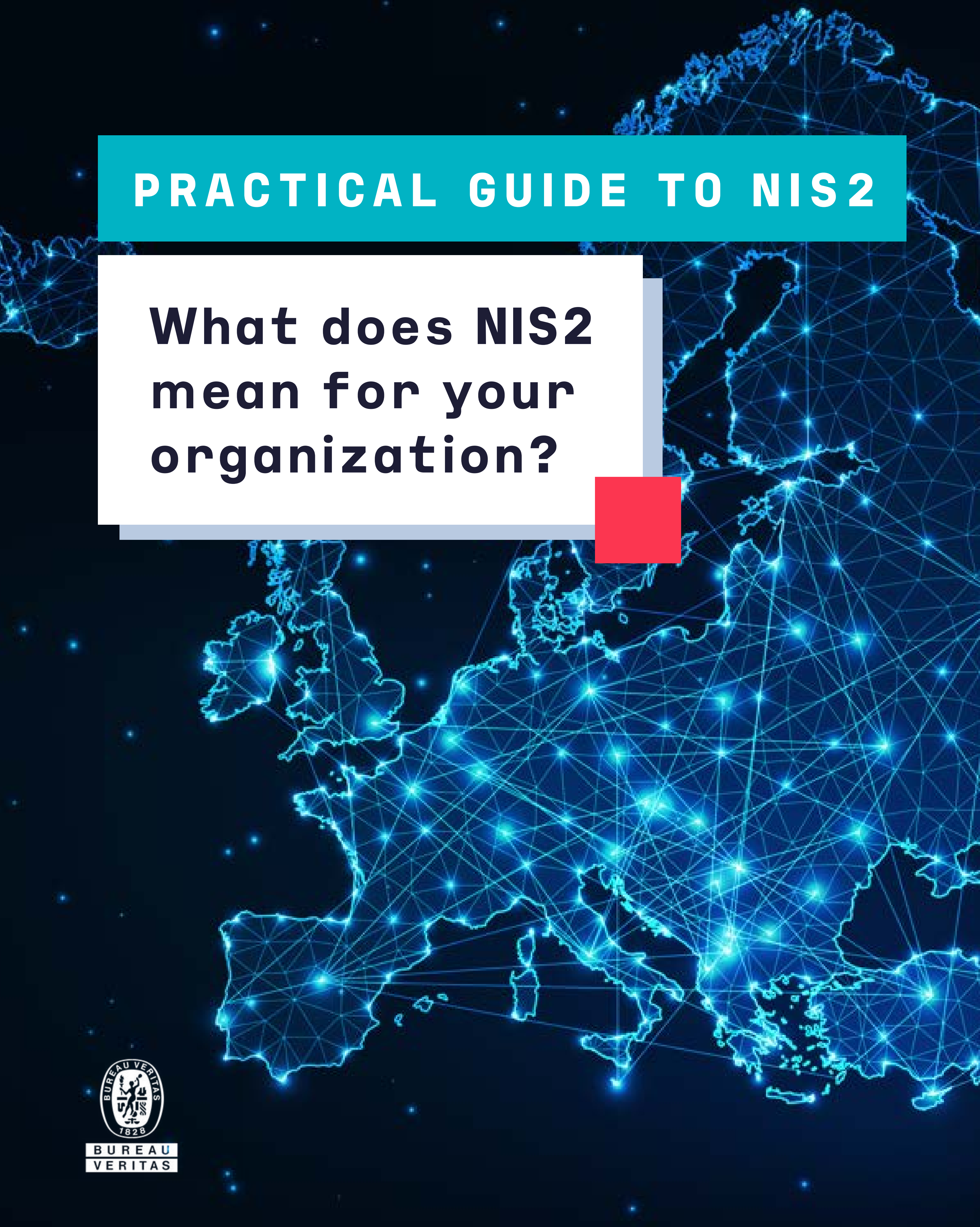
Secura
A BUREAU VERITAS COMPANY



PRACTICAL GUIDE TO NIS2

What does NIS2 mean for your organization?

BUREAU VERITAS 1828
BUREAU
VERITAS

CONTENTS

TABLE OF CONTENTS

‘European society needs to be protected against cyber threats: this is the main and valid reason for the new EU NIS2 directive. How will NIS2 impact you? This document gives you a first overview and some background information. I hope these insights will help you get underway to NIS2 compliance.’

Dirk Jan van den Heuvel, Managing Director Secura | BV

1. What is NIS2 and why do we need it?

The Network and Information Security 2 directive, or NIS2 directive, is new European legislation designed to make European organizations more resilient to cyber threats. It also aims to improve cooperation throughout the EU when it comes to cybersecurity. The directive will apply to more than **160.000 organizations** in Europe. Member States must integrate NIS2 into their national laws by the **17th of October 2024**.

