NZ Law Firm IT Risk Self-Assessment

This self-assessment is for partners, practice managers, and operations leads at small-to-mid New Zealand law firms. It is the same control set we work through with our own legal clients before AML audits, trust account reviews, NZLS practice inspections, and cyber insurance renewals.

You will get a printable self-assessment covering twelve risk areas: AML/CFT obligations for the legal sector, Privacy Act 2020 for client data, NZLS rules of conduct as they intersect with technology, e-discovery and document management, trust account audit-readiness, secure file sharing with clients and courts, confidentiality and privilege in the cloud, encrypted email, staff onboarding and offboarding, BYOD risk, ransomware impact on litigation deadlines, and cyber insurance for legal practices.

Why this matters for NZ law firms

Law firms hold one of the densest concentrations of sensitive information in any small business in New Zealand: trust account ledgers, conveyancing files with full identity verification, litigation strategy, family law records, commercial deals under NDA, and increasingly large volumes of opposing-party data brought in during discovery. The legal sector is also a known target for two specific attack patterns: business email compromise targeting conveyancing settlements, and ransomware timed to court deadlines.

The Department of Internal Affairs supervises the legal sector under the AML/CFT regime for captured activities. The New Zealand Law Society (NZLS) administers the Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008, which include obligations around confidentiality (Rule 8) and competence (Rule 3) that have a technology component. The Office of the Privacy Commissioner has issued guidance specifically referencing the legal sector after several publicised breaches, and the NZLS itself publishes practice briefing notes on cyber risk.

Conveyancing fraud has been the most consistent loss vector. The pattern is well documented by NZ Police and by the NZLS: a compromised email account at the firm or at the client allows an attacker to insert a fake bank account at the settlement step. Funds are transferred, the attacker withdraws them within hours, and recovery is rare. The technical controls that close this gap (DMARC enforcement, MFA on partner mail, out-of-band verification of bank details) are not novel. They are simply not deployed consistently.

And then there is the litigation deadline problem. A firm hit by ransomware on a Wednesday with a Friday court filing has a real, immediate, and non-negotiable continuity problem. Cyber resilience for a law firm is not abstract. It is whether you can file on time, settle on time, and respond to discovery on time, after a bad day.

Get the self-assessment

Printable PDF covering twelve risk areas. Use it in your next partner meeting or AML audit prep session.

The Self-Assessment

What the self-assessment covers

Twelve risk areas. Each is grounded in a specific NZ obligation, a specific NZLS rule, or a specific failure mode we see in legal practices.

1. AML/CFT obligations for the legal sector

Law firms providing captured activities (managing client funds, conveyancing, trust and company formation, real-estate-adjacent work) are reporting entities supervised by the Department of Internal Affairs. DIA expects a written risk assessment, a written compliance programme, evidence of customer due diligence on every client in scope, suspicious activity reports as required, and an independent audit at least every three years.

The self-assessment covers the IT controls that produce this evidence: access control on the CDD repository, retention of identity verification documents, audit logs on the AML officer's mailbox, and the technical controls that prevent CDD data leaking into the general firm-wide file share.

2. Privacy Act 2020 for client data

The Privacy Act 2020 applies to client personal information held by the firm. The notifiable breach threshold (serious harm likely) requires notification to the Office of the Privacy Commissioner and to affected individuals as soon as practicable. Legal sector breaches that have been publicly reported tend to involve mass exposure of conveyancing or family law records and are treated by the OPC as high-severity.

The self-assessment maps the thirteen Information Privacy Principles to firm-level controls and gives you the OPC notification template ready to use during an incident.

3. NZLS rules of conduct as they intersect with technology

The Lawyers: Conduct and Client Care Rules 2008 include obligations that have a direct technology mapping. Rule 8 (confidentiality) requires lawyers to protect client information; a misconfigured file share is a Rule 8 breach. Rule 3 (competence) extends to the systems a firm uses; choosing a document management platform with weak security is, on a careful reading, a competence issue. Rule 5 (independence and conflict) intersects with how matters are walled off in your DMS.

The self-assessment translates each of these obligations into a concrete IT control and the evidence to demonstrate compliance.

4. E-discovery and document management

NetDocuments, iManage, Worldox, LEAP, Actionstep, and Smokeball are the platforms most commonly used in New Zealand. Each has a different security model, a different audit log story, and a different position on data location. For e-discovery in particular, the chain of custody on

documents has to be defensible: who created, modified, last accessed, exported, and the audit log retention has to outlast the matter.

The self-assessment gives you the vendor-question template, the typical answers, and the security configuration gaps to close on each major platform.

5. Trust account audit-readiness

The Lawyers and Conveyancers Act (Trust Account) Regulations 2008 set the rules for trust account operation, including annual reporting and external audit. The IT side of trust account audit-readiness is often what trips firms up: who has access to the trust accounting system, what is logged, how reconciliations are evidenced, and how the audit trail is preserved beyond the system's default retention.

The self-assessment covers access control on the trust system (LEAP Trust, Actionstep, MYOB AccountRight, dedicated trust platforms), the segregation of duties expected by the NZLS Inspector, and the evidence to capture for the annual trust audit.

