Information Leadership™
CONFIDENCE, BY DESIGN

March 2026

# Controlled Documents: A Practical Guide

## A Whitepaper for New Zealand & Australian Organisations

Microsoft Solutions Partner
AI Cloud
Modern Work
Change & Adoption

# Contents


Introduction 2

Why this matters now 2

What is a Controlled Document? 3

Key Characteristics 3

Which Documents Should You Control? 4

Action: Create a Document Classification Matrix 4

What Good Looks Like 5

A Single Source of Truth 5

Clear Ownership and Accountability 5

Appropriate Review Cadences 5

A Controlled Change Process 5

Managed Version History 5

What Happens When Documents Are Not Controlled 6

Getting Started: A Practical Roadmap 7

① Identify High-Need Areas 7

② Curate and Assess Existing Documents 7

③ Assign Governance and Migrate in Batches 7

④ Define Your Process 7

⑤ Communicate and Train 7

⑥ Monitor and Expand 7

Proving Your Document Control Works 8

How Information Leadership Can Help 9

Appendix A:
Implementation Checklist 10

Appendix B:
Quick Reference – Controlled Documents Essentials 11

Appendix C:
Frequently Asked Questions 12

About Information Leadership 13

# Introduction

**Picture this**

A staff member responds to a privacy complaint using a procedure last updated

A health and safety inspector requests your confined space entry procedure and finds three different versions

An auditor asks who approved the current procurement policy, and nobody can say for certain

These are not outliers. They happen routinely in organisations that store documents without truly controlling them. And the consequences – compliance failures, legal exposure, wasted time, and eroded trust – are entirely preventable.

This guide is written for senior leaders: Corporate Services Managers, Risk and Compliance Managers, Legal Counsel, and CIOs who need to ensure their organisation's critical documents are always current, properly governed, and defensible under scrutiny. It is not a technical manual. It is a practical overview of what controlled documents are, why they matter, what good looks like, and how to get started.

## Why this matters now

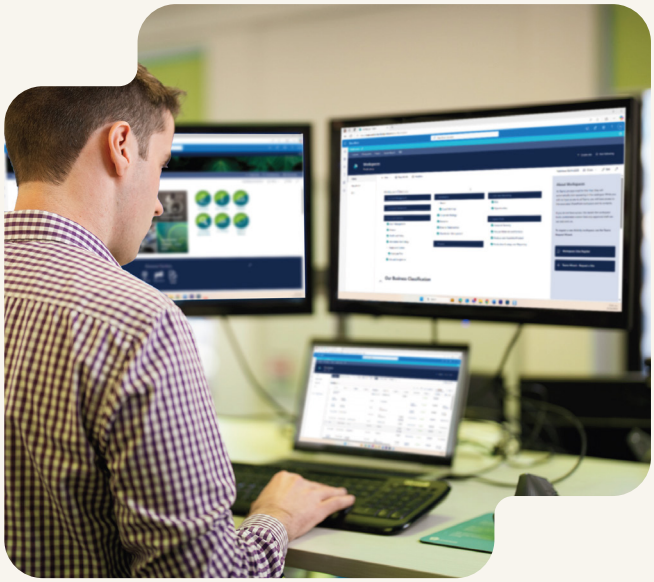
Privacy legislation, AI usage, rising audit expectations, and increasing public scrutiny mean organisations can no longer afford to treat document control as a back-office afterthought.

If your information is hard to trust, your decisions are too.

# What is a Controlled Document?

A controlled document is an official organisational document managed through a defined process of creation, review, approval, distribution, and periodic review. In plain terms, it is a document your organisation treats with a high level of oversight to ensure it is always accurate, up to date, and used correctly.

The primary purpose is to prevent people from accidentally relying on an old or unapproved version. With proper control, everyone accesses a single source of truth – the latest approved version – and old versions are clearly archived or removed from everyday use.



## Key Characteristics

**A controlled document typically has:**

- Unique identification including version numbers and effective dates
- Formal approvals before publication
- Defined review dates
- Access controls that restrict who can edit versus read
- A clear status (draft, approved, archived)
- An assigned owner and approver.

