Roadmap to DORA compliance

The road for organisations to achieve compliance with DORA

devoteam
Cyber Trust

The Digital Operational Resilience Act (DORA) aims to enhance the cybersecurity of financial entities, such as banks, insurance companies, and investment firms, and to ensure that the financial sector in Europe can remain resilient in the event of severe operational disruption.

DORA harmonises the rules regarding the operational resilience of the financial sector, applying to 20 different types of financial entities and third-party ICT service providers.

The key obligations under DORA are:

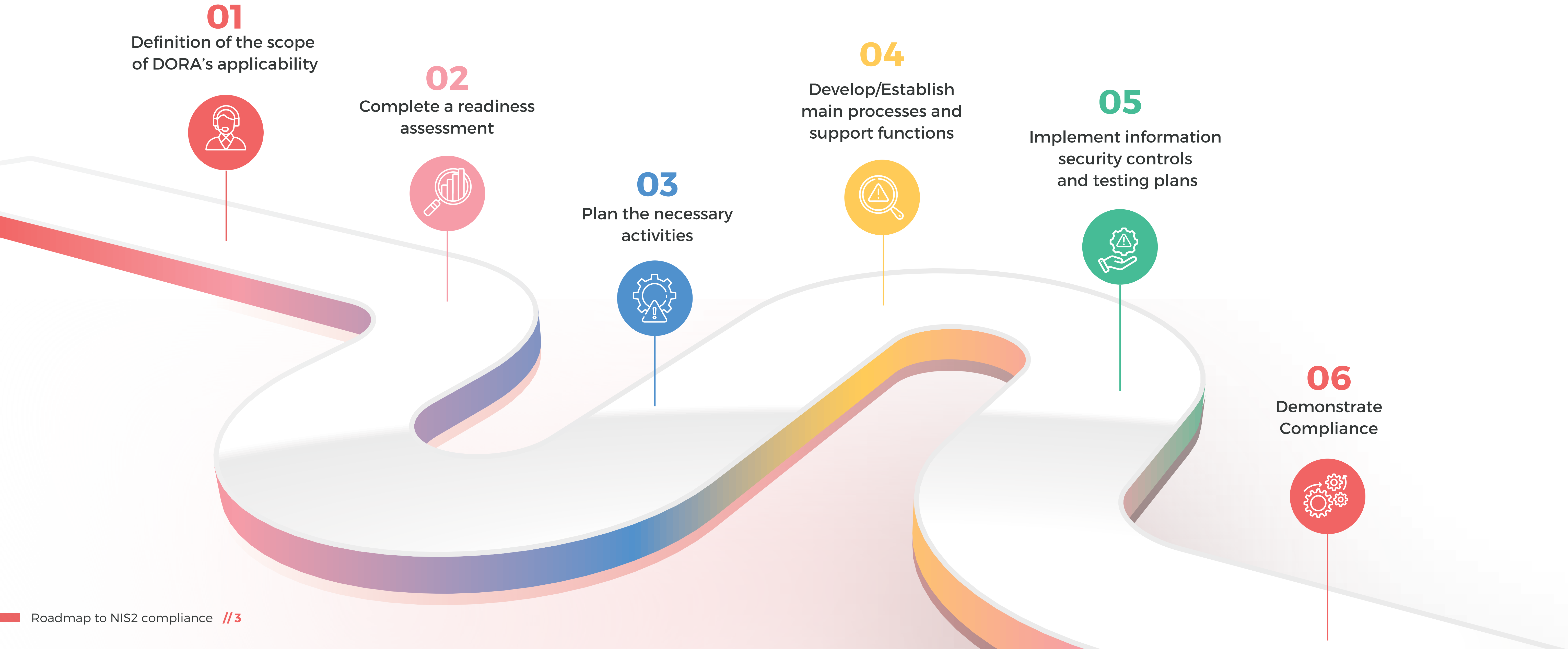
- ICT risk management
- Management, classification, and reporting of ICT-related incidents
- Digital operational resilience testing
- Management of ICT risk due to third parties
- Information sharing arrangements

Roadmap to DORA compliance is a specialised service aimed at supporting organisations in all the activities they must undertake to meet the requirements and obligations imposed by the DORA regulation.

Over a period of time, determined by the context and scope of application in each organisation, activities will be carried out to assess the stage of compliance/maturity, assist in the development of an effective framework for ICT governance and risk management, aid in the implementation of information security controls and comprehensive testing plans, and the preparation of mandatory documented information to demonstrate compliance with DORA.

