WEBSITE RESOURCE
PRODRIVEIT.CO.UK

Supplier cyber security due diligence checklist for law firms

A 10-step resource to assess every technology supplier that may access, process, support or influence your firm's systems and data.

Use this checklist before onboarding a new supplier, renewing a key contract or answering client and insurance questions about supplier cyber risk. For managing partners, compliance officers, operations teams and practice managers.

HIGH PERFORMING IT STARTS WITH SECURE SUPPLIERS, CLEAR EVIDENCE AND PRACTICAL GOVERNANCE

FIRM NAME	SUPPLIER BEING ASSESSED
SERVICE SUPPLIED	DATE / ASSESSOR

Important note: This resource is a practical due diligence tool. It is not legal advice or a substitute for your firm's own professional judgement.

Why supplier cyber security matters

Law firms depend on a wide range of technology suppliers, not just their main IT support provider. Software platforms, document portals, telecoms, cloud systems, artificial intelligence tools, outsourced support and specialist consultants can all create cyber and confidentiality risk.

A good supplier review should produce four outputs

1. A **risk rating** for the supplier.
2. **Evidence** that supports the supplier's answers.
3. An **action plan** for weak or unclear areas.
4. A **decision record**: approved, approved with actions, escalated or rejected.

Traffic-light scoring

SCORE	RATING	MEANING	RECOMMENDED ACTION
3	Green	Good evidence and suitable controls.	Accept and review annually.
2	Amber	Partial evidence or some improvement needed.	Accept with a dated action plan.
1	Red	Weak, missing or unclear control.	Escalate before contract signature or renewal.
0	Blocker	Unacceptable risk or no usable answer.	Do not proceed without partner approval.

Supplier risk matrix

SUPPLIER CRITICALITY	LOW AVERAGE SCORE	MEDIUM AVERAGE SCORE	HIGH AVERAGE SCORE
Critical to firm operations or client data	Block or partner escalation	High risk: action plan before approval	Medium risk: monitored acceptance
Important but not business critical	High risk: action plan needed	Medium risk: approve with actions	Low risk: review annually
Limited access or low impact	Medium risk: improve before renewal	Low risk: review at renewal	Low risk: accept

1 Governance and accountability

WHY IT MATTERS FOR A LAW FIRM

Law firms handle client money, confidential instructions and sensitive personal information. Supplier security must therefore be managed, not assumed.

RISK IF IGNORED

No clear owner, poor escalation, weak evidence for clients or insurers, and uncertainty during an incident.

WHAT GOOD LOOKS LIKE

Named owner, current security policies, supplier assurance pack and evidence of regular management review.

KEY SUPPLIER QUESTIONS

Who is accountable for cyber security? Can you provide your cyber security policy, risk assessment process and customer assurance pack?

SCORE

☐ 3 ☐ 2 ☐ 1 ☐ 0

EVIDENCE RECEIVED

ACTION NEEDED

2 Independent assurance and certifications

WHY IT MATTERS FOR A LAW FIRM
Independent assurance gives your firm more confidence than verbal claims or marketing statements.

RISK IF IGNORED
Weak baseline controls, limited evidence, and difficulty satisfying client, insurer or regulator due diligence.

WHAT GOOD LOOKS LIKE
Cyber Essentials, Cyber Essentials Plus, IASME Cyber Assurance, ISO27001, SOC2 or equivalent standards with valid certificates.

KEY SUPPLIER QUESTIONS
Which certifications do you hold and what is in scope? Are the certificates current, and what is the expiry date? Can you provide certificates or audit summaries?

SCORE	EVIDENCE RECEIVED	ACTION NEEDED
☐ 3 ☐ 2 ☐ 1 ☐ 0		

3 Identity and access control

WHY IT MATTERS FOR A LAW FIRM
Supplier accounts can be a route into law firm IT systems, email, documents and case management software.

RISK IF IGNORED
Account compromise, unauthorised access, fraudulent payment activity and wider compromise of firm systems.

WHAT GOOD LOOKS LIKE
Multifactor authentication for all users and administrators, least privilege, named accounts and regular access reviews.

KEY SUPPLIER QUESTIONS
Is multifactor authentication mandatory? How is administrator access approved, logged and reviewed?

SCORE	EVIDENCE RECEIVED	ACTION NEEDED
☐ 3 ☐ 2 ☐ 1 ☐ 0		

4 Staff training and secure working practices

WHY IT MATTERS FOR A LAW FIRM
People are often targeted first. Supplier staff need to understand legal sector confidentiality and secure handling expectations.

RISK IF IGNORED
Phishing compromise, accidental disclosure, poor handling of confidential information and slow escalation.

WHAT GOOD LOOKS LIKE
Mandatory training, role-based technical training, phishing awareness and records showing completion.

KEY SUPPLIER QUESTIONS
How often do staff complete cyber security training, and is it mandatory? Do technical teams receive additional training?

SCORE	EVIDENCE RECEIVED	ACTION NEEDED
☐ 3 ☐ 2 ☐ 1 ☐ 0		

5 Data protection and confidentiality

WHY IT MATTERS FOR A LAW FIRM

Law firms need clarity about where data is stored, who can access it and how it is protected.

RISK IF IGNORED

Data breach, confidentiality failure, regulatory exposure and loss of client trust.

WHAT GOOD LOOKS LIKE

Clear data processing terms, data location transparency, encryption, confidentiality controls and secure deletion at contract end.

KEY SUPPLIER QUESTIONS

Where is our data stored? Do you have a data processing agreement? How do you delete or return data when the contract ends?

SCORE	EVIDENCE RECEIVED	ACTION NEEDED
☐ 3 ☐ 2 ☐ 1 ☐ 0		

6 Subcontractors and supply chain risk

WHY IT MATTERS FOR A LAW FIRM

A law firm's real risk may sit with the supplier's suppliers, including hosting, support, monitoring and software platforms.

