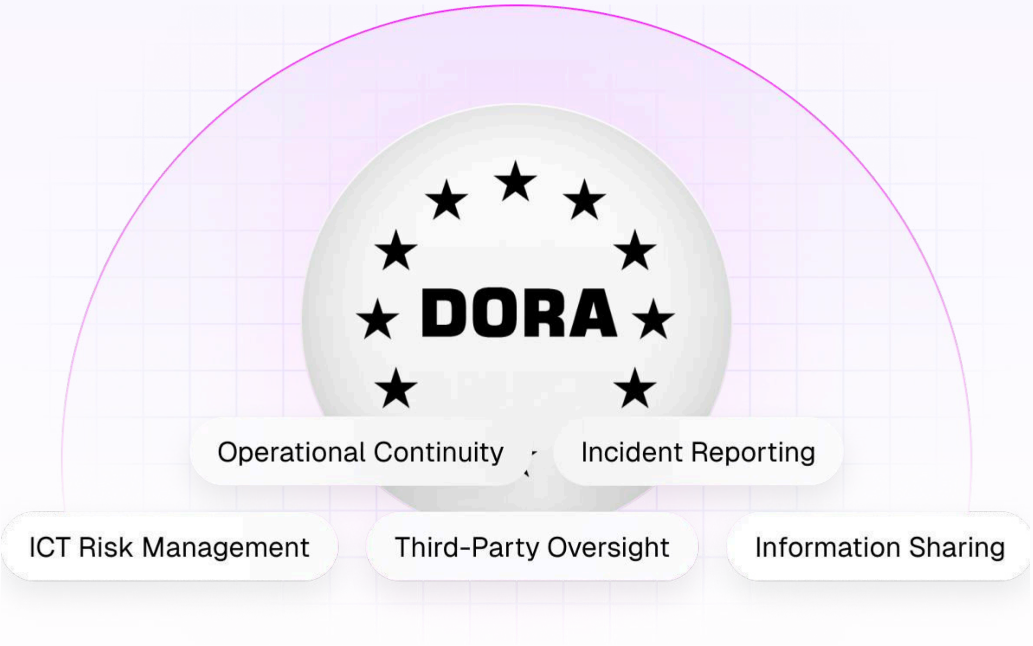
Cyber Upgrade

VendorGuard

ICT third-party risk management

The Digital Operational Resilience Act (DORA) introduces a transformative regulatory framework for financial institutions in the European Union, necessitating urgent compliance.

DORA requires a **proactive approach to managing ICT third-party** relationships, with a particular focus on the security and resilience of direct vendors and their subcontractors.



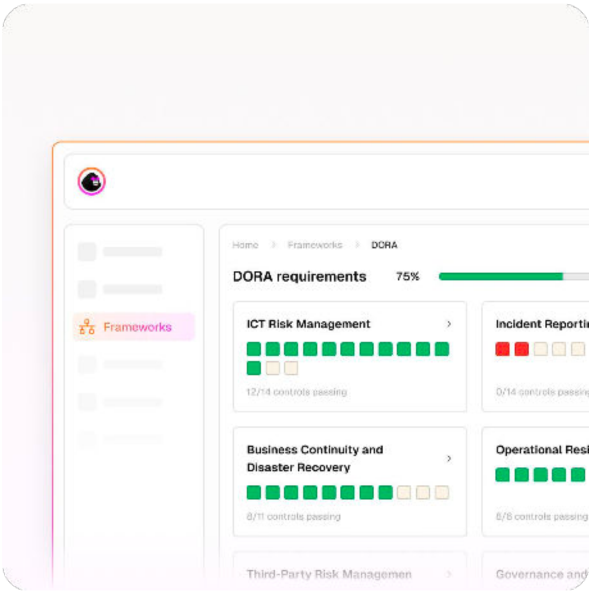
What is CyberUpgrade?

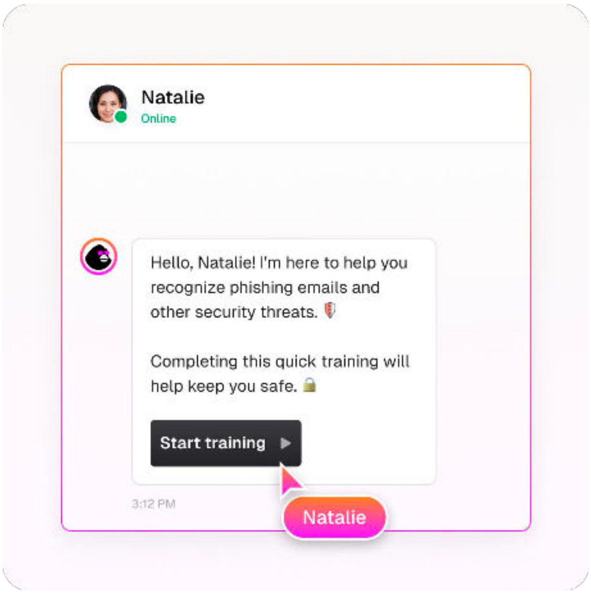
CyberUpgrade is a platform that helps offload 80% of ICT security and compliance tasks.

It’s like having a dedicated cybersecurity and compliance team running on autopilot 24/7 and at the cost of a monthly subscription.

Audit at a push of a button. Extract information, evaluate risk & present results. We have you covered.

Our platform stores, evaluates, and compares evidence against requirements, identifies vulnerabilities, groups them by severity, and generates reports.





