DORA Services

Does DORA apply to your organization? Then you are required to comply with this EU regulation as of January 2025. This will involve effort. We can help you - from the start of your compliance process to full DORA compliance.

These DORA Services give you:

Insight into gaps

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

A clear roadmap

You know which measures you still need and receive a clear roadmap to improvement.

Help with implementation

You receive expert help in implementing the measures needed to reach full DORA compliance.

Why DORA Services?

To raise the cyber resilience of its financial sector, the EU has adopted the the **Digital Operational Resilience Act (DORA)**.
This regulation applies to all European financial institutions, from credit and payment institutions to pension funds, investment firms and insurance companies. If DORA applies to your organization, you face five basic requirements.

1. Have an risk management framework in place and improve this in an ongoing cycle.
2. Conduct regular tests and audits.
3. Monitor third-party ICT service providers.
4. Report serious incidents to authorities.
5. Share relevant information with the sector.

We can help you prepare for compliance with these basic requirements.

Which DORA Services do we offer?

DORA Boardroom Training

DORA Gap Assessment

DORA Implementation Support

Risk Management

Supply Chain Security

DORA Boardroom Training

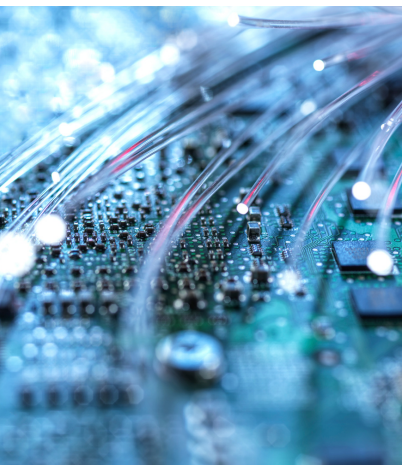
The **DORA Boardroom Training** empowers your executives to make informed decisions about DORA. This is important because DORA explicitly holds board and senior management accountable for compliance with the regulation. You will receive relevant legal insights from our partner **De Clercq Lawyers and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

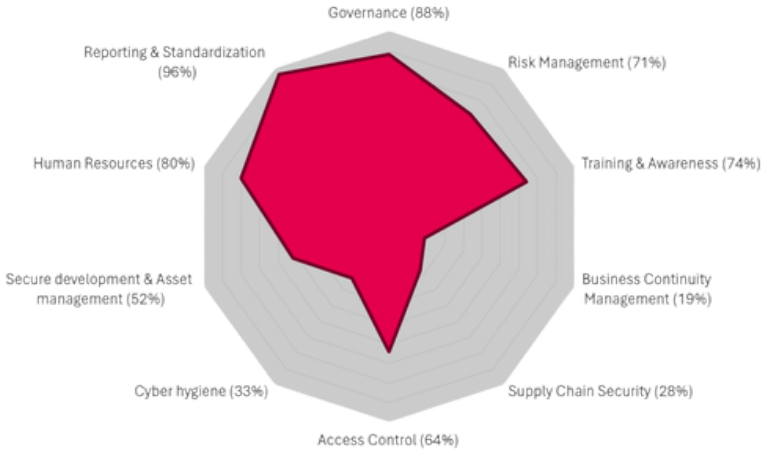
- Your board will have sufficient knowledge to judge which measures are needed to protect your organization from cyber threats.
- You will meet the boardroom training requirements of DORA.

DORA Gap Assessment

You can also conduct a **DORA Gap Assessment.** What is the security maturity level of your organization? Which gaps are there when it comes to DORA 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 DORA requirements not yet covered by default. You will see the outcome in a graphic like this:





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

DORA Implementation Support

Depending on the gaps revealed by the DORA 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

DORA 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

DORA expects 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 DORA covered, since we are ISO 27001 certified. However, Secura’s Gap Assessment showed us that some of our processes were not covered by our ISO certification, so it turned out we weren’t ready for DORA yet.”

More information on DORA

Practical Guide to DORA

What are the main requirements of DORA? What do they mean in practice? You can find more information in our Practical Guide to DORA, written by our experts: **secura.com/dora**

What is Threat-Led Penetration Testing?

TLPT is testing from a realistic perspective, using up-to-date threat intelligence. Read more about TLPT and DORA's requirements on **secura.com/tlpt**

Webinars and events

Our consultants regularly share their expertise during webinars and events on DORA. You can find upcoming webinars and events on **secura.com/events**

Secura
A BUREAU VERITAS COMPANY

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 | DORA Services

What problem did the customer have?

The board of large insurance company from the Netherlands had limited knowledge of cybersecurity. The CISO was concerned about this, because the company falls under DORA and ultimately the board is responsible for cybersecurity.

Result

The board of this insurance company followed the DORA Boardroom Training. This really opened their eyes to the fact that this was a subject they needed to consider. The training made them aware of their responsibilities and of risks.

BUREAU VERITAS 1828

Interested?

Contact us today to start raising your cyber resilience.

info@secura.com

+31 (0) 88 888 3100

secura.com