RISK IF IGNORED

Unknown data flows, unapproved access, delayed breach notification and weak onward controls.

WHAT GOOD LOOKS LIKE

Maintained subprocessor list, supplier assessment process, contractual flow-down terms and clear change notification.

KEY SUPPLIER QUESTIONS

Which subcontractors can access our data or systems? How do you assess and monitor subcontractors?

SCORE	EVIDENCE RECEIVED	ACTION NEEDED
☐ 3 ☐ 2 ☐ 1 ☐ 0		

7 Vulnerability management and testing

WHY IT MATTERS FOR A LAW FIRM

Attackers exploit unpatched systems, insecure configuration and exposed services. Suppliers should find issues before criminals do.

RISK IF IGNORED

Avoidable compromise, unsupported security claims and slow remediation of serious weaknesses.

WHAT GOOD LOOKS LIKE

Regular vulnerability management, independent penetration testing where appropriate, tracked remediation and executive summaries.

KEY SUPPLIER QUESTIONS

Do you carry out penetration testing and vulnerability management, and how are findings addressed? Can you provide a recent executive summary or remediation evidence?

SCORE	EVIDENCE RECEIVED	ACTION NEEDED
☐ 3 ☐ 2 ☐ 1 ☐ 0		

8 Incident response and breach notification

WHY IT MATTERS FOR A LAW FIRM

If a supplier incident affects the firm, partners may need to make quick decisions about clients, insurers and reporting obligations.

RISK IF IGNORED

Delayed containment, missed evidence, late notification and poorly managed stakeholder communication.

WHAT GOOD LOOKS LIKE

Documented incident response plan, tested process, named contacts, customer notification process and lessons learned reviews.

KEY SUPPLIER QUESTIONS

How quickly will you notify us of a suspected incident? What information will you provide? When was your plan last tested?

SCORE	EVIDENCE RECEIVED	ACTION NEEDED
☐ 3 ☐ 2 ☐ 1 ☐ 0		

9 Backup, recovery and business continuity

WHY IT MATTERS FOR A LAW FIRM

Law firms depend on technology to meet deadlines, serve clients and protect records. Recovery capability must be tested.

RISK IF IGNORED

Extended downtime, data loss, missed deadlines, lost billable time and client dissatisfaction.

WHAT GOOD LOOKS LIKE

Protected backups, restore testing, documented business continuity plan and clear recovery objectives.

KEY SUPPLIER QUESTIONS

Are backups protected and tested? What are your recovery time objectives? When was recovery of your backups last tested?

SCORE

☐ 3 ☐ 2 ☐ 1 ☐ 0

EVIDENCE RECEIVED

ACTION NEEDED

10 Legal sector support and evidence pack

WHY IT MATTERS FOR A LAW FIRM

Law firms increasingly need evidence for clients, insurers and regulatory expectations. A good supplier should make this easier.

RISK IF IGNORED

Slow responses to due diligence, weak client assurance, renewal friction and partner uncertainty.

WHAT GOOD LOOKS LIKE

A ready supplier assurance pack, contract support, data protection evidence, insurance evidence and annual review process.

KEY SUPPLIER QUESTIONS

Can you provide a security controls summary? How do you support client and insurer audit questionnaires?

SCORE

☐ 3 ☐ 2 ☐ 1 ☐ 0

EVIDENCE RECEIVED

ACTION NEEDED

Supplier results summary and action plan

STEP	CONTROL	RISK	SCORE 0–3	ACTION OWNER / DUE DATE
1	Governance and accountability	☐ Green ☐ Amber ☐ Red ☐ Blocker		
2	Independent assurance and certifications	☐ Green ☐ Amber ☐ Red ☐ Blocker		
3	Identity and access control	☐ Green ☐ Amber ☐ Red ☐ Blocker		
4	Staff training and secure working practices	☐ Green ☐ Amber ☐ Red ☐ Blocker		
5	Data protection and confidentiality	☐ Green ☐ Amber ☐ Red ☐ Blocker		
6	Subcontractors and supply chain risk	☐ Green ☐ Amber ☐ Red ☐ Blocker		
7	Vulnerability management and testing	☐ Green ☐ Amber ☐ Red ☐ Blocker		
8	Incident response and breach notification	☐ Green ☐ Amber ☐ Red ☐ Blocker		
9	Backup, recovery and business continuity	☐ Green ☐ Amber ☐ Red ☐ Blocker		
10	Legal sector support and evidence pack	☐ Green ☐ Amber ☐ Red ☐ Blocker		
TOTAL RISK SCORE (40 = LEAST RISK, 0 = MOST RISK)				

Decision record

SUPPLIER DECISION

☐ Approved ☐ Approved with actions ☐ Escalated ☐ Rejected

KEY RISKS ACCEPTED

CONDITIONS BEFORE GO-LIVE OR RENEWAL

NEXT REVIEW DATE

APPROVER

About Pro Drive IT

Pro Drive IT helps law firms, accountancy firms and financial services businesses improve IT performance, cyber security and technology governance. Our approach is built around practical advice, measurable standards and the belief that **High performing IT is possible**.

HOW WE CAN HELP

- Strategic IT support with cyber security standards, controls and governance for law firms built in.
- Supplier security reviews and evidence gathering.
- Cyber Essentials Plus preparation and ongoing alignment.
- Incident response planning and tabletop exercises.
- Strategic IT reviews for law firm leadership teams.

GET IN TOUCH

Book a switching consultation to find out about moving your IT support to Pro Drive, or contact us with any other questions.

☎ **0330 124 3599**
✉ **hello@prodriveit.co.uk**
🌐 **prodriveit.co.uk**