Hello, Natalie! I'm here to help you recognize phishing emails and other security threats. 🛡️

Completing this quick training will help keep you safe. 🔒

Push security tasks and training to each individual employee. Capture compliance status and factual evidence over and over again.

CyberUpgrade ensures every team member's active involvement, crucial for accurately capturing operational compliance and evidence.

How VendorGuard helps meet key DORA ICT third-party risk management requirements

Requirement	Relevant DORA article(s)	How VendorGuard helps
ICT third-party risk strategy and assessments	Article 28(2) Financial entities must adopt and regularly review a strategy for managing ICT third-party risks as part of their ICT risk management framework.	• Coordinates with vendors to complete questionnaires • Delivers technical and legal analysis for compliance with recommendations • Provides automated quarterly updates to the vendor registry
Contractual requirements	Articles 28(4), 28(5), 28(6) Contracts with ICT third-party service providers must include: • Access rights for financial entities, auditors, and competent authorities. • Obligations for incident reporting and performance updates. • Provisions ensuring cooperation with authorities.	Provides addendum templates to ensure the inclusion of all DORA-mandated clauses.
Monitoring and oversight	Article 28(1) Financial entities must monitor the performance and risks associated with ICT third-party service providers.	• Automates vendor monitoring • Generates risk-based tasks • Provides real-time oversight
Exit strategies	Article 28(2) Policies must include termination procedures and exit strategies to ensure business continuity if a service is disrupted.	Provides exit strategies tailored to critical vendor relationships, ensuring business continuity.
Register of information	Article 28(3) Maintain a comprehensive register of all contractual arrangements with ICT third-party service providers, including: • The nature of services provided. • Associated risks and the criticality of functions. • Details on subcontractors.	• Manages your vendor register, including DORA's 15 mandatory templates • Ensures data accuracy with regular updates and annual reports
Trainings	Articles 6(1), 11 Financial entities must ensure vendors are trained on cybersecurity risks and operational resilience, with documented evidence for regulators.	• Automates cybersecurity training with 1-on-1 employee engagement • Tracks progress and provides proof of compliance • Updates content to align with evolving standards

Understanding DORA penalties:
The cost of ignoring compliance

Financial

Non-compliance with DORA can lead to fines of up to **€2 million or 2% of annual turnover** for cybersecurity failures. Late incident reporting may result in fines starting at €250,000, depending on the risk posed.

Administrative

Repeated or severe violations **can lead to license suspension or mandatory corrective actions** imposed by regulators. These costly measures ensure organizations address deficiencies to maintain market stability.

Criminal

Executives may face criminal liability for gross negligence under DORA, with potential imprisonment for wilful non-compliance that causes significant financial disruptions

Are you ready for March 31st and initial DORA audits?

Book your first consultation ▶

VendorGuard

Key features & benefits

Contract updates

Ensure that all third-party contracts include the critical provisions required by DORA.

Vendor inventory

Build and maintain a comprehensive vendor inventory.

Risk assessment & reporting

Collect vendor compliance data, assess risks, and generate detailed reports with recommendations.

Resolution plans

Develop and enforce tailored resolution plans and monitor progress.

Ongoing reporting & compliance monitoring

Provide regular security state reports and track vendor compliance to ensure continued adherence to DORA.

Exit & continuity planning

Create exit strategies for critical vendors, ensuring smooth transitions if necessary.

Why choose VendorGuard?

VendorGuard goes beyond a typical compliance tool. We provide a proactive, strategic solution to streamline vendor risk management, reduce operational risk, and enhance efficiency. Our expertise in DORA ensures that your vendor ecosystem remains resilient and compliant.

Key benefits of working with us

Efficiency

Free up internal resources to focus on strategic initiatives while we handle vendor management.

Reduced risk

A proactive, tailored approach that ensures full DORA compliance and mitigates vendor-related risks.

Cost savings

Optimize vendor performance and negotiate better terms to drive long-term savings.

Peace of mind

Trust us to manage vendor relationships professionally, ethically, and in full compliance with DORA.

> “Working with CyberUpgrade on preparation to DORA regulation has been a game-changer for our project. Their agility and speed in adapting to our needs, combined with impeccable attention to detail, have moved us a very long way in quite short time.”

fmpay

Roman Loban
Managing director at fmpay

CyberUpgrade key pillars

Advisory Team

- Consulting & Guidance
- Practical CyberSec
- Fast ICT Compliance

Copilot

- Engages every employee and initiates assessments
- Includes 1000+ pre-defined workflows for streamlined compliance

CoreGuardian

- Evidence database
- Report automation
- 24/7 monitoring

Cyber Upgrade

Solutions

Black Box Pen Tests · Data Leak Scan · Static Code Analysis

Phishing Simulator · Vulnerability Scan · Cloud Misconfiguration Scan

And more

Generate and easily access compliance documentation. Audits shouldn't be a huge project or burden for your team.

ISO 27001 · AICPA SOC 2 · NIS2 DIRECTIVE · DORA · NIST · HIPAA COMPLIANT · CYBER ESSENTIALS · COBIT 5

With VendorGuard, you get more than just third-party risk management – you will have a trusted partner dedicated to strengthening your company's operational resilience.

At CyberUpgrade, we bring deep expertise in DORA and third-party risk management, simplifying complexities with tailored guidance and real-time support. We help you maintain a resilient, compliant vendor ecosystem.

Ready for DORA compliance?

Take control of your vendor risk management today and ensure resilience for tomorrow. Contact us for a tailored quote.

More info available on www.cyberupgrade.net

Book a Demo ▶