# Which Documents Should You Control?

Not every document needs formal control. The test is straightforward: if using the wrong or an outdated version could lead to compliance issues, safety risks, legal exposure, or significant operational failures, that document should be controlled.

**Documents that typically warrant control include:**

| | |
|---|---|
| Policies, standard operating procedures, and manuals | The documents that define how your organisation operates and must remain consistent for compliance and quality. |
| Process documents and work instructions | Guides for how work is performed, where outdated instructions could lead to errors, safety incidents, or quality failures. |
| Legal, regulatory, and compliance documents | Contracts, compliance manuals, privacy policies, codes of conduct, and anything referenced in audits or regulations. |
| Official forms and templates | Blank forms used to capture important data (incident reports, inspection checklists, evaluation forms). The template should be controlled; each completed form becomes a record managed through recordkeeping practices. |
| Critical plans | Emergency response plans, business continuity plans, and key records with ongoing legal or operational relevance. |

Conversely, if the consequences of an error are minor – a team's internal process for organising a social event, for instance – standard document or template management practices will suffice.

The goal is to avoid wasting effort over-controlling trivial documents while ensuring nothing critical slips through.

## Action: Create a Document Classification Matrix

- Categorise documents by importance and risk.
- High-criticality documents go into the controlled documents system.
- Less critical documentation can remain in general libraries with simpler versioning.
- This prevents wasted effort while ensuring truly critical documents are governed.

# What Good Looks Like

A well-functioning document control system is not about bureaucracy. It is about making the right thing easier than the wrong thing. Here are the hallmarks of an effective system.

## A Single Source of Truth

Staff know exactly where to find current controlled documents – typically a well-organised online library or intranet portal. Old versions are either hidden from general search or clearly marked as superseded. If people are always pulling documents from the central repository, they are inherently getting the latest version.

## Clear Ownership and Accountability

Every controlled document has a designated owner who is responsible for its content, an approver who gives final sign-off, and a defined review schedule. These details are visible in the document's metadata, so there is never confusion about who is accountable.

**Document Owner:** Responsible for content accuracy. Triggers reviews and updates. Usually a subject matter expert or department manager.

**Approver:** Gives final sign-off before publication. Sufficiently senior to take accountability for the document's content and authority.

**Reviewers / SMEs:** Provide expert feedback before approval. Advise on accuracy and workability but do not formally approve.

**Document Controller:** Ensures the process runs smoothly: manages the register, sends review reminders, checks metadata. Often part of Compliance or Information Management.

**End Users:** Know where to find current documents, use only official versions, and flag errors or needed updates through proper channels.

## Appropriate Review Cadences

All controlled documents are reviewed on a defined schedule, with the frequency matched to risk:

| | | |
|---|---|---|
| **High-risk documents** | Safety manuals, compliance policies, business continuity plans | Every 6–12 months |
| **Moderate-risk documents** | Standard operating procedures, financial guidelines | Every 12–24 months |
| **Lower-risk documents** | internal team procedures, general guidelines | Every 24 months or as needed |

In addition to scheduled reviews, trigger-based reviews should occur whenever regulations change, audits identify issues, incidents occur, or processes are significantly updated. Every document should have a "next review date" from day one.

## A Controlled Change Process

No one should simply open a controlled document and change it on the fly. Changes follow a defined workflow: a new draft is created, reviewed, approved, and then published as the current version. The previous version is automatically archived. Users are notified of significant changes.

The process can and should be proportionate. Minor corrections (typos, formatting) can be fast-tracked with a single approver. Major changes (policy shifts, procedural overhauls) go through full review. Emergency changes follow an expedited path with retrospective documentation. The mantra: as simple as possible, but as rigorous as necessary.

## Managed Version History

Superseded versions are archived – accessible to auditors and investigators, but removed from everyday circulation so staff cannot accidentally use them.

