NZ Accounting Firm IT & Compliance Checklist

This checklist is for partners, practice managers, and operations leads at small-to-mid New Zealand accounting firms. It is the same control set we work through with our own accounting clients before AML audits, cyber insurance renewals, and Privacy Act incident reviews.

You will get a printable checklist covering eleven control areas: Privacy Act 2020 obligations for client data, AML/CFT supervision requirements under DIA oversight, Inland Revenue data retention, multi-factor authentication on practice management tools, email authentication, backup of practice data, audit trails, third-party software review, staff offboarding, incident response, and cyber insurance readiness.

Why this matters for NZ accounting firms

The Office of the Privacy Commissioner publishes notifiable breach statistics each year. Professional services, including accounting, sit in the upper band for reported breaches involving disclosure of personal information. Most of those breaches are not novel attacks. They are misconfigured email forwarding rules, staff who left months ago still holding Xero practice access, and backups nobody had tested in a year.

Accountants also sit under AML/CFT supervision when they provide captured activities (managing client funds, forming companies, acting as a trustee, real-estate-adjacent work). The Department of Internal Affairs is the supervisor for most accounting and tax practices. DIA expects evidence of a written risk assessment, a written programme, customer due diligence records, and ongoing monitoring. The technology side of that is the audit trail: who accessed what, when, and what they did with it.

Inland Revenue requires business records to be kept for at least seven years (Tax Administration Act 1994, section 22). That obligation flows to your practice management data, your trust account ledgers, your workpapers, and to anything supporting a position taken on a client return. If your backup retention is shorter than seven years for these classes of data, or if your cloud vendor's deletion policy overrides yours, you have a compliance gap that is invisible until you are asked to produce records.

And then there is the threat side. Business email compromise targeting accountants follows a predictable pattern: phish an inbox, set a forwarding rule to an attacker-controlled mailbox, watch invoice traffic, intercept and reissue an invoice with new bank details. The remediation is well understood, but it requires controls that are configured rather than assumed.

Get the checklist

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

The Checklist

What the checklist covers

Eleven control areas. Each one is grounded in a specific NZ obligation or a specific failure mode we see in practice.

1. Privacy Act 2020 obligations for client data

The Privacy Act 2020 introduced mandatory breach notification: any privacy breach that has caused, or is likely to cause, serious harm must be notified to the Office of the Privacy Commissioner and to affected individuals as soon as practicable. For an accountant, client tax data, IRD numbers, trust deeds, and bank statements all fall inside the personal information definition.

The checklist walks through the thirteen Information Privacy Principles in the context of practice work: how IPP 5 (storage and security) maps to your Xero or MYOB tenancy permissions, how IPP 6 (access) maps to client request handling, and how IPP 10 (limits on use) intersects with marketing automation tools that ingest your client list.

2. AML/CFT supervision evidence (DIA)

If your practice provides captured activities, you are a reporting entity supervised by the Department of Internal Affairs. DIA's annual compliance levies for the accounting sector typically range from a few hundred to several thousand dollars depending on firm size, and DIA on-site reviews ask for the same artefacts every time: the written risk assessment, the AML programme, CDD records on file, suspicious activity reports, and the audit log showing who accessed those records.

The checklist covers the IT side of that evidence: how to demonstrate access control on your CDD repository, how to retain SAR drafts so they are discoverable but not exposed, and how to lock down the AML compliance officer's mailbox so that internal correspondence is not accidentally shared.

3. Inland Revenue retention (seven years)

Section 22 of the Tax Administration Act 1994 requires business records to be retained for seven years. For accounting practices that obligation extends to your client workpapers, the supporting evidence behind every position on a return, and your trust account ledgers. Your cloud practice management vendor's default retention is not your retention policy. Several major platforms purge deactivated tenant data after as little as ninety days.

The checklist gives you a concrete retention matrix: what to keep, how long, where it lives (primary, secondary, immutable), and how to prove on demand that nothing has been altered in the intervening period.

4. MFA on Xero, MYOB, FYI, SuiteFiles, and Karbon

Multi-factor authentication on every practice management tool is now the baseline, not the upgrade. Xero requires MFA for all users by default. MYOB AccountRight and Business support MFA but do not always enforce it across all roles. FYI Docs, SuiteFiles, Karbon, and APS use the underlying Microsoft 365 or Google identity, so the strength of your MFA on those tools is the strength of your tenant identity controls.

