Roadmap to
NIS2 compliance

The route for organisations to achieve compliance with the NIS2 Directive

devoteam
Cyber Trust

A NIS2 Directive establishes the reference framework for cybersecurity risk management measures and notification obligations in the sectors covered by its scope.

Cybersecurity risk management measures should take into account the level of dependence of essential or important entities on network and information systems. They should include measures to identify incident risks, prevent and detect incidents, respond to incidents, enable recovery after incidents, and mitigate their impact. The security of network and information systems should cover the security of stored, transmitted, and processed data.

Key requirements and obligations for organisations include:

- Information security and cybersecurity risk management process.
- Assessment of the effectiveness of information security and cybersecurity risk mitigation measures.
- Management of information security and cybersecurity incidents.
- Business continuity management.
- Supply chain security.
- Security in acquisition, development, and maintenance.
- Basic cybersecurity hygiene practices and cybersecurity training.
- Access management and use of multi-factor authentication or continuous authentication solutions.
- Cryptography and, where appropriate, encryption.
- Security of human resources.

The NIS2 Compliance Roadmap is a specialised service aimed at supporting organisations in all activities required to meet the requirements and obligations set by the NIS2 Directive.

Over a period of time, to be determined based on the context and scope of each organisation, activities such as assessing the level of compliance/maturity, creating mandatory documented information, establishing/consolidating a Risk Management process, establishing/consolidating an Incident Management process, and operationalising all ongoing operation and management processes recommended by the NIS2 Directive will be carried out.

Our focus is to provide specialised and experienced assistance tailored to the specific needs of each organisation, with the ultimate goal of achieving compliance with the NIS2 Directive.

Roadmap to NIS2 compliance

01
Define the scope of NIS2 application

02
Perform an assessment of NIS2 compliance/maturity

03
Define and operationalise policies and procedures

04
Establish/consolidate a Risk Management process

05
Establish/consolidate an Incident Management process

06
Manage compliance with NIS2

Requirements	Estimated Duration
“Designated Contact Point”: Entities must designate a contact point responsible for coordinating the interaction between our consulting team and all business units within the organisation involved in providing services deemed essential or significant under the NIS2 Directive.	**Dependent on the context and scope of each organisation** "Access to Documentation”: Our consultants need to have access to relevant documentation, including security policies, risk management procedures, and system and network configurations as needed.
"Team Availability”: It is necessary for members of all business units within the organisation involved in service provision to be available for periodic working sessions, consultations, and clarifications regarding the services and ICT infrastructure supporting them.	"Commitment to Security”: It is important that the organisation demonstrates a commitment to improving cybersecurity, being open to receiving feedback and willing to consider the recommendations provided.

Deliverables

01

Define the scope of NIS2 application

- Identify essential / important services / critical activities.
- Identify related information assets.

02

Perform an assessment of NIS2 compliance/ maturity

- Identify gaps that the organisation may have regarding NIS2 requirements and obligations.
- Identify similar gaps in the supply chain.

03

Define and operationalise policies and procedures

- Policies on risk analysis and information system security.
- Incident management procedures.
- Business continuity policies and procedures, such as backup management, disaster recovery, and crisis management.
- Policies and procedures to assess the effectiveness of cybersecurity risk management measures.
- Policies and procedures regarding the use of cryptography.
- Human resources security, access control policies, and asset management.

04

Establish/consolidate Risk Management process

- Operationalise the Risk Management methodology.
- Conduct a risk management iteration.
- Establish a risk treatment plan.

05

Establish/consolidate an Incident Management process

- Operationalise incident management procedures.
- Establish internal and external incident notification mechanisms.

