NET-DEFENCE

From Assessment to Action: Strengthening Supply Chain Resilience in Law Firms

Managed Service Offerings

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

net-defence.com

For Public Use

Agenda

- Why supply chain risk needs action after assessment
- Creating focus: prioritising suppliers and dependencies
- Practical cyber and operational risk reduction
- Avoiding over-reaction: risk judgement, not checklists
- Introducing the 3-2-1 Supplier Risk Action Model
- Interactive exercise: building your 3-2-1 action plan
- Closing reflections and Q&A

Gap between assessment and action?

- Translate results into prioritised action
- Remove uncertainty, avoiding overreaction or inaction
- Apply proportionate, cyber-led risk reduction
- Embed ongoing supplier oversight

Introducing the 3-2-1 Supplier Risk Action Model

- Creating focus after assessment
- Setting priorities, with action in mind
- Balancing quick wins with internal improvements and external supplier action

Remember: Supplier Risk is not a one-off exercise

The 3-2-1 Supplier Risk Action Model

- 3 suppliers to focus on
- 2 improvements within your control
- 1 quick win

Remember: Supplier Risk is not a one-off exercise

After the Assessment: Creating Focus

Establish context

Prioritise your suppliers:

- High risk → attention and prioritisation
- Medium risk → planned improvement
- Low risk → monitor and review on change

Not all suppliers are created equally!

After the Assessment: Creating Focus

Consider Impact – material or manageable?

Key Considerations

- Would supplier disruption impact your service delivery?
- Would sensitive client or business data be exposed?
- Is this supplier a single point of failure?

Real operational impact vs theoretical worst-case scenario

After the Assessment: Creating Focus

Identify what you can control!

Key Considerations

- Can access or permissions be reduced?
- Can monitoring, logging, or alerts to enhanced?
- Can internal controls compensate the weakness

Understand dependency and breadth of real risk

After the Assessment: Creating Focus

Other key considerations in your decision making

- Distinguish risk from uncertainty
- Proportionate response
- Document your rationale

Now you are ready to apply the 3-2-1 model

The 3-2-1 Supplier Risk Action Model

- 3 suppliers to focus on
- 2 improvements within your control
- 1 quick win

Remember: Supplier Risk is not a one-off exercise

Assessment Item Categories

- Governance
- Key technical controls
- Incident response
- Data protection
- Subcontractors

3 Suppliers

- Suppliers who score the highest on your risk assessment
- Impact would be material
- Weak or lack of evidence
- Single point of failure – high dependency
- Longterm supplier where risk may have been assumed

Remember: Show me, don’t tell me

2 Internal Improvements

- Actions that do not impact the supplier
- Validate evidence
- Implement improved internal controls
- Reduce / limit access

Remember: Not all suppliers are created equally

1 Quick Win

- Smaller / quick actions
- Request evidence
- Updating supplier register
- Documenting risks to escalate
- Assess supplier dependency

Remember: Supplier Risk is not a one-off exercise

Identifying Risk Gaps to Escalate

- Risk indicators to flag (not fix)
- Breach notification uncertainty
- Sub-processor visibility gaps
- Control weaknesses (MFA, patching, encryption)

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.

Remember

- Weighting the assessment is critical
- Engage with suppliers – educate and collaborate!
- Schedule re-assessment - review at renewal or annually
- Implement this as part of supplier onboarding
- Don’t forget if there is a material change in service assess again

Questions?

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

net-defence.com

For Public Use