The reason behind NIS2: protecting critical sectors from increased cyber threats. ‘Cybercrime has become a big business, with an entire illicit economy set up to support it with service providers, recruiters and financial services,’ according to Europols ninth organized crime assessment.

In 2023 ENISA identified the biggest cyber threats to the EU as ransomware (accounting for 34% of threats), DDoS attacks (28% of threats) and threats to data (17% of threats.) Sectors targeted most often are government, healthcare, digital infrastructure and manufacturing.

The NIS2 directive prescribes a set of minimum security requirements. Member States might be more strict when translating the directive into national laws.

NIS2 was 2 years in the making: the first NIS2 proposal was introduced on the 16th December 2020. The final version was tabled on 27th December 2022.

First NIS directive	NIS2, amendment of NIS
Applies to <4.000 organizations, mostly critical infrastructure and large businesses	Applies to >160.000 organizations, from energy to healthcare and postal services, also to medium sized businesses
Requirements are high level	Requirements are more specific
EU directive into force: 1 August 2016	EU directive into force: 16 January 2023
National laws into force: 9 May 2018	National laws into force: 17 October 2024

2. Does NIS2 apply to your organization?

Two factors determine if your organizations falls under NIS2. If both of these factors are true for your organization, you can assume NIS2 applies to you.

1. **Your organization falls into either an essential or important sector, as defined by the NIS2 directive.**
2. **Your organization has more than 50 employees or an annual 10 million euro turnover.** Smaller organizations are not subject to NIS2. There are a few exceptions. For instance: providers of domain name registration services are marked as highly critical and fall under NIS2 regardless of their size.

Sectors covered by NIS2
NIS2 has marked several sectors as vital to society. These are **essential** and **important** entities. The same rules apply to both categories. The main difference between the categories is the way an organization is audited by regulators and which penalties can be expected for non-compliance. You can find the list of sectors in ANNEX I of the NIS2 text.

ESSENTIAL ENTITIES ‘sectors of high criticality’

ENERGY

TRANSPORT

FINANCIAL INSTITUTIONS

HEALTH

WATER

DIGITAL INFRASTRUCTURE

LOCAL GOVERNMENT BODIES

SPACE

IMPORTANT ENTITIES ‘other critical sectors’

POSTAL & COURIER SERVICES

WASTE MANAGEMENT

CHEMICAL

FOOD

GENERAL MANUFACTURING

DIGITAL PROVIDERS

RESEARCH

Questions our customers ask us about NIS2

‘Where can I check whether NIS2 applies to my organization?’

In most cases you can deduce whether or not NIS2 will apply to your organization by checking the sectors marked as essential and important. Some European governments have launched **self-assessment tools** to help you. For instance in the Netherlands: https://regelhulpenvoorbedrijven.nl/NIS-2-NL/ and in Sweden: Infosäkkollen (msb.se).

‘Only part of my company can be categorized as essential or important. Does my entire organization have to comply to NIS2?’

A company might deliver different services that are not all covered by NIS2, or that fall into different categories. For instance: a postal service falls into the category ‘important.’ If the same postal company also offers transport services, this part falls into the category ‘essential.’ The European Commission (EC) will supply member states with guidelines as to which parts of complex organizations must be in scope.

‘I’m not sure whether NIS2 applies to my company; what should I do?’

If you are in doubt, the best course of action is to contact your regulator. There are valid reasons to aim for compliance anyway:

1. If you are a supplier your customers might demand compliance, even if you technically don’t fall under NIS2. They are expected to control the security of their supply chain.
2. Your organization might be required to comply in the future, for instance if you expect to grow significantly in size and turnover.
3. The ultimate goal of NIS2 is to raise the cyber resilience of companies across the EU: using the directive as a guideline will strengthen your security posture, whether the directive actually applies to you or not.

‘My company has offices and sites all over Europe. If I comply with NIS2 in France, does that compliance cover my sites in Germany?’

National laws will typically apply to any site physically present in that country. In complex situations legal expertise or EC guidelines might be required.

3. What are the main security requirements of NIS2 for companies and what do they mean in practice?

NIS2 details all kinds of requirements and the cooperation between Member States. The main requirements for companies are specified in articles 20-24. These are some of the most notable requirements.

NIS2 will apply to more than 160.000 entities in the EU.

ARTICLE 20

The management of your organization is accountable for NIS2 compliance

NIS2 introduces management liability, making upper-level management of companies accountable for non-compliance with cybersecurity obligations. The responsibility for cybersecurity measures has shifted to the highest level of organizations. This is a major change compared to the original NIS directive.

In practice this means that the members of your management need to be able to judge which cybersecurity measures are appropriate. That is why NIS2 explicitly requires members of management to follow cybersecurity training, to be able to pass these judgments.