The checklist covers the gotchas: service accounts and shared logins that quietly bypass MFA, contractor accounts left without MFA after the engagement ends, and the small but real risk of SMS-based MFA on partner accounts that handle bulk client data.

5. Email authentication: SPF, DKIM, DMARC

Every accounting firm we onboard has an SPF record. Roughly half have DKIM signing on their actual sending domain. Fewer than a third have a DMARC policy stricter than p=none. The result is that any third party can spoof your domain to your clients, send a fake invoice update, and your inbound mail server will not flag it.

The checklist walks through the three records, the practical alignment requirements for marketing platforms (Mailchimp, ActiveCampaign, HubSpot), and how to move DMARC from monitoring to enforcement without breaking legitimate mail.

6. Backup of practice data (and the restore test)

Microsoft 365 and Google Workspace do not back up your data in the way most practitioners assume. Microsoft's own service description is explicit about this: their replication protects against infrastructure failure, not against deletion, ransomware, or rogue admin activity. The same logic applies to Xero practice data, FYI documents, and SuiteFiles content. A third-party backup with documented retention and a tested restore is what closes the gap.

The checklist covers what to back up, retention periods that align with the seven-year tax retention obligation, and the restore test cadence that an auditor or insurer will ask about. A backup you have never restored is a hope, not a control.

7. Audit trails on practice management and the file server

An audit trail is only useful if it is enabled, captured, and retained beyond the retention period of the underlying records. Microsoft 365 audit logs default to ninety days on lower licensing tiers and one year on E5 or with the Audit Add-on. Xero retains practice activity logs but expose them through specific reports rather than a continuous feed. Your file server, if you still run one, should be logging access at file level.

The checklist covers what to log, how long to keep it, and how to make the audit trail itself tamper-evident so that a future Privacy Commissioner investigation or AML audit has the evidence it needs.

8. Third-party tool review

Most accounting practices now use somewhere between fifteen and forty cloud tools across compliance, advisory, document management, and marketing. Each one is a separate data processor under the Privacy Act, each one has its own breach history, and each one needs its

access reviewed when you offboard a staff member. Without an inventory, that review cannot happen.

The checklist gives you a starting inventory format, the questions to ask each vendor (data location, sub-processor list, breach notification SLA, deletion on termination), and the cadence for re-reviewing the list.

9. Staff onboarding and offboarding controls

Offboarding is where most accounting firms have a measurable, recurring gap. A leaver still holds Xero practice access two weeks after departure. Their personal device still has the SuiteFiles app cached. Their forwarding rule is still active in the shared inbox. None of this is malicious by default, but all of it is a notifiable breach waiting to happen.

The checklist provides an offboarding sequence in dependency order: disable identity first, revoke session tokens, remove from practice tools, archive mailbox with legal hold, transfer file ownership, and finally retrieve the device.

10. Incident response plan for client data exposure

The Privacy Act's notifiable breach threshold ("serious harm" likely) is a judgement call, and that judgement is much easier to defend if you made it inside a documented process at the time. An incident plan does not need to be sixty pages. It needs to name the people, define when external help is engaged, give the partners a script for client communication, and capture the timeline so the OPC notification is defensible.

The checklist gives you a one-page plan template with the OPC notification form fields, the CERT NZ contact path, and the trigger conditions for each external party.

11. Cyber insurance readiness

Cyber insurance applications for professional services firms have hardened significantly since 2022. Underwriters now ask, in writing, about MFA coverage, EDR deployment, backup immutability, and email filtering. 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.

The checklist gives you the underwriter-question checklist most NZ brokers are now using, 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 accounting firms on the full stack: identity, backup, audit, and compliance evidence.

Managed IT

End-to-end IT management for accounting firms: identity, device, email, file storage. We run the controls and produce the evidence your AML supervisor and your insurer want to see.

Managed IT →

Security Operations

Twenty-four-hour monitoring of your Microsoft 365 tenant, your endpoints, and your practice management access. We see the forwarding rule before the fake invoice goes out.

Security Operations →

Compliance Support

Privacy Act readiness, AML/CFT IT evidence, cyber insurance application support. We turn the checklist into auditable controls and produce the artefacts your supervisor asks for.

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