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

Roadmap for compliance with DORA



01
Definition of the scope of DORA's applicability

02
Complete a readiness assessment

03
Plan the necessary activities

04
Develop/Establish main processes and support functions

05
Implement information security controls and testing plans

06
Demonstrate Compliance

Requirements

“Designated Contact Point”: Entities must designate a contact point responsible for coordinating the interaction between our team of consultants and all business units of the organisation involved in digital operational resilience processes, particularly in the security of network and information systems that support their operational processes under DORA.

“Team Availability”: Members of all business units of the organisation involved in service delivery must be available for periodic work sessions, consultations, and clarifications regarding ICT infrastructures and related operational processes.

Estimated duration

Depends 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, ICT infrastructure inventories, and a list of ICT services provided by third parties, as necessary.

“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 Scoping

- Inventory of critical or important operational functions supported by ICT
- Sources of risk associated with ICT
- Inventory of information assets and ICT assets
- Processes that depend on third-party ICT service providers
- Inventory of ICT service providers

02 Assessment

- DORA GAP analysis report for the organisation
- DORA GAPs analysis reports related to the third-party ICT service providers

03 Planning

- Detailed implementation plan
- Identification and quantification of the resources needed to implement the plan

04 Development

- Compliance Governance Structure
- Policies for ICT Risk Management
- Procedures for Incident Reporting and Management
- Mechanisms for internal and external information sharing
- Training Programs

05 Implement

- Risk Assessment matrix
- Risk Treatment Plan
- Incident Response Plan
- Test Results Reports
- Third-Party Risks Reports

06 Compliance

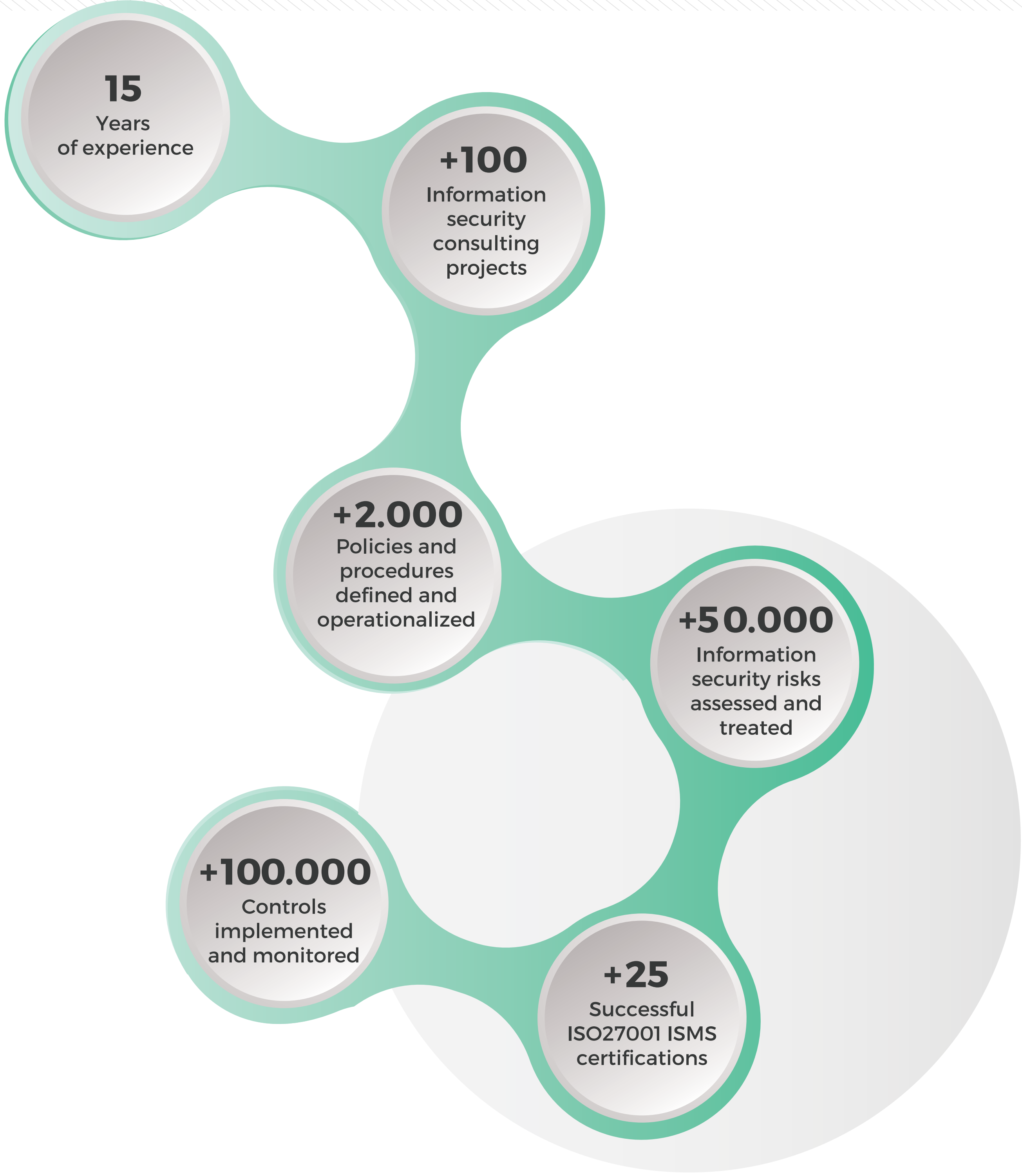
- Awareness campaigns
- Identification and characterization of monitoring tools and risk indicators
- Audit records