6. Secure file sharing with clients and courts

Emailing a PDF of a sensitive document to a client is no longer the safe option, if it ever was. Secure file sharing platforms (NetDocuments ShareSpaces, iManage Share, ShareFile, OneDrive with sharing restrictions, dedicated platforms like Mimecast Sync and Share) provide controlled access with audit logs and the ability to revoke. Court filings have their own portals (the Senior Courts Civil eDuty portal, the Maori Land Court online lodgement, Companies Office Justify) with their own credential management.

The self-assessment covers when to use each, how to enforce the secure path as the default, and how to handle the credential exposure risk on the various court and tribunal portals.

7. Confidentiality and privilege in the cloud

Legal professional privilege is not lost simply because a document is stored in Microsoft 365 or Google Workspace, but the protection of that privilege depends on the controls around access. Sub-processor disclosure, data location, and the firm's ability to respond to a subpoena directed at the cloud provider all matter. A standard Microsoft 365 tenant configured well meets the privilege threshold; the same tenant with consumer-grade sharing enabled does not.

The self-assessment gives you the tenant configuration baseline (sharing policies, external collaboration controls, sensitivity labels, retention) that protects privilege in practice.

8. Encrypted email and secure messaging

Most NZ law firms use Microsoft 365 or Google Workspace, both of which support message encryption (Microsoft Purview Message Encryption, Google's Confidential Mode). Both also support inline DLP rules that can flag or block sensitive outbound messages. SPF, DKIM, and DMARC alignment is the prerequisite: without DMARC enforcement on the firm's domain, your outbound encryption story is undermined by the inbound spoofing risk.

The self-assessment covers the three email authentication records, the encryption configuration in the major platforms, and the DLP rules most often used by NZ firms.

9. Staff onboarding and offboarding controls

Lateral partner moves, paralegal departures, and contractor engagements all create access change events. The offboarding gap (a leaver retaining access to a former matter's documents) is the most common privilege breach we see during audits. The onboarding side has its own risk: a new joiner being given firm-wide access by default and then accidentally being added to a conflicting matter.

The self-assessment provides an onboarding and offboarding sequence: identity first, matter access by exception, audit log on the access grant itself, and the trigger conditions for a more thorough conflict review.

10. BYOD risk for legal staff

Lawyers routinely work from personal devices: a partner reading drafts on a personal iPad, a junior associate accessing the DMS from a home laptop, a contractor working from their own machine. Without a documented BYOD policy and a technical control set (Microsoft Intune app protection, conditional access, restricted save-to-device for privileged documents), every personal device is an uncontrolled copy of client data.

The self-assessment gives you a BYOD policy template, the Microsoft 365 or Google Workspace controls that enforce it, and the offboarding sequence when a contractor's engagement ends.

11. Ransomware impact on litigation deadlines

Ransomware on a law firm is a different problem from ransomware on most other businesses. Court filing deadlines are statutory. Settlement dates are contractual. Discovery obligations are enforced. A firm with no documented continuity plan for a ransomware event is a firm that will be making applications for extensions of time under duress, and disclosing the cause in the application.

The self-assessment covers the immutable backup configuration, the offline copy of active matter documents, the partner contact tree, and the template communications to courts and counterparties that should be ready in advance.

12. Cyber insurance for legal practices

Cyber insurance for legal practices has hardened in line with the broader market. Underwriters now ask, in writing, about MFA coverage, EDR deployment, backup immutability, email filtering, and incident response retainers. A "yes" that cannot be evidenced at claim time gives the insurer a defensible reason to decline. We have seen claims declined for exactly that reason, and we have seen partners personally exposed when professional indemnity and cyber cover did not align cleanly.

The self-assessment gives you the underwriter-question checklist most NZ brokers are using for legal practices, with notes on what evidence to keep on file so a claim is paid rather than disputed.

How Belton Helps

If you want the controls implemented, not just listed

We work with NZ law firms on the full stack: identity, DMS, trust accounting, e-discovery, and compliance evidence.

Managed IT

End-to-end IT management for law firms: identity, devices, email, DMS, trust accounting. We run the controls and produce the evidence the NZLS Inspector, your AML auditor, and your insurer want to see.

Managed IT →

Security Operations

Twenty-four-hour monitoring of your tenant, your endpoints, and your DMS access. We see the unusual mailbox rule before the conveyancing settlement goes to the wrong account.

Security Operations →

Compliance Support

Privacy Act readiness, AML/CFT IT evidence, cyber insurance application support, NZLS practice review preparation. We turn the self-assessment into auditable controls.

Compliance →

Want a one-on-one review?

Book a 30-minute Discovery and Security Session with one of our senior engineers. We will review your current setup, where the regulatory exposure sits, and what would change first.

outlook.office.com/book/BeltonDiscoveryandSecuritySession@belton.co.nz

Belton IT Nexus · Level 3, 101 Carlton Gore Road, Newmarket, Auckland 1023 · 09 974 2379 · support@belton.co.nz