Quantified Cyber Risk Management

Quantified cyber risk assessment proposal template

Prepared by: Dephiant Consulting Inc.
Service: Quantified Cyber Risk Management
Contact: info@dephiantconsultinginc.com
Generated: 2026-09-21

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].