GRC+ SERVICE SHEET · NOVEMBER 2026

DORA Compliance Audit

Article 6(6) of DORA requires your ICT risk management framework to be audited regularly by auditors with sufficient knowledge, skills and expertise in ICT risk. We carry out that audit, and on request the other pillars, against DORA and its technical standards, so your internal audit plan and your supervisor have the evidence they expect.

SERVICE
Advisory service

What It Is

An independent audit of your ICT risk management framework and the other DORA pillars, as Article 6(6) asks of internal audit, with its technical standards.

WHY IT MATTERS
Internal audit may lack ICT depth
DORA asks for auditors with sufficient expertise in ICT risk; many audit functions need that expertise for the first cycles.
- Supervisors review DORA compliance in their inspections
- Technical standards add detail beyond the regulation
- Findings need a formal follow-up process

THE OUTCOME
Evidence for the audit committee and the supervisor
Your audit plan is covered, and you can show the supervisor an independent audit with tracked follow-up.
- Report for the audit committee
- Findings tracked to closure
- Input for the next audit cycle

What We Audit

ICT risk management framework	Governance under Article 5, the framework of Articles 6 to 15 and RTS 2024/1774, or the simplified framework of Article 16 where it applies.
Incidents and testing	Classification and reporting under Articles 17 to 19 and the reporting standards, and your resilience testing programme.
ICT third-party risk	Your strategy, contracts and register of information against Articles 28 to 30 and the register standard.
Each finding with a recommendation	Every gap comes with its risk, the article or standard concerned and a practical recommendation.

What You Receive

The audit report PDF	Scope, method and a conclusion for each area, mapped to DORA and its technical standards.
Findings and recommendations Excel finding list	Each gap with its risk, the article concerned and a practical recommendation, ready for follow-up.
A DORA control mapping Excel mapping	Every test linked to its article or standard, for your next audit cycles.
A briefing for the audit committee Presentation and a closing call	The result and the decisions needed.

From Scoping to Audit Report

1	**Scoping** Entities, pillars and proportionality in scope, agreed with your head of internal audit.
2	**Documents** The framework, policies, registers, incident and test records.
3	**Interviews and testing** Sessions with the first and second line and tests of the controls on evidence.
4	**Draft findings** You see every conclusion before it is final and can add evidence.
5	**Audit report** The report for your audit committee and supervisor.

A guide, not a fixed promise: the length of each phase depends on your scope and on how quickly evidence and people are available.

Regulations That Ask for It

DORA	An independent audit of your ICT risk management framework and the other DORA pillars, as Article 6(6) asks of internal audit, with its technical standards.
PSD2	
DORA Register of Information ITS	
DORA ICT Risk Management RTS	
DORA Third-Party Policy RTS	
DORA Incident Classification RTS	
DORA Incident Reporting RTS	
DORA Subcontracting RTS	
DORA TLPT RTS	
EBA ICT Guidelines	
EBA/GL/2019/02	
GEO 14/2026 (Romania)	

Why Financial Entities Choose GRC+ for DORA

ICT risk expertise, as Article 6(6) asks	Audits are led by an auditor who holds CISA, CRISC and CISSP.
Regulation and standards together	Every test covers the article and its technical standards, so nothing is audited against the regulation alone.
Proportionate	We scope the audit to your size and risk profile, including the simplified framework where it applies.
One audit, more frameworks	Our mappings link DORA to ISO 27001, NIS2 and Swift CSP, so the evidence serves those audits too.

Questions Buyers Ask

Who may audit the ICT risk management framework?

Article 6(6) asks for auditors with sufficient knowledge, skills and expertise in ICT risk and appropriate independence. Your internal audit function can carry out the audit itself or bring in external auditors who meet that standard.

Do you audit the register of information?

Yes. We check your register against the implementing standard on the register of information and your contracts against Article 30.

Talk to Us

Tell us your entity type, the pillars in scope and your audit plan dates. We send a written proposal with scope, dates and a fixed fee.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/dora-compliance-audit