ARTICLE 20 NIS2 DIRECTIVE

> ‘Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis.’

The NIS2 Directive has 46 articles. Articles 20-24 contain information on specific cybersecurity measures companies are required to take.

‘I have worked on NIS2 24/7 for the past years. We wanted to make cybersecurity *Chefsache*, as they say in Germany: a matter for the CEO. For too long cybersecurity has been a matter for the IT-guy, working in the background. I'm glad NIS2 has made it a boardroom issue.’

**Rapporteur Bart Groothuis, who negotiated the NIS2 on behalf of the European Parliament - **in a Secura webinar on NIS2

ARTICLE 21

Your organization is required to take adequate cybersecurity risk-management measures

NIS2 mandates you to adopt and regularly update a set of cybersecurity risk management measures. These measures should include both technical and organizational strategies, to prevent and minimize the impact of cybersecurity incidents. Ten of these measures are set out in some detail.

‘You could say that these measures are the essence of what NIS2 will mean for individual companies. These will take the most effort to implement: they mean getting your cybersecurity in order across the board, from your people to your processes and technology’, explains Bram Blaauwendraad.

ARTICLE 21 NIS2 DIRECTIVE

“Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems.”

ARTICLE 21 | 10 RISK MANAGEMENT MEASURES

1 **Policies on risk analysis**
You need to have a risk management framework in place and a policy regarding information system security. □

2 **Incident handling**
You need to be able to show that your organization can technically handle a cyber incident. For instance: do you have an incident response plan in place? □

3 **Business continuity**
If disaster strikes, how will your business cope? You have to show readiness for crisis. The text specifically mentions backup management, disaster recovery, and crisis management. □

4 **Supply chain security**
You are expected to control the security of your supply chain. This might mean: knowing how secure your suppliers are and what security measures they take. □

5 **Network and systems security**
You need to demonstrate your networks and information systems are secure, when buying, developing or maintaining them. □

6 **Policies to assess effectiveness**
Do your risk-management measures actually work in practice? You have to be able to show they do, for instance by testing and assessments. □

7 **Basic cyber hygiene practices**
Your organization is required to practice basic cyber hygiene. You are also required to offer your employees basic cybersecurity training. □

8 **Cryptography**
You are required to have policies and procedures regarding the use of cryptography and, where appropriate, encryption. □

9 **Access control**
Who can access systems? How do you handle employees onboarding and offboarding? How do you manage assets? These are questions you will expected to answer. □

10 **Use of multi-factor authentication**
You are required to use either MFA or other authentication solutions, where appropriate. The emergency communication systems within your organization are expected to be secure. □

ARTICLE 23

You are required to report cyber incidents.

Cybercriminals do not stop at a country's borders. That is why NIS2 aims to increase cooperation and information sharing around cyber incidents throughout the EU. That means you are required to report significant incidents to relevant authorities within a specified timeframe. Which authorities that will be is to be determined by Member States.

- First notification with 24 hours
- First report within 72 hours
- Full report within a month after notification

Reporting incidents sounds simple, but this requirement actually has far-reaching consequences. To do proper reporting, you first need to have adequate detection in place, including follow-up: such as incident response and forensics. You also need to know whether these measures work as they should. This means investing in business continuity management procedures, tabletop crisis exercises or crisis management simulations.

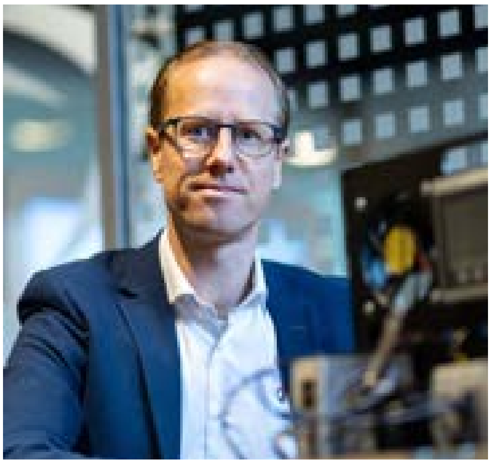
ARTICLE 23 NIS2 DIRECTIVE

"Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority of any incident that has a significant impact on the provision of their services."

The word 'crisis' is mentioned 32 times in the NIS2 text: the directive prioritizes being able to deal with incidents adequately.

'These requirements are actually things every company should be doing. Even if your company is not covered by NIS2, it's a good idea to use these requirements as a guide to becoming more cyber resilient.'

Sjoerd Peerlkamp
Manager Industrial Market Group Secura



4. How does NIS2 relate to ISO 27001?

Chances are high that your organization already uses a cybersecurity standard to manage risks, for instance ISO 27001. ‘It makes sense to use an internationally recognized standard such as ISO 27001 as a benchmark to reach NIS2 compliance’, says Bram Blaauwendraad. ‘There are many overlaps between the NIS2 directive and the ISO 27001 standard: 80 to 90% of NIS2 compliance will probably be covered if you are ISO 27001 certified.’