You'll find our practical Checklist and Quick Reference Guide in the Appendix

# What Happens When Documents Are Not Controlled

**The risks of uncontrolled documents compound over time:**

| | |
|---|---|
| Outdated information in use | Staff follow obsolete procedures, leading to errors, safety incidents, or non-compliance with current regulations. |
| Compliance failures | Auditors find non-conformities when you cannot demonstrate current, approved documents. This can lead to audit findings, lost certifications, or penalties. |
| Legal and financial exposure | An outdated contract template or privacy policy used by mistake can create liability. Using an old privacy policy could violate new data protection laws. |
| Wasted time and rework | Staff spend hours searching for the "right" version or recreating documents they cannot find. This erodes confidence and slows decision-making. |
| Reputational damage | Multiple versions circulating sends mixed messages to customers, regulators, and employees, undermining trust in your organisation's governance. |

The cumulative effect is what we call document chaos – mounting risk, cost, and frustration that becomes harder to address the longer it is left.

Check out our FAQs in the Appendix

# Getting Started: A Practical Roadmap

Implementing document control can feel daunting, but the most effective approach is targeted and incremental. Rather than trying to bring everything under control at once, focus on where controlled documents will have the most impact first.

## ① Identify High-Need Areas

Start with functions or processes that carry the highest compliance or risk exposure: health and safety, privacy and data protection, HR, financial controls, and key operational procedures. Engage leaders and risk managers in these areas to confirm which documents are considered essential.

## ② Curate and Assess Existing Documents

Gather the documents that already exist for your priority areas – even if they are scattered across network drives, email attachments, OneDrives, or personal folders. Identify gaps (important topics with no formal documentation) and redundancies (multiple versions of the same policy). Choose the best or most current version as the basis for the controlled document.

## ③ Assign Governance and Migrate in Batches

For each priority document, assign an owner, an approver, and a review schedule. Move documents into the controlled system in manageable batches, updating content and applying standard metadata as you go. Route each through formal review and approval before publishing.

## ④ Define Your Process

Document the lifecycle: how documents move from draft to approved to published to archived. Include how new documents enter the system, how changes are managed, and what triggers a review. This documented procedure is itself a controlled document – and the first thing an auditor will ask to see.

## ⑤ Communicate and Train

Launch the repository with clear communication about where to find controlled documents and why it matters. Train document owners and approvers on the workflow. For general staff, a brief orientation showing them how to find and recognise current documents is usually sufficient.

## ⑥ Monitor and Expand

With the highest-impact documents under control, gradually extend to other areas as business needs dictate. Use a risk-based lens to periodically reassess whether new regulations or changes introduce new categories of documents that should be controlled.

### The Adoption Challenge

The hardest part of document control is not the system – it's the behaviour change.

Make the controlled repository easier to use than the workarounds.

Explain the "why" with real examples.

Ensure leaders visibly use the system themselves.

And treat the process as something that can be improved – gather feedback and adjust.

When people experience fewer headaches finding information and passing audits, commitment follows.

# Proving Your Document Control Works

A well-designed system pays for itself at audit time. To satisfy an auditor or regulator, you need to demonstrate both a defined process and evidence of following it.

**Key elements include:**

| | |
|---|---|
| A written Document Control Procedure | Describing your process for approvals, versioning, distribution, review, and archiving. |
| A Controlled Document Register | Listing each document with its title, version, approval date, owner, and next review date. |
| Approval records | Showing who approved each version and when – whether via electronic workflow logs, signed cover sheets, or email records. |
| Version history | Demonstrating a traceable chain of changes, including what changed and who authorised it. |
| Evidence of distribution and awareness | Usage statistics, read acknowledgements, or communications notifying staff of updates. |
| Archived superseded versions | Clearly marked as obsolete and stored separately from current documents. |

When an auditor asks **"How do you know this procedure was valid and approved at the time of the incident?"** you should be able to answer quickly and with evidence. If you can do that, you will provide confidence in your ways of operating.

# How Information Leadership Can Help

Information Leadership's iWorkplace™ Controlled Documents solution is built on Microsoft 365 and SharePoint, adding dedicated document control capabilities to the platform your teams already use. It provides automated approval workflows, version management with one-click publishing, review date tracking with reminders, and a built-in audit trail that logs every approval and publishing event.

