Quantified Cyber Risk Management

Quantified cyber risk compliance matrix

Prepared by: Dephiant Consulting Inc.
Service: Quantified Cyber Risk Management
Contact: info@dephiantconsultinginc.com
Generated: 2026-11-22

Quantified cyber risk compliance matrix

Compliance matrix

Quantified cyber risk assessment

This matrix shows how the engagement maps to common control frameworks and regulatory expectations. Confirm the applicable set with your compliance lead before use.

ID | Requirement or expectation | Source reference | Engagement deliverable | Owner
R-01 | Identify and document cyber risks to the organization | NIST CSF Identify, ID.RA | Loss scenario register and quantified model | Advisory lead
R-02 | Assess and prioritize risk using a repeatable method | ISO 27001 Clause 6.1.2, 6.1.3 | Documented method, assumptions, and treatment plan | Advisory lead
R-03 | Report risk to governing bodies | NIST CSF Govern, GV.OV | Board and executive reporting pack | Accountable executive
R-04 | Maintain a risk assessment that is reviewed and updated | ISO 27001 Clause 8.2, 9.3 | Refresh schedule and re-measurement procedure | Risk owner
R-05 | Assess risk arising from third parties | NIST CSF GV.SC, ISO 27001 A.5.19 | Vendor compromise scenario and vendor assurance indicator | Third party risk owner
R-06 | Assess risk to personal data processing | GDPR Article 32 and Article 35 | Cloud data exposure scenario and data mapping input | Data protection lead
R-07 | Demonstrate operational resilience and impact tolerance | DORA Chapter II, NIS2 Article 21 | Business interruption loss forms and restore coverage indicator | Resilience owner
R-08 | Define measurable security performance indicators | NIST CSF GV.OV, SOC 2 CC3 and CC4 | Key risk and control indicator set with thresholds | Security lead
R-09 | Link investment decisions to risk reduction | ISO 27001 Clause 6.1.3 e, NIST CSF GV.RM | Prioritized treatment plan with expected exposure reduction | Finance and security leads
R-10 | Retain evidence of risk decisions and acceptance | SOC 2 CC3, ISO 27001 Clause 5.3 | Decision log and signed acceptance record | Accountable executive

Items to confirm with the client

1. The regulatory set that applies across every operating region
2. The internal risk appetite statement and thresholds already approved
3. Existing audit findings that the model must address
4. The reporting cycle the board already runs on