Risetime

THOUGHT LEADERSHIP WHITEPAPER

THE COST OF NOT KNOWING

How Intelligent Migration Turns Orphaned Content into Governed Information

Generic classification understands the industry. Intelligent Migration learns the organization.

By Patrick A Windsor II

risetime.com

EXECUTIVE SUMMARY

Most organizations do not make a deliberate decision to keep every document forever. They get there slowly, as people leave, departments change, applications are replaced, and old file shares are carried forward.

I have seen this happen many times. The files are still there, but the people who understood them are gone. A filename tells you very little. A folder may refer to a department that no longer exists. A scanned image may be an important record, a duplicate, or something whose retention period expired years ago. Without the right metadata, there is no reliable way to know.

Once that context is lost, people become cautious. They keep the content because deleting it feels risky. Over time, that fear becomes the organization's unofficial retention policy.



The organization may have a retention schedule, but it cannot apply that schedule to content it cannot identify.

Keeping everything does not remove the risk. It moves the risk into storage, backups, security, privacy, future migrations, investigations, legal holds, and discovery. Storage may be inexpensive, but managing information that nobody understands is not.

We developed Intelligent Migration to solve that problem. It identifies documents in the context of the company that owns them. A broad label such as "contract" or "invoice" is often not enough. The useful answer is the company's actual document type, the metadata it requires, where it belongs, and which retention rule applies.



In this ebook, I explain why unknown content accumulates, what it really costs to keep it indefinitely, and how organizations can turn that content into information they can manage with confidence.

CONTENTS

01	When Institutional Knowledge Walks Out the Door	4
02	How Fear Becomes a Retention Strategy	5
03	The Real Cost of Keeping Everything	6
04	Why Generic Classification Is Not Enough	8
05	From Recognition to Company Specific Understanding	9
06	The Intelligent Migration Approach	10
07	Two Common Sources of Unknown Content	12
08	Case Study: Two Million Inherited Documents	13
09	Case Study: More Than Ten Million Paper and Network Documents	14
10	From Identification to Defensible Action	16
11	Human Oversight, Confidence, and Trust	17
12	Building the Business Case	18
13	A Practical Roadmap	19
14	Conclusion: Govern What You Know	21

WHEN INSTITUTIONAL KNOWLEDGE WALKS OUT THE DOOR

Unknown content is often the residue of ordinary business change, not deliberate neglect.

In my experience, unknown content is rarely caused by one bad decision. It is usually the result of normal business change. The people who created the documents understood the abbreviations, project names, folder conventions, and the difference between a working copy and a final record. They did not write all of that down because everyone involved already knew it. Then someone retires. A department is combined with another group. A business is acquired or sold. A legacy application is shut down. A shared drive is copied into a new environment so it will remain available. Years later, the files are still there, but the people who knew what they meant are not. That is a loss of institutional knowledge at the document level. The organization still has the files, but it has lost the context needed to manage them.

How content becomes orphaned

- Employees leave before documenting their folder structures, naming conventions, or business rules.
- Teams reorganize, leaving content associated with departments, cost centers, or projects that no longer exist.
- Legacy systems are exported into file shares, preserving bytes but losing application metadata and context.
- Paper records are scanned in bulk with filenames that identify only a box, batch, or scan date.
- Copies accumulate through email attachments, local drives, collaboration sites, and backup restores.
- Older company specific terminology no longer matches the organization's current taxonomy or retention schedule.

The problem compounds over time

Every year of delay makes interpretation more difficult. The remaining employees are further removed from the original process. Systems change again. New copies are created. The organization may know how much data it has, but not what proportion is valuable, redundant, sensitive, obsolete, or subject to retention requirements. This is why the problem cannot be solved solely by asking employees to clean up their folders. The employees with the necessary knowledge may no longer be present, and current staff may reasonably hesitate to make disposition decisions about documents they did not create.



Organizations do not merely lose track of files. They lose the business context required to govern those files.

HOW FEAR BECOMES A RETENTION STRATEGY

When the content cannot be identified confidently, keeping it feels safer than deleting it.



I understand why organizations keep information they cannot identify. A document may support a contract, a transaction, an employment decision, a regulatory requirement, or an intellectual property claim. It may also be subject to a legal hold. If nobody knows what it is, deleting it feels like an unnecessary risk.

That uncertainty produces familiar reactions:

- "Someone may need it someday."
- "It might be a record."
- "We do not know which retention rule applies."
- "Legal should approve deletion, but legal cannot review millions of files manually."
- "Storage is inexpensive, so keeping it is easier."