Because iWorkplace™ works within your existing Microsoft 365 environment, adoption is straightforward – staff edit documents in Word as they are used to, with governance running in the background. There is no separate system to learn or maintain.

We have helped corporate organisations, councils, and government agencies across New Zealand move from scattered documents and manual tracking – to systems that pass audits with confidence. If you would like to discuss what this could look like for your organisation, we would welcome the conversation.

## How it works

Automate publishing, version control, and access for critical content.

**Self Manage:** Own your policies, procedures, and templates without relying on IT.

**Intuitive Interface:** Simple to use with built-in views for upcoming reviews and recent updates.

**Real-Time Collaboration:** Work together on documents, share feedback, and co-author changes instantly.

**Effortless Compliance:** Automated tracking and reporting help you meet legal and regulatory requirements with ease.

**Unmatched Security:** Access controls ensure only authorised users can view, edit, or share key documents.

**Automated Publishing & Version Control:** Keep everything current with seamless publishing, audit logs, and archiving. No manual effort required.

## Tangible Benefits

Your team always works with the lastest approved documents without chasing files or updates.

**Empowered Teams:** Collaborate easily while staying compliant and in control.

**Productivity:** Save time with automation and easy access to approved content.

**Reduced Risk:** Eliminate errors, outdated files, and unauthorised access.

**Peace of Mind:** Know your documents are secure, compliant, and always up to date.

Streamline, secure, and control your policies, procedures, and sensitive documents. Get in touch today.

0800 001 800
info@informationleadership.com
**informationleadership.com**

# Appendix A: Implementation Checklist

Use this checklist to ensure you've covered the bases when establishing your controlled documents program.

**This can serve as a handy summary of the steps discussed:**

| | |
|---|---|
| ○ Identify Critical Documents | List which document types (policies, procedures, forms, etc.) will be controlled. Don't try to control everything; focus on those that impact compliance, safety, quality, or legal obligations. |
| ○ Assign Document Owners and Approver | Every controlled document has a designated Owner responsible for its content and updates, and a defined Approver who gives final sign-off. Decide on any additional required roles (e.g., who will serve as document controller/coordinator, who are the typical reviewers). |
| ○ Set up a Central Repository | Create a single source of truth (a secure shared drive, SharePoint site, or dedicated system). Organise it in a logical way (by department, document type, etc.) and control permissions (e.g., only owners/editors can edit; everyone else can read). Populate it with the current versions of all in-scope documents. |
| ○ Define the Process | Document the lifecycle for how documents move from draft to approved to published to archived. This should include how new documents are added to control, how changes are made (with review/approval steps), and how often review is required. |
| ○ Implement Versioning and Templates | Ensure version control is active. Decide on your version numbering convention (e.g., major.minor format) and apply it consistently. Set up templates for common document types to standardise formatting and metadata (like title, dates, owner name, etc.). |
| ○ Migrate/Archive Old Documents | For existing documents, move the important ones into the new system after proper review and approval. Archive the rest or leave them as read-only if necessary, with clear "uncontrolled" labels. Over time, phase out any old repositories to avoid confusion. |
| ○ Schedule Reviews and Reminders | For each controlled document, set a next review date based on your policy (e.g., 1 year for most, shorter for critical content). Implement a reminder mechanism (automatic if using software, or manual calendar reminders) to alert owners when review dates are approaching. |
| ○ Training and Communication | Train those involved in the process (especially document owners and approvers) on how to use the system and follow the procedures. Announce the launch of the controlled documents repository to all staff, explaining how to access it and why it's important. Provide ongoing support or a point of contact for questions. |
| ○ Monitor and Adjust | After implementation, monitor how it's going. Check if documents are being reviewed on time and if people are accessing the controlled versions. Gather feedback and make improvements to the process or provide additional training as needed. |

This checklist can be used as a project plan outline for rolling out document control. Each checked item brings you closer to a fully functional system of controlled documents.

