ISO 27001 • Law Firms • Professional Services • Client Trust

ISO 27001 Law Firm Readiness Checklist

A practical downloadable checklist for law firms and professional services firms preparing for ISO 27001, client security reviews, cyber insurance, or internal audit readiness.

How to score your readiness

Tick each item that is already in place and supported by evidence. Count completed items at the end. The goal is not perfection. The goal is to quickly see where your firm needs attention before a client, insurer, or auditor asks.

Score	Readiness meaning	Recommended next step
0-25%	Early-stage readiness. Core ownership, evidence, and risk work are missing.	Start with scope, data mapping, and access reviews.
26-60%	Some controls exist, but evidence is inconsistent or scattered.	Build evidence packs and close high-risk gaps.
61-85%	Good foundation. Internal audit prep and management review are likely the next focus.	Run a readiness review before certification.
86-100%	Strong readiness. Validate evidence quality and confirm audit scope.	Prepare internal audit and certification roadmap.

Firm name: _____ Completed by: _____

Date: _____ Target review date: _____

1. Scope and Governance

Start by defining what the ISMS covers and who owns the work.

Done	Readiness item	Evidence to keep	Owner
☐	Defined which legal or professional services are in ISO 27001 scope.	Approved scope statement	Leadership
☐	Listed offices, remote workers, systems, and client data processes in scope.	Scope inventory	ISMS owner
☐	Assigned an ISMS owner and executive sponsor.	Ownership matrix	Managing Partner / COO
☐	Identified control owners for access, vendors, incidents, backups, and policies.	Control owner list	ISMS owner
☐	Created a management review cadence for security and ISO decisions.	Management review schedule	Leadership

2. Client Confidential Information Map

Law firms and advisory firms must know where sensitive client information lives.

Done	Readiness item	Evidence to keep	Owner
☐	Mapped where client files are stored, shared, archived, and backed up.	Client data map	Operations / IT
☐	Included email, SharePoint, Teams, OneDrive, case systems, portals, and backups.	System inventory	IT
☐	Identified which vendors process or store confidential client information.	Vendor register	Operations
☐	Defined retention and archive rules for client matter files.	Retention schedule	Records owner
☐	Documented how client data is securely deleted or returned when required.	Deletion / return procedure	Operations

3. Microsoft 365, SharePoint, and Cloud Access

Microsoft 365 is often the highest-value audit area for law firms.

Done	Readiness item	Evidence to keep	Owner
☐	MFA is enforced for all users and especially administrators.	MFA report	IT
☐	Privileged Entra ID and Microsoft 365 roles are limited and reviewed.	Admin role review	IT / Security
☐	SharePoint client folders and matter sites have named owners.	Site owner list	Operations

Done	Readiness item	Evidence to keep	Owner
☐	External sharing and anonymous links are restricted or reviewed.	Sharing settings evidence	IT
☐	Guest users and former staff are reviewed and removed where needed.	Guest access review	IT / Site owners
☐	Offboarding includes Microsoft 365, legal tools, portals, and SaaS apps.	Offboarding checklist samples	HR / IT

4. Risk Register and Risk Treatment

ISO 27001 expects risk decisions to be documented and reviewed.

Done	Readiness item	Evidence to keep	Owner
☐	Created a risk register with specific law-firm risks.	Risk register	ISMS owner
☐	Assigned owners for each risk.	Risk owner field	Leadership
☐	Defined likelihood, impact, treatment decision, and residual risk.	Risk methodology	ISMS owner
☐	Linked risk treatments to evidence, tickets, or corrective actions.	Evidence links	Risk owners
☐	Reviewed high risks with leadership.	Management review minutes	Leadership

5. Policies and Staff Awareness

Policies must match real operations and be approved by the right people.

Done	Readiness item	Evidence to keep	Owner
☐	Approved core policies: information security, access, acceptable use, vendor, incident, backup, and remote work.	Approved policy library	ISMS owner
☐	Each policy has an owner, approval date, review date, and version history.	Policy metadata	ISMS owner
☐	Staff acknowledged policies that apply to daily work.	Acknowledgement report	HR / Operations
☐	Security awareness training is assigned to all staff and new hires.	Training completion report	HR
☐	Policy reviews are scheduled and overdue reviews are escalated.	Review workflow / tracker	ISMS owner

6. Vendor and Outsourced IT Risk

Managed IT, cloud tools, legal platforms, and client portals need formal review.

Done	Readiness item	Evidence to keep	Owner
☐	Built a vendor register with owner, data handled, criticality, and review status.	Vendor register	Operations
☐	Reviewed critical vendors before approval or renewal.	Vendor review records	Vendor owners
☐	Collected and reviewed SOC 2 reports, ISO certificates, contracts, or DPAs where relevant.	Assurance review evidence	Operations / Legal
☐	Defined MSP responsibilities versus firm cybersecurity ownership.	Responsibility matrix	Leadership / vCISO
☐	Tracked next review dates for critical vendors.	Vendor review schedule	Operations

7. Incident Response and Business Continuity

A written plan is useful. A tested plan is stronger evidence.

Done	Readiness item	Evidence to keep	Owner
☐	Approved an incident response plan with roles and escalation paths.	IR plan	Leadership / IT
☐	Ran a tabletop exercise for a realistic scenario such as partner mailbox compromise or ransomware.	Tabletop record	ISMS owner
☐	Documented client notification and legal/privacy escalation steps.	Notification procedure	Legal / Leadership
☐	Confirmed backups cover critical client data systems.	Backup configuration evidence	IT
☐	Completed at least one restore test and saved the result.	Restore test record	IT / MSP

8. Evidence, Internal Audit, and Management Review

The difference between good security and audit readiness is often evidence quality.

Done	Readiness item	Evidence to keep	Owner
☐	Created a central evidence vault, ideally in SharePoint ISMS.	Evidence vault	ISMS owner
☐	Saved evidence with clear names, dates, owners, and control areas.	Evidence naming standard	Control owners
☐	Prepared evidence packs for access, vendors, incidents, backups, risks, policies, and training.	Evidence pack index	ISMS owner
☐	Completed an internal audit or readiness review.	Internal audit report	Internal auditor / vCISO

Done	Readiness item	Evidence to keep	Owner
■	Tracked findings and corrective actions through closure evidence.	CAPA register	ISMS owner
■	Held management review and recorded decisions, risk acceptance, owners, and due dates.	Management review minutes	Leadership

Readiness Summary

Use this page after completing the checklist. It helps turn the checklist into action.

Area	Score / notes	Top next action
Scope and governance	_____	_____
Client data mapping	_____	_____
Microsoft 365 / SharePoint access	_____	_____
Risk register	_____	_____
Policies and awareness	_____	_____
Vendor risk	_____	_____
Incident response and continuity	_____	_____
Evidence and audit readiness	_____	_____

Recommended next step

If your firm has many unchecked items, start with a 30-minute ISO 27001 readiness call. Canadian Cyber can help define your scope, build your SharePoint ISMS evidence workspace, review Microsoft 365 access, and create a practical implementation roadmap.