NET-DEFENCE

Assessing Supplier Risk in the Legal Sector

Managed Service Offerings

- IT Support
- Business Resilience as a Service
- Cyber Certifications and Resilience
- Telephony and Communication

net-defence.com

Agenda

- What is supply chain risk?
- Why use an assessment model & how to tier suppliers
- Scoring model & the importance of weighting
- Final calculation & Post assessment

What is supply chain risk?

Supply chain risk refers to the potential for disruptions anywhere along the supply chain that can negatively affect the flow of goods, services, information, or finances.

It is anything that can go wrong in the process of getting a product or service from the supplier to the customer.

Why Supply Risk Matters

- Law firms hold high-value client data; high target for ransomware & supply-chain attacks.
- Attacks increasing in frequency & sophistication.

Regulatory Landscape 2025–2026

- Cyber Security & Resilience Bill brings MSPs & data centres into scope.
- Critical supplier designation & mandatory oversight.
- Use of CE/CE+, ISO27001, Lexcel expected.

Why use an assessment model?

- **Weights reflect your firm’s unique risk appetite** : you decide which factors matter most (e.g., criticality or technical controls).
- **No “one-size-fits-all” model** : weighting must match your operational realities, regulatory exposure, and tolerance for disruption.
- **Custom weighting drives meaningful risk scores** : ensuring results genuinely prioritise what *your* firm sees as high or low risk.

Tiering approach

- **Focus effort where risk is highest** - critical suppliers need deeper checks than low-impact ones.
- **Apply proportionate due diligence** - avoids over-assessing simple, low-risk vendors.
- **Create a consistent, defendable process** - aligns with NCSC guidance to classify suppliers before assessing them.

Supplier Tiering Model

- Tier 1 – Critical suppliers (MSPs, case mgmt, VOIP).
- Tier 2 – Important suppliers (CRM, HR/payroll).
- Tier 3 – Low-impact suppliers (catering, office supplies).

How to tier suppliers

- Assess operational criticality.
- Assess data sensitivity.
- Assess system integration & access.

Pre-assessment template

- List all suppliers in the Pre-Assessment Log so you have full visibility of your supply chain.
- Record three key factors for each supplier: operational criticality, data sensitivity, and system/network access. These determine how risky they could be.
- Assign a Tier (1-3) based on those factors; this ensures checks are proportionate and consistent.
- Tier 1 and 2 require assessment; Tier 3 needs only minimal checks.
- Reassess when things change e.g., service changes, new access, or new risks as recommended by NCSC/GovUK guidance.

Assessment Template Overview

- Governance checks.
- Technical controls.
- Incident response.
- Data protection.
- Subcontractor risk.

Governance & Accountability

- Named cybersecurity owner.
- Documented policies.
- Risk register maintained.

Key Technical Controls

- Cyber Essentials / ISO 27001.
- Patch & vulnerability mgmt.
- MFA & secure config.
- Encryption & access control.

Incident Response & Reporting

- Tested IR plan.
- Breach history.
- Notification time window.

Data Protection & Offshoring

- Data residency.
- UK GDPR compliance.
- Safeguards for offshore data.

Subcontractor Transparency

- Use of subcontractors.
- Equivalent controls.
- Visibility & evidence.

Scoring Model

- Scoring: 1=Good/Low Risk, 2=Adequate/Medium Risk, 3=Weak/High Risk.
- Weights reflect impact: Criticality & Technical controls are weighted higher.

The importance of weighting

- **Weights reflect your firm's unique risk appetite** - you decide which factors matter most (e.g., criticality or technical controls).
- **No "one-size-fits-all" model** - weighting must match your operational realities, regulatory exposure, and tolerance for disruption.
- **Custom weighting drives meaningful risk scores** - ensuring results genuinely prioritise what *your* firm sees as high or low risk.

The final calculation

- **Each response is converted into a numerical score** (1 = strong/low risk, 2 = adequate/medium risk, 3 = weak/high risk).
- **Scores are multiplied by predefined weights;** higher-impact areas like criticality and technical controls carry more weight.
- **Weighted scores are totalled and averaged** to produce an overall supplier risk rating.
- **The final weighted average determines the risk band** (low, medium, or high) shown in the dashboard and register.

Post Assessment

- Prioritise follow-up actions - focus first on suppliers rated High (e.g., improve controls, request evidence, update contracts).
  Risk-prioritisation logic approach
- Engage the supplier to address gaps - clarify weaknesses such as missing certifications, poor patching cadence, or unclear subcontractor use.
- Schedule re-assessment - review at renewal, onboarding, and whenever there is a material change in service, as recommended by GovUK/NCSC guidance.

Options When You Can’t Reduce Supplier Risk

- Accept the risk
  Formally document that the firm understands and accepts the residual risk because the supplier is essential or there are no suitable alternatives.
- Add it to the firm’s Risk Register
  Record the risk, assign an owner, and monitor it through your normal governance cycle (monthly, quarterly, etc.).
- Implement compensating controls internally
  Examples: extra monitoring, stricter access controls, additional logging, reduced permissions, or more frequent reviews of the supplier.

Options When You Can’t Reduce Supplier Risk

- Escalate contractually
  Add stronger clauses at renewal - e.g., breach notification requirements, minimum security standards, right to audit, or mandatory improvements.
- Seek an alternative supplier at contract renewal
  If the risk remains high and the supplier can’t or won’t improve, plan to move to a better-controlled provider.
- Limit the supplier’s scope
  Reduce the data they access, remove privileged access, or restrict the functions they perform to lower exposure.
- Increase review frequency
  High-risk suppliers may need quarterly check-ins rather than annual assessments.

Questions?

Secure your data.
Protect your business.
Defend against cyber threats.
Business resilience starts with us.

net-defence.com