Accessible, Sovereign, Auditable

Accessible, Sovereign, Auditable

Why Every Organisation Must Retain Local Copies of Their Accounting Data Under Global Tax Law

Executive Summary

Digital accounting systems have transformed the way organisations record, store, and interact with financial information. Yet one thing has not changed: the legal obligation to maintain complete, accessible, and auditable books and records within the jurisdiction where tax obligations arise.

Across New Zealand, Australia, the United Kingdom, the European Union, France, Canada, and the United States, tax authorities place the responsibility squarely on the taxpayer—not the software provider—to retain records for statutory periods and to produce those records promptly in accepted formats.

Cloud accounting platforms were never designed to fulfil this legal obligation. Their storage locations, export limitations, API restrictions, and service availability do not necessarily align with tax authorities' expectations for local accessibility, continuous retention, and audit-ready evidence.

This white paper explains the universal principles behind tax data obligations, outlines specific requirements across major jurisdictions, and presents a practical framework for maintaining lawful continuity of financial records in an era where operational tools and compliance expectations are increasingly misaligned.

The conclusion is consistent across borders: Every organisation must independently maintain auditable copies of its accounting data in its own jurisdiction. Cloud software does not meet this obligation on its own.

1. The Global Shift: Audits in a Digital-First World

Tax audits no longer revolve around paper binders or manual sampling. Authorities now operate in an environment where digital evidence is expected, complete transaction histories are standard, and machine-readable formats are compulsory.

To meet these expectations, auditors assume that businesses can produce:

- Complete ledgers covering the statutory retention period
- Original and amended transactions, including voids, edits, and deletions

- Source documents such as invoices, receipts, and contracts
- Machine-readable exports (CSV, XML, JSON, or country-specific formats like France's FEC)
- Prompt access, without relying on third-party availability or system uptime
- Integrity evidence, including versioning, timestamps, and verification against alteration

Most importantly, auditors do not differentiate between local software and cloud software. If a system stores data offshore, becomes unavailable, or cannot export full history, the organisation—not the vendor—is responsible for the failure.

Cloud platforms are designed for operations, not statutory retention. When an audit begins, convenience gives way to compliance, and the gap becomes painfully visible.

2. Universal Legal Principles for Financial Record Keeping

Across all major tax jurisdictions, four core principles appear again and again. They form the backbone of legal compliance regardless of country:

1. Retention

Businesses must retain books and records for statutory periods (typically 5–10 years). Retention includes every element necessary to validate a tax position.

2. Accessibility

Records must be "readily available," meaning they can be produced promptly and without dependence on third-party systems, outages, or cross-border data transfers.

3. Local Availability

Most tax authorities require that records be stored physically or logically within the jurisdiction—or be accessible in that jurisdiction without foreign legal barriers.

4. Auditability

Authorities expect businesses to produce records in structured, verifiable formats that support digital audit processes. Some formats are strictly regulated (e.g., French FEC).

These principles, though interpreted differently by each country, lead to one unavoidable conclusion: The taxpayer must control their own copy of their accounting data.

3. Jurisdiction-Specific Requirements

Below is a consolidated view of the major requirements from key jurisdictions. Despite variations in language, the underlying obligations are strikingly consistent.

New Zealand – Inland Revenue (Tax Administration Act 1994; GST Act)

- Records must be retained for seven years.
- Records stored offshore require explicit approval from Inland Revenue.
- Businesses must be able to produce full records on demand, in readable formats.

- Loss of records due to system failure is not accepted as a defence without independent backups.

Implication: A cloud platform storing data offshore does not meet NZ obligations unless the organisation maintains a local, accessible copy.

Australia – ATO (Record-Keeping Requirements, Corporations Act)

- Records must be retained for five years minimum.
- Records may be stored electronically, but they must be “accessible and convertible” for the ATO at any time.
- Storing data outside Australia is permitted only if accessibility is guaranteed.
- ATO may require records in specific formats, including exports suitable for digital analysis.

Implication: A business must maintain a fully accessible, standalone dataset, independent of SaaS uptime or API limits.

United Kingdom – HMRC (VAT Notice 700/21, MTD Regulations)

- Businesses must keep complete digital audit trails.
- Digital links between systems must be preserved.
- Records must be produced “without delay and on demand.”
- Cloud storage does not exempt the business from maintaining its own accessible records.

Implication: If a cloud system limits historic exports or has no true restore path, the business is non-compliant.

European Union – GDPR + National Tax Codes

- Retention periods vary by country (typically 5–10 years).
- Tax authorities require records to be available within the EU.
- If data is processed outside the EU, strict legal mechanisms must be in place.
- The business is accountable for maintaining audit-ready records, regardless of vendor architecture.

Implication: Relying solely on non-EU cloud providers creates sovereignty and accessibility risks.

France – L102B du Livre des Procédures Fiscales; BOI-CF-COM-10

France is one of the strictest jurisdictions in the world.

- Records must be retained for ten years.
- Businesses must be able to produce a Fichier des Écritures Comptables (FEC)—a precisely defined machine-readable export.
- Failure to produce a compliant FEC automatically triggers financial penalties, regardless of intent.
- Relying solely on a cloud platform that cannot generate a valid FEC is non-compliant.

Implication: All French entities must maintain their own FEC-compatible dataset.

Canada – CRA Record-Keeping Requirements

- Records must be retained for six years.
- Offshore electronic records require permissions and safeguards.
- Loss of electronic records (corruption, outage, vendor failure) is treated as failure to keep records.

