Quantified Cyber Risk Management

Offer pack: proposal template, budget narrative, and compliance matrix

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

Quantified cyber risk assessment proposal template

Quantified cyber risk assessment
Proposal template

Prepared by Dephiant Consulting Inc. for [CLIENT NAME]. Replace every bracketed field before use.

1. Purpose

[CLIENT NAME] requires a defensible financial view of cyber risk so that the executive team and the board can prioritize and fund security work against the exposure it removes. This engagement produces that view using a FAIR-informed method, and leaves behind the model, the indicators, and the reporting pack so the organization can maintain it.

2. Scope

The engagement covers the following in-scope estate: [BUSINESS UNITS, PLATFORMS, REGIONS]. The following are explicitly out of scope: [OUT OF SCOPE ITEMS].

3. Method

1. Frame. Confirm the decisions the model must support, the in-scope estate, the loss forms that matter, and the data sources available.
2. Model. Build the loss event scenarios, document threat and control assumptions, and agree the ranges with the accountable owners.
3. Quantify. Run the simulation, produce exposure ranges per scenario, and run sensitivity analysis on the assumptions that drive the result.
4. Report and operate. Deliver the board pack, agree the key risk indicators and thresholds, and set the refresh schedule.

4. Loss scenarios to be modeled

[LIST THE AGREED SCENARIOS. The standard starting set is ransomware on core systems, cloud data exposure, critical vendor compromise, business email compromise, insider exfiltration, and identity provider takeover.]

5. Deliverables

- Quantified risk model with documented assumptions and data sources
- Scenario report with exposure ranges and sensitivity analysis
- Board and executive reporting pack
- Key risk indicator set with definitions, owners, and thresholds
- Prioritized treatment plan showing expected exposure reduction per investment
- Refresh procedure so the organization can re-measure without external help

6. Timeline

[WEEKS]. A typical first engagement runs across a phased schedule agreed in writing before work begins.

7. Commercial terms

Fees are fixed and written before work begins. Scope for this engagement: [FEE]. Re-measurement can be carried inside an ongoing retainer or annual agreement.

8. Assumptions

- Named owners are available for the scenario workshops
- Existing asset, incident, and control data can be shared in a redacted form where required
- Findings and figures remain confidential to [CLIENT NAME]

9. Acceptance

Acceptance is confirmed when the board pack and the indicator set have been reviewed and signed off by

[ACCOUNTABLE EXECUTIVE].

Quantified cyber risk budget narrative

Budget narrative

Quantified cyber risk assessment

Prepared by Dephiant Consulting Inc. Replace every bracketed amount with the figures agreed in writing.

Category | Basis of estimate | Phase 1 | Refresh cycle | Total
Senior advisory time, framing and scoping | Fixed fee for workshops, decision framing, and data source review | [AMOUNT] | [AMOUNT] | [AMOUNT]
Risk modeling and quantification | Fixed fee for scenario construction, calibration, simulation, and sensitivity analysis | [AMOUNT] | [AMOUNT] | [AMOUNT]
Control and data analysis | Fixed fee for control effectiveness review and indicator data preparation | [AMOUNT] | [AMOUNT] | [AMOUNT]
Board and executive reporting | Fixed fee for the reporting pack and the board session | [AMOUNT] | [AMOUNT] | [AMOUNT]
Enablement and handover | Fixed fee for the refresh procedure and owner training | [AMOUNT] | [AMOUNT] | [AMOUNT]
Travel, if requested | At cost, agreed in advance and only where onsite work is requested | [AMOUNT] | [AMOUNT] | [AMOUNT]

Justification by line

Senior advisory time covers the framing work that decides what the model must answer. Without it the model measures the wrong thing. Risk modeling and quantification is the core analytical effort, and the level of effort scales with the number of loss scenarios agreed in scope. Control and data analysis is required because exposure ranges are only defensible when the control assumptions behind them are tested rather than asserted. Board and executive reporting converts the analysis into a decision pack an audit committee can act on. Enablement and handover exists so the organization owns the model afterwards and is not dependent on an external party to re-measure.

Commercial principles

All fees are fixed and written before work begins. There is no percentage of budget, percentage of award, or contingent pricing. Travel is only charged at cost where onsite work is requested. Re-measurement is priced as a defined cycle rather than an open retainer unless the client prefers a retainer.

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