura.com**