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.



15 Years of experience

+100 Information security consulting projects

+2.000 Policies and procedures defined and operationalized

+50.000 Information security risks assessed and treated

+100.000 Controls implemented and monitored

+25 Successful ISO27001 ISMS certifications

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)

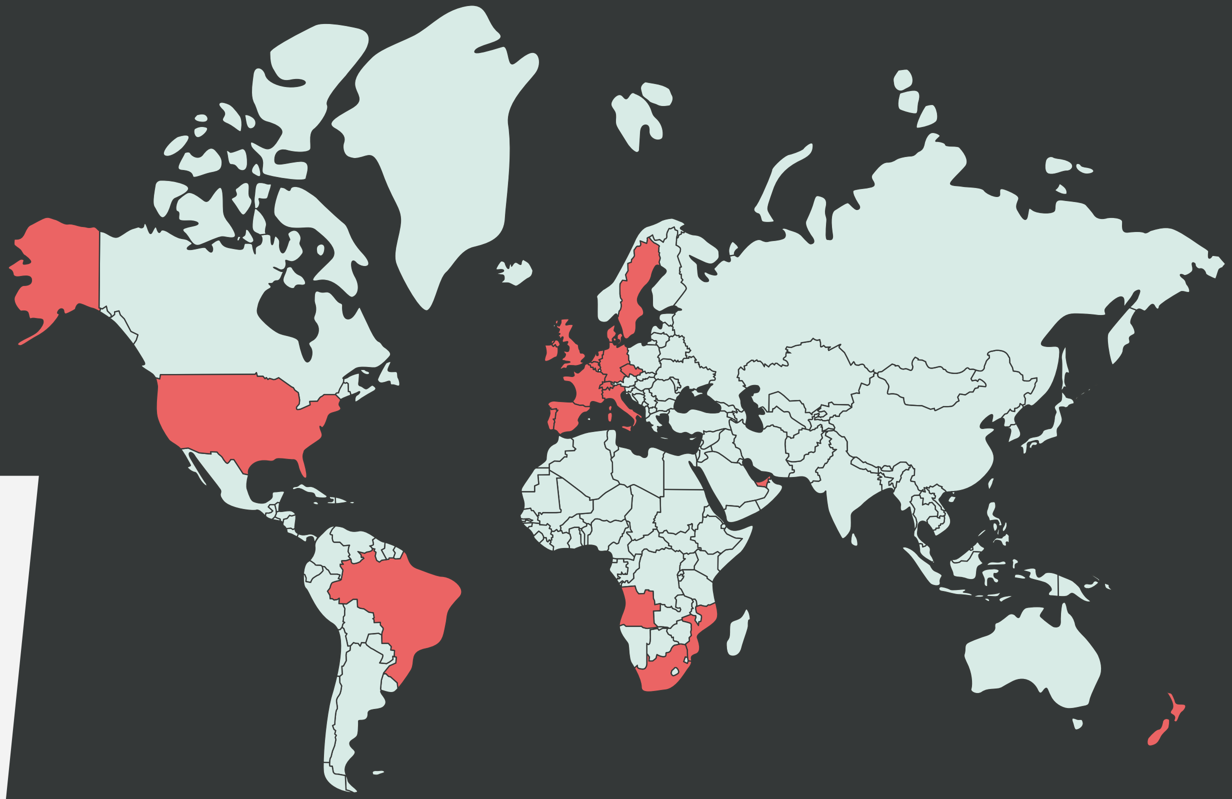
ISO 9001 (2014)

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.

Contact us

✉ info@integrity.pt

Present in 18 countries in the EMEA region

www.integrity.pt

devoteam
Cyber Trust

About devoteam Cyber Trust

www.integrity.pt

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.