complus

Law Firms

IT & Cyber Resilience Checklist

A practical checklist for solicitors, chambers, and specialist legal practices

MANAGE. PROTECT. ASSURE.

www.complus-it.com info@complus-it.com

Purpose of This Checklist

IT and Cyber Readiness for Law Firms

Law firms rely on secure access to information, reliable systems, and strict confidentiality. Gaps in IT or cyber controls can disrupt legal work, expose client data, and create professional risk. This checklist helps law firms assess whether their IT setup supports daily operations and protects the firm during critical deadlines.

Why this checklist matters

- Remote and hybrid working is now standard
- Email and document sharing are central to legal work
- Client and matter data sits across multiple systems
- Court and client deadlines leave no room for downtime

Where Risk Commonly Appears

Most incidents result from everyday gaps, not advanced attacks.

- Phishing and email impersonation
- Lost or unsecured devices
- Access not removed when roles change
- Backups assumed to work but never tested
- Over-reliance on cloud platforms for recovery

MANAGE

IT That Supports Legal Work Without Friction

Use this checklist to review whether your IT environment is structured, consistent, and capable of supporting legal work without disruption.

IT Systems & Access

- Case and practice management systems are stable and centrally supported
- Secure access is available for office, home, and court working
- User access reflects role and responsibility

Devices & Oversight

- Firm-owned devices are centrally managed and kept up to date
- Personal device use follows a defined policy
- System changes and updates are applied consistently

Support & Accountability

- IT support response times are clearly defined
- Responsibility for IT oversight is established

Why this matters

Weak operational control increases the risk of downtime, unauthorised access, and missed deadlines, particularly during high-pressure legal work.

PROTECT

Client Data, Confidentiality, and Email Security

Use this checklist to assess whether sensitive client information and user identities are adequately protected across the firm.

Data & Information Security

- Client and matter data is securely stored and shared
- Access to sensitive information is restricted and monitored
- Data is protected across cloud and on-premise systems

Email & Identity Protection

- Multi-factor authentication is enforced on email and all cloud
- Email threats such as phishing and impersonation are actively filtered
- Domain and sender protections reduce spoofing risk

Device & Threat Protection

- All devices accessing firm data are protected against malware
- Lost or stolen devices can be remotely secured
- Security alerts are monitored and acted upon

Why this matters

Email and identity compromise remain the primary causes of data breaches in law firms, often leading to client impact and reputational damage.

ASSURE

Continuity, Recovery, and Risk Control

Use this checklist to review whether the firm can maintain operations and recover quickly during IT or cyber disruption.

Backup & Recovery

- Critical data is backed up regularly and securely
- Backup restoration is tested, not assumed
- Backups are protected from unauthorised access

Business Continuity

- Key systems have defined recovery priorities
- Downtime planning considers court and client deadlines
- Staff understand escalation steps during incidents

Governance & Preparedness

- Incident response roles and responsibilities are defined
- IT and cyber risks are reviewed periodically
- Recovery plans are documented and maintained

Why this matters

Without tested recovery and clear response processes, disruption can escalate into prolonged downtime and loss of client confidence.

Your Resilience Snapshot

What This Checklist Reveals

It helps you identify whether:

- IT systems support daily legal operations without friction
- Client and matter data is adequately protected
- Email and user access present avoidable risk
- Devices are consistently managed
- Backup and recovery can be relied upon
- Your firm can operate during IT or cyber incidents

Consider a deeper review if:

- Working patterns have changed
- Systems or suppliers have evolved
- Email is central to client communication
- Backup and recovery have not been tested recently

Next Step

If you would like a second opinion

This checklist is intended as a starting point. If you would like an independent assessment of your firm's IT and cyber readiness, Complus IT can provide structured, confidential guidance aligned to legal operations.

How to get in touch

Email
info@complus-it.com

Address
32 Threadneedle St. London, EC2R8AY