# Appendix B: Quick Reference – Controlled Documents Essentials

A condensed reference for the key principles and practices covered in this guide.

**Key elements include:**

| PRINCIPLE | WHAT IT MEANS IN PRACTICE |
|---|---|
| Single source of truth | One authoritative location for all controlled documents. Staff always access the latest version from this central repository. |
| Formal approval before use | Every document is reviewed and approved by authorised personnel before publication. No document goes live without sign-off. |
| Version control | Each revision gets a new version number. Superseded versions are archived and clearly marked. Only the current version is in active circulation. |
| Defined review schedule | Every document has a next review date based on its risk level. Reviews are triggered by schedule and by events (regulatory changes, incidents, audit findings). |
| Clear ownership | Each document has a named owner (responsible for content) and approver (responsible for sign-off). Responsibilities are visible in metadata. |
| Controlled changes | No unilateral edits. Changes follow a workflow: draft, review, approve, publish. Minor edits can be fast-tracked; major changes go through full review. |
| Audit trail | All approvals, publishing events, and changes are logged. You can demonstrate the full history of any document on request. |
| Managed access | Published documents are read-only for general users. Edit permissions are restricted to owners and authorised editors. |

# Appendix C: Frequently Asked Questions

## What's the difference between storing a document and controlling it?

Storing a document means saving it without special oversight. Controlling a document means managing it through formal version control, review, approval, and distribution. Controlled documents are official, version-controlled, and traceable – only the latest approved version is available for use, all changes are tracked, and old versions are archived. In short, controlling a document ensures it remains accurate and authoritative.

## Do we need a document control system if we already use SharePoint or Teams?

SharePoint and Teams provide basic version history and permissions, but they are not purpose-built for rigorous document control workflows. Many organisations using only these platforms struggle with uncontrolled copies, missing approvals, and difficulty tracking which version is official. To achieve true document control, you need either additional configuration (custom approval workflows, metadata, dedicated libraries) or a purpose-built solution like iWorkplace™ that adds structured governance to your existing Microsoft 365 environment.

## Is a form a controlled document?

The blank form template should usually be controlled – it needs version control and approval when changed. However, each filled-out form (a completed incident report, for example) is a record, not a controlled document. Records are managed through recordkeeping practices with appropriate retention, but they are not versioned once completed. Template = controlled; completed form = record.

## Can someone just edit a controlled document directly?

No. Once published, a controlled document should be read-only for general users. Any needed changes create a new draft version that goes through the review and approval workflow. This preserves content integrity and creates a traceable record of who changed what. That said, the process can be designed to make minor corrections quick – the goal is proportionate control, not unnecessary friction.

## What does ISO 9001 require for document control?

ISO 9001:2015 requires that documents are approved before use, kept current and available where needed, protected from unauthorised changes, and managed so that obsolete versions are identified and prevented from unintended use. It does not mandate specific software – you could pass an audit with a manual system – but the more documents you have, the harder that becomes. Electronic systems inherently support these principles through built-in version control, access permissions, and audit trails.

## Are spreadsheets and shared drives good enough?

They can work as a starting point, but they become risky and inefficient as you grow. Manual tracking is labour-intensive and error-prone – someone must remember to update the spreadsheet, move files to archives, manage permissions, and chase approvals. There is no automated audit trail. Most organisations reach a tipping point where the overhead and risk of manual methods outweigh the cost of a dedicated solution. If you have more than a handful of controlled documents, or operate in a regulated environment, purpose-built software will save time and reduce risk.

## How do we get staff to follow document control procedures?

Make the right thing easier than the wrong thing. Provide a well-organised, easy-to-navigate central library. Explain why document control matters using real examples. Ensure leaders visibly use the system. Provide brief, practical training. Use automated reminders and notifications. And treat the process as improvable – gather feedback and adjust. Adoption builds over time as people experience fewer headaches finding information and passing audits.