Implication: A business must control its own data, not merely access it via vendor-controlled systems.

United States – IRS Publications 583 & 552

- Records must be retained for 3–7 years, depending on the return.
- The IRS requires complete books, including digital originals and amendments.
- The method of storing records is flexible, but the taxpayer bears full responsibility for producing them.

Implication: Using a SaaS platform does not shift the obligation; taxpayers must maintain independent access.

4. The Silent Vulnerability of Cloud Accounting Platforms

Cloud accounting tools accelerate workflows, reduce operational friction, and improve accessibility—but their design rarely aligns with statutory interpretation of “books and records.”

Several structural challenges appear across major SaaS systems:

Vendor-Controlled Storage Locations

Data may reside offshore or migrate between regions without explicit customer control.

Limited or Partial Exports

Full-history exports often lack:

- deleted transactions
- versioning
- audit trails
- attachments
- metadata and relationships

No Guaranteed Restore Path

Many platforms cannot restore prior states in full fidelity.

Availability and Downtime Risks

During an audit, an outage—even a planned maintenance window—can constitute failure to produce records.

API Throttling or Deprecation

APIs are not statutory mechanisms; they are operational conveniences that may change without notice.

Vendor Business Continuity Risks

Acquisitions, pricing changes, data migrations, or feature retirements can compromise access.

The legal through-line is simple: SaaS convenience does not satisfy statutory requirements unless the organisation retains full, sovereign, auditable copies of all records.

5. What “Local, Accessible, Auditable” Really Means

A compliant data retention strategy must satisfy three fundamental criteria:

1. Locality

Records must exist within the taxpayer’s jurisdiction or in a legally compliant sovereign area. “Accessible via the internet” is not the same as “located in-country.”

2. Accessibility

The organisation must be able to produce its data:

- Immediately
- Without vendor assistance
- Without needing live SaaS systems
- In response to a compulsory notice
- In perpetuity for the retention period

3. Auditability

Auditors expect:

- structured, machine-readable exports
- chronological completeness
- unmodified historical accuracy
- version control
- links to source documents
- replication of the system’s internal logic

These expectations exceed what operational cloud systems typically provide.

6. Real-World Scenarios (Composite Case Studies)

Case 1: Xero API throttling during an audit (NZ)

An SME attempted to export four years of invoices during an audit. API rate limits prevented extraction. Inland Revenue required immediate production of records. The business faced penalties despite the vendor's limitations.

Case 2: Failure to produce a compliant FEC (France)

A French retailer using a global SaaS platform could not generate the mandated FEC. Under French law, this alone constituted a procedural offence, resulting in automatic fines.

Case 3: Migration to a new system erased audit trail (UK)

A UK practice migrated clients from one cloud platform to another. Historic VAT trails were lost. HMRC deemed the records incomplete, triggering a detailed audit and adjustments.

Case 4: Offshore SaaS without retention controls (Australia)

A business used a US-hosted accounting system that changed its export policy. When the ATO requested ledger-level data, only partial exports were available. The entity failed its record-keeping obligations.

Each scenario reinforces the same principle: relying solely on operational SaaS is not a compliance strategy.

7. Towards Legal Continuity: A Modern Record-Retention Framework

A compliant organisation must implement a structured approach to retaining financial data, independent of its cloud providers.

A robust framework includes:

- Independent, automatic data extraction from operational systems
- Full-history versioning, capturing all changes
- Storage in a sovereign environment under the organisation's legal jurisdiction
- Machine-readable, standards-compliant formats (CSV, JSON, XML, FEC)
- Immutability or tamper-evidence, ensuring the integrity of historical data
- Automated retention schedules aligned with jurisdictional rules
- Periodic restore testing to verify usability
- Documented policies that evidence compliance during audits

This framework shifts the organisation from reactive dependency to proactive control.

8. The Strategic Opportunity Behind Compliance

Although the legal obligation is the catalyst, the benefits extend far beyond audit protection:

- Evidence-based governance
- Cleaner, higher-quality datasets

- Resilience against vendor outages or lock-in
- Simplified system migrations
- Richer analytics and forecasting
- Improved fraud detection and internal controls
- Greater confidence for investors and acquirers

Compliance is the foundation. Continuity and intelligence are the strategic dividends.

9. How Control-C Supports Legal Data Continuity (Optional Section)

While this white paper avoids product-centric narrative, it is relevant to acknowledge what a compliant solution typically includes.

A continuity platform such as Control-C provides:

- Sovereign, in-country storage options
- Daily (or continuous) automated extraction of full ledger data
- Complete versioning and immutable backups
- Machine-readable exports, including FEC (France)
- Independent access outside the SaaS provider
- Unlimited retention aligned with tax law
- Operational analytics and anomaly detection

This aligns directly with statutory requirements across jurisdictions, while also strengthening operational resilience.

Conclusion

Tax authorities worldwide expect organisations to maintain complete, auditable, accessible financial records within their jurisdiction for the entirety of the statutory retention period.

Cloud accounting platforms, while powerful for daily operations, do not replace this obligation. They may store data offshore, limit exports, restrict version histories, or become unavailable at critical moments. None of these risks excuse a business from compliance.

To meet modern tax expectations, every organisation—regardless of size, sector, or geography—must retain independent, sovereign, audit-ready copies of its accounting data.

This is the new baseline of financial governance: Accessible. Sovereign. Auditable.

Everything else is operational convenience layered on top.