However, being ISO 27001 certified does not automatically mean you are NIS2 compliant – the scope of your ISO 27001 certification might be too limited to ensure NIS2 compliance. And there are a few NIS2 requirements that are not covered by ISO 27001 controls, for instance the management accountability or management oversight and the control you are required to have on your supply chain security. This means you should check for gaps between the NIS2 directive and the standard you use.

How does NIS2 relate to other cybersecurity standards?

ISO 27001 is not the only standard you can use to measure your NIS2 compliance. It does not really matter which standard you comply with, as long as you can argue that this standard is the most relevant to your organization and that the standard is of sufficient quality. There are several mapping tools available to map NIS2 requirements against different standards. ENISA has a tool mapping the different security measures of the current NIS directive to standards like ISO 27001, NIST CSF and ISA/IEC 62443. It is expected that this mapping tool will be updated to cover the NIS2 directive.

5. How seriously should your organization take NIS2 compliance?

Organizations will be expected to comply with NIS2 from the 18th of October 2024. The consequences of non-compliance are more serious for essential entities than for important entities. The EU has emphasized that it will take enforcement of NIS2 more seriously than of the current NIS directive. Articles 32 to 34 elaborate on penalties for non-compliance:

Essential entities

- Face random audits from competent authorities to make sure they are compliant.
- Potential consequences are:
  - Adhere to binding instructions
  - External supervision
  - Suspend management
  - Suspend certificates
- The maximum fine for non-compliance is 10 million euro or 2% of turnover

Important entities

- Face audits after indications of non-compliance
- Potential consequences are
  - Adhere to binding instructions
- The maximum fine for non-compliance is 7 million euro or 1.4% of turnover

> ‘The implementation of NIS2 requires not only technical and organizational know-how, but also legal expertise. The cooperation between Secura and De Clercq can help you reach compliance in time and in all areas.’
>
> **Natascha van Duuren**
> **Lawyer/partner - De Clercq Lawyers and Notary**

6. Where to start with NIS2 compliance?

If you are fairly certain your company is covered by NIS2, there are a few things you can do to start preparing for compliance. Because the requirements as a total are complex, we advise you to take enough time to implement them.

1. Get management on board

Make sure the board and management are aware of NIS2 and are aware that they will be accountable for compliance. You might suggest they follow a training as a first step.

2. Conduct a gap assessment

Are there gaps between your existing security measures and the NIS2 requirements specified for organizations in articles 21-24? A gap assessment is a good starting point. If management is on board, this is something to discuss with them.

3. Make a road map

To reach compliance, any gaps need to be addressed. The next step might be to create a concrete road map detailing how and when you will tackle these issues.

4. Find out more about your regulator and your reporting duties

Which authority oversees your organization? To which body are you obligated to report cyber incidents? It is better to conduct this research now, than when you are in the middle of a cyber incident. You can find your regulator using the NIS directive tool made by ENISA. This tool is expected to be updated to NIS2.

5. Discuss with your industry peers

What are other companies in your sector doing to reach compliance? How have they solved issues? Discussing with peers can give you valuable insight.

7. How Secura / Bureau Veritas / De Clercq can help you reach compliance

Translating the requirements of the NIS2 directive into practical and appropriate measures requires specific expertise.

Secura and Bureau Veritas can help you reach NIS2 compliance, as we are doing for a number of customers already. We offer the following NIS2 services:

NIS2 Boardroom Training

Customers usually start with a NIS2 Boardroom Training: a one-day training that will help your management when judging which measures are needed to protect your organization from cyber threats. We offer this training in collaboration with our legal partner, De Clercq Lawyers and Notary. After completing this 1-day training, your board will meet the NIS2 training requirement and receive a certificate.

NIS2 Gap Assessment

As a logical next step we can conduct a NIS2 Gap Assessment. Is your organization actually covered by NIS2? What is the security maturity level of your organization? Which gaps do we see when it comes to NIS2 compliance and which steps are needed to bridge these gaps? We can even create a concrete road map to compliance for you.

Wide range of cybersecurity services

Bridging the gaps requires different actions for each organization. We can help you with a wide range of cybersecurity services. Maybe your company needs invest in awareness: we offer a SAFE awareness program. You might need an incident response cycle: we can help you with our Incident Response PRO service. We also offer technical penetration testing and vulnerability assessment services, to make sure your networks and systems are secure.

Secura

A BUREAU VERITAS COMPANY

About Bureau Veritas / Secura

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.

Contact us

Contact us today for more information on how we can help your organization reach NIS2 compliance.

✉ **info@secura.com**

☎ **+31 (0) 88 888 3100**