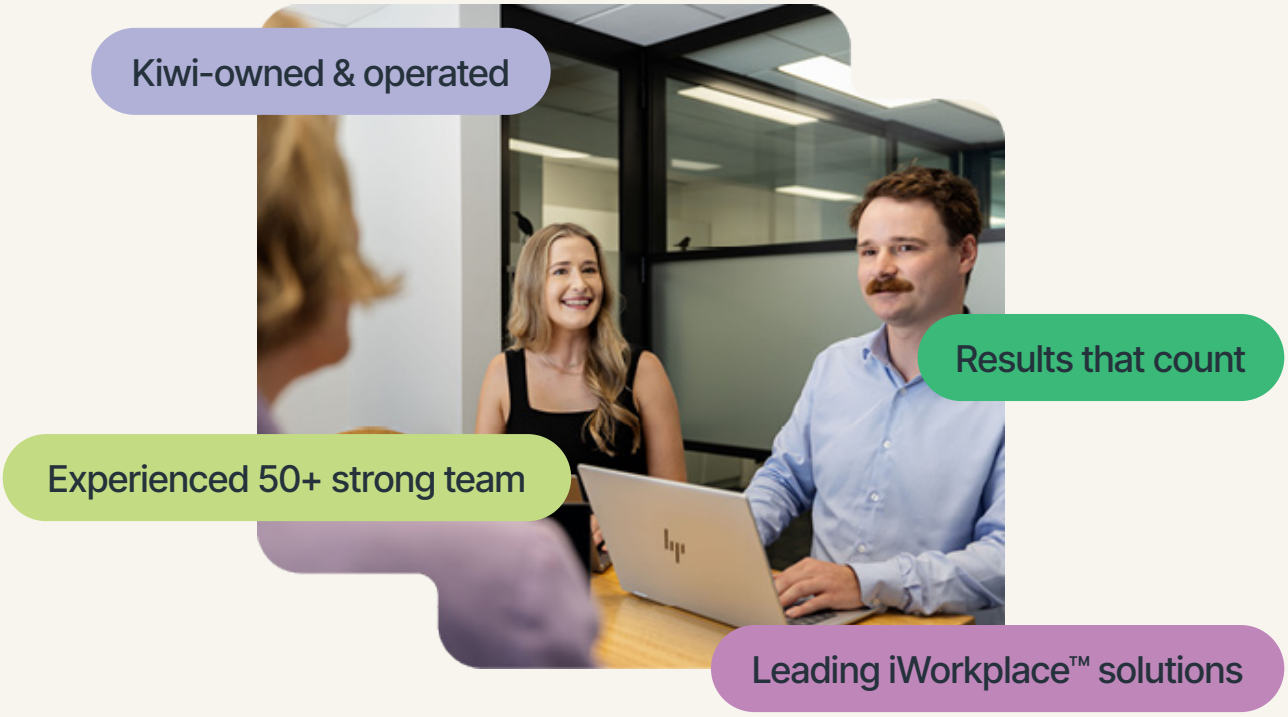
## How much training is needed?

For general staff who just need to find and read documents: a brief orientation (15–30 minutes) showing where documents live and how to recognise the current version. For document owners and approvers: a focused session (1–2 hours) covering the full lifecycle from creation to archive. Provide quick-reference guides for ongoing support. Because modern solutions like iWorkplace™ Controlled Documents work within familiar Microsoft 365 platforms, the learning curve is typically modest.

# About Information Leadership

Reliable information powers reliable outcomes. That's why for over 20 years we've helped organisations turn Microsoft 365 into a place people trust. We guide government agencies, councils, iwi organisations and private enterprises to work with structure, safety, and confidence.

As a Microsoft AI Cloud, Modern Work, and Change & Adoption Partner, we extend M365 with proven iWorkplace™ solutions and frameworks and people-first delivery.




**Make compliance easier – and more reliable.**

If new regulations and audit pressure are raising the stakes, we can help. Our experts design Microsoft 365 solutions that reduce risk, save time, and build trust.

Contact us to get started

0800 001 800
info@informationleadership.com
**informationleadership.com**

Information Leadership™
CONFIDENCE, BY DESIGN