06

Manage compliance with NIS2

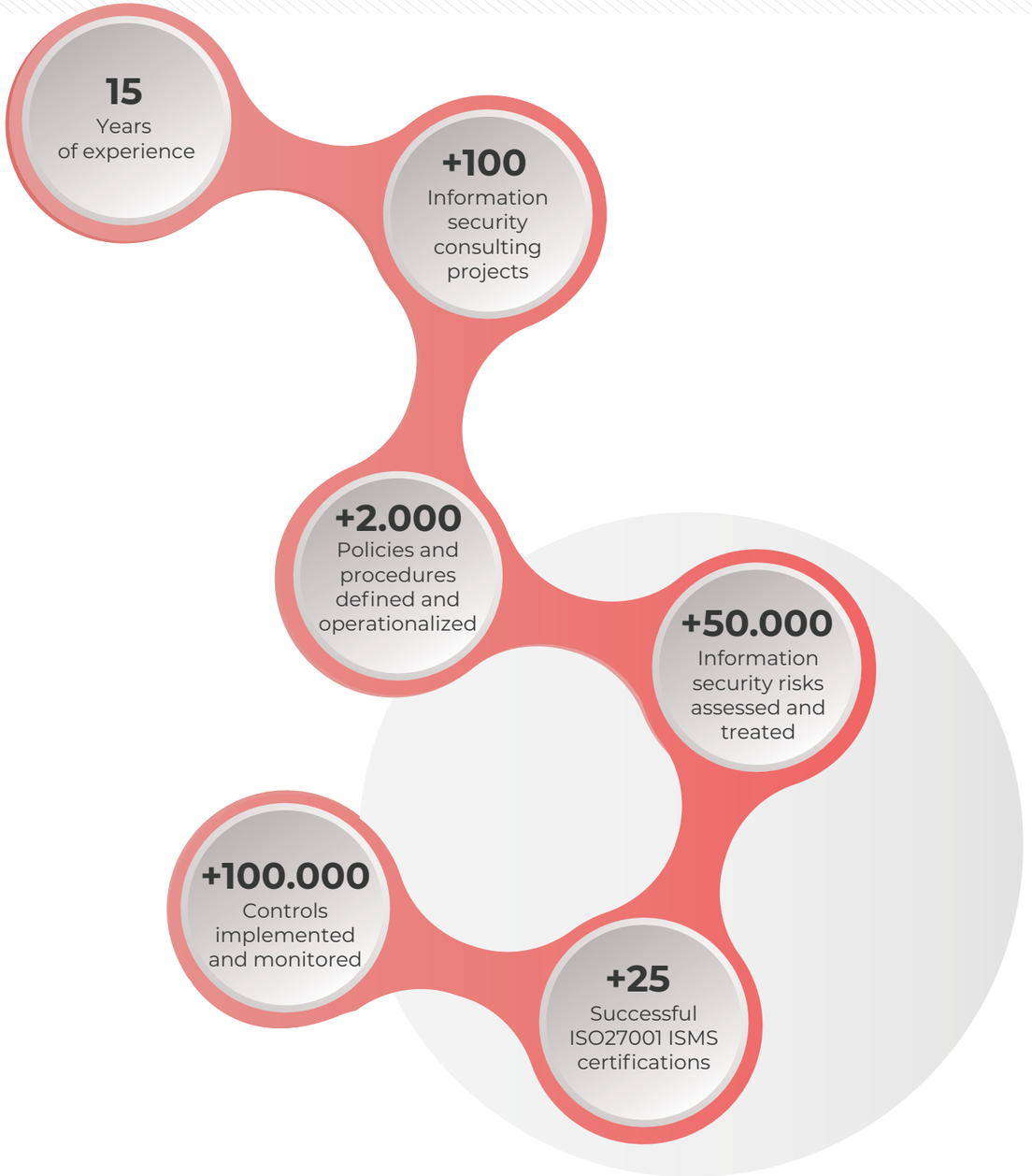
- Characterize the applicable compliance requirements set(s) of NIS2 (compliance trees).
- Map the compliance requirements set(s) (compliance trees) to related resources, activities, and evidence.
- Map the compliance requirements set(s) (compliance trees) to other standards, such as ISO27K, NIST CSF, ISA/IEC 62443, etc.

Our experience

For over 15 years, our cybersecurity consulting practice has been helping businesses across a wide range of sectors proactively manage their cybersecurity risks. We have helped dozens of companies assess and mitigate thousands of risks, and we have drafted hundreds of policies and procedures to ensure compliance with cybersecurity regulations and standards.

Our team of cybersecurity experts has extensive experience working with large and medium-sized B2B clients, and we hold relevant certifications such as ISO 27001 LA/LI, CISA, CISM, CRISC, CDPSE and others. We have a deep understanding of the evolving cybersecurity landscape and stay up-to-date with the latest threats, trends, and regulations.

We take a customised approach to cybersecurity consulting, working closely with our clients to understand their unique needs and develop tailored solutions that mitigate risks and enhance their cybersecurity posture.
Our proven track record of success speaks for itself, and we are committed to providing the highest quality cybersecurity consulting services to our clients.



Certifications & Clients

Backed by a diverse portfolio of global clients and a wide range of certifications, including CREST, ISO 27001, ISO 27701, ISO 9001 and PCI QSA, Devoteam Cyber Trust is the premier choice for organisations seeking the highest level of expertise in third party cyber risk management.

ISO 27001 (2012)

CREST (2014)

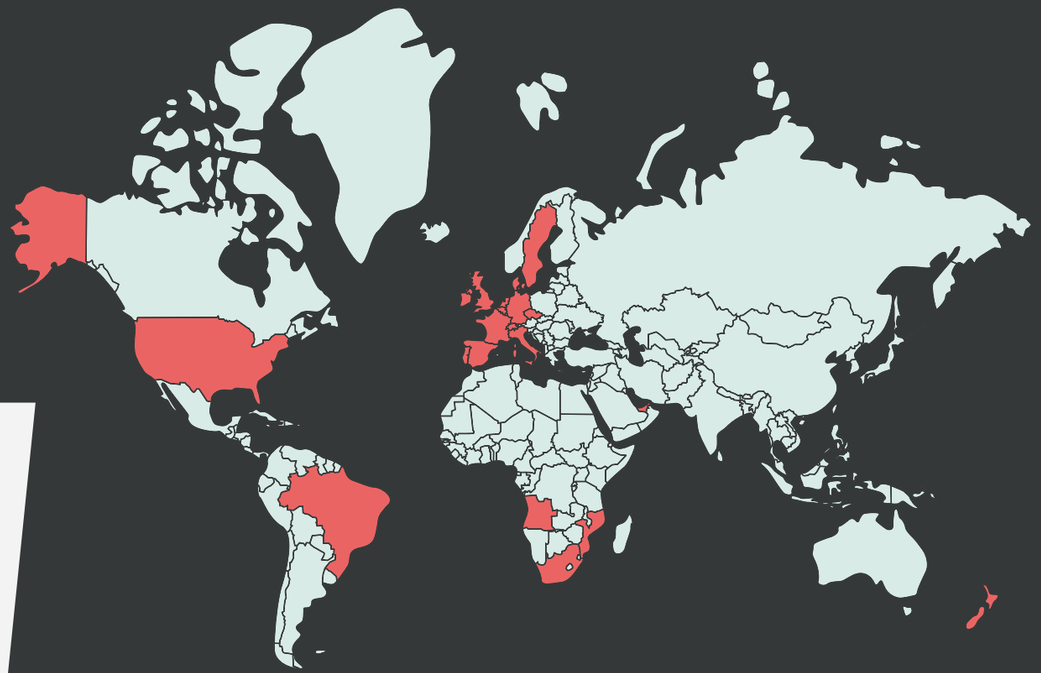
ISO 9001 (2014)

PNSC (2017)

PCI (2020)

Bancontact (2021)

ISO 27701 (2023)



More than 20 countries over the world

With HQ in Lisbon, we provide services to a wide number of large and **medium-sized companies**, both at a national and international level.

Why engage with
Devoteam Cyber Trust

- Deep expertise and experience in cybersecurity consulting with over 15 years of industry-leading experience.
- A team of highly certified and experienced security professionals, including ISO 27001, NIS2, and GDPR experts, who provide customised solutions to meet the unique needs and goals of each organisation.
- Comprehensive coverage and flexibility, with a wide range of consulting services and methodologies tailored to the specific cybersecurity risks and challenges facing your organisation.
- A commitment to quality and excellence, with a focus on delivering the highest levels of service and customer satisfaction.
- Access to advanced technology and tools, including our proprietary IntegrityGRC tool, to help clients manage their governance, risk, and compliance requirements.
- Compliance with industry standards and regulations, including ISO 27001, NIS2, GDPR, and other relevant guidelines and frameworks, to help clients mitigate cybersecurity risks and avoid penalties and legal liabilities.
- A focus on long-term partnerships and ongoing support, with continuous monitoring and reporting providing ongoing feedback and risk management capabilities.
- A global footprint and reputation, with clients in over 20 countries and a proven track record of delivering effective and high-quality cybersecurity consulting services.

Devoteam Cyber Trust is the right partner to support your organisation in this intense and evolving threat landscape, with best-in-class Offensive Security Services.

This is why dozens of medium-large clients from over 20 countries worldwide trust our services.

We are happy to share **our experience** and help you improve your **cybersecurity practice.**

Balanced risk management requires a solid strategy.

Talk to us.

devoteam
Cyber Trust

Contact us

Get in touch

Present in 18 countries in the EMEA region

www.devoteam.com

About devoteam Cyber Trust

www.devoteam.com/expertise/cyber-trust

Devoteam Cyber Trust is the Cybersecurity specialist arm of the Devoteam Group. With our 800+ experts located across EMEA, we aim to establish cybersecurity as an enabler of business success rather than a gatekeeper. We leverage an end-to-end approach to Cyber Resillience, Applied Security, and Managed Security services to secure the tech journey of large and medium-sized companies from all sectors and industries.

Since 2009, previously known as INTEGRITY, our team based in Portugal is specialised in providing cutting-edge Managed Security Services that combine its expertise and proprietary technology to consistently and effectively reduce the cyber risk of our clients. The comprehensive service range includes Persistent intrusion Testing, ISO 27001, PCI-DSS, GRC Consulting and Solutions, and Third-Party Risk Management, ISO 27001 (Information Security), ISO 27701 (Privacy Information Management) and ISO 9001 (Quality) certified, PCI-QSA, and member os CREST and CIS - Centre for Internet Security, we provide services to a considerable number of clients, operating in more than 20 countries.

About devoteam

www.devoteam.com

Devoteam is a leading consulting firm focused on digital strategy, tech platforms and cybersecurity.

By combining creativity, tech and data insights, we empower our costumers to transform their business and unlock the future.

With 25 years' experience and 10,000 employees across Europe, the Middle East and Africa, Devoteam promotes responsible tech for people and works to create better change.

Creative tech for Better Change.