Each decision seems reasonable on its own. Taken together, they create an unmanaged policy of indefinite retention. The approved retention schedule may say one thing, but the daily practice becomes, "Keep everything unless someone can prove it is safe to delete."

Retention by fear is not neutral

Indefinite retention preserves obligations along with information. The organization must continue securing the content, maintaining access controls, including it in backup and disaster recovery processes, moving it during future migrations, and evaluating it when litigation, an investigation, or a privacy request arises.

The answer is not aggressive deletion. The answer is intentional retention. Valuable records should be kept for the correct period. Information covered by a legal hold must be protected. Information that has met its retention requirements should move through an authorized and documented disposition process.

Defensible disposition is not indiscriminate deletion. It is the consistent application of approved rules to information that has been understood well enough to classify.

THE REAL COST OF KEEPING EVERYTHING

The price of a stored document is larger than the number of gigabytes it occupies.

Storage pricing encourages a narrow calculation: capacity multiplied by a monthly rate. That figure is real, but it is only one component of the information's lifecycle cost. Every retained document may be copied, replicated, backed up, indexed, scanned, secured, migrated, searched, preserved, reviewed, and produced.

Cost dimension	What indefinite retention creates
Storage and resilience	Primary capacity, replicas, backup copies, archives, disaster recovery, and data transfer.
Administration	Monitoring, patching, indexing, permissions, support, recovery testing, and repository maintenance.
Security and privacy	A larger attack surface, more sensitive content to protect, and more data to locate for access or deletion requests.
Migration	Repeated assessment, transfer, validation, and reconciliation of content with no continuing value.
Compliance	Difficulty demonstrating that approved retention and disposition policies are operating consistently.
Litigation and investigation	More potentially responsive information to preserve, collect, process, search, review, and produce.

THE REAL COST OF KEEPING EVERYTHING

Total retention cost = storage + administration + security + migration + compliance + legal discovery

01

Storage and operational cost

A file that remains for decades rarely stays in one place. It is backed up, replicated, restored, indexed, and eventually moved to new infrastructure. During each technology refresh, unknown content creates a dilemma: migrate it again, or fund a separate effort to understand it. Organizations frequently choose another lift and shift because the migration deadline arrives before the classification work can be completed. The organization then pays repeatedly to move the same uncertainty from one platform to another.

02

Compliance and privacy cost

Retained information must be protected. The U.S. Federal Trade Commission advises businesses not to collect and retain personal information unless it is integral to the product or service and warns that keeping sensitive information longer than necessary raises risk. International privacy regimes also apply the principle of storage limitation to personal data. Requirements vary by jurisdiction and industry, but the governance lesson is consistent: retaining information without a defined need can create exposure rather than eliminate it. [1][2]

03

Litigation and investigation cost

In litigation, potentially relevant electronically stored information may need to be preserved, collected, processed, reviewed, and produced. Federal discovery rules expressly address electronically stored information, proportionality, preservation, and the consequences of failing to preserve information that should have been retained. They do not create a universal requirement to keep every document forever. Sound information governance must coordinate routine disposition with the suspension of deletion when a valid legal hold applies. [3]

Documents kept without a business or legal need can still become part of the discovery population if they are relevant and within the organization's possession, custody, or control. Even if a document is ultimately irrelevant or privileged, the organization may incur expense to determine that fact.

WHY GENERIC CLASSIFICATION IS NOT ENOUGH

Recognizing the broad category of a document is useful. Governing it requires a more specific understanding.

Many tools can read a scanned image and decide that it looks like a contract, invoice, or personnel document. That is useful, but it is not enough to govern the document. We still need to know who owns it, which business process created it, what the company calls it, which metadata is required, where it belongs, and which retention rule applies.

Level of understanding	Illustrative result	Decision value
Generic	"This is a contract."	Supports broad search or routing.
Industry specific	"This is a healthcare provider agreement."	Adds domain context and narrows likely handling.
Company specific	"This is our Provider Services Agreement for this relationship and business process."	Supports mapping to the company's taxonomy, metadata, repository, ownership, and retention rules.

Two companies in the same industry can use completely different templates, terminology, metadata, approval processes, and retention schedules. A label that works for one may be far too broad for the other. Even inside one company, the same words can mean different things across business units or different periods in its history.



Generic classification understands the industry.
Intelligent Migration learns the organization.

OCR is not understanding

Optical character recognition can convert an image into machine readable text. Search can locate words and phrases. Neither capability, by itself, establishes the document's role in a company specific business process. A scan may contain the word "invoice" but actually be a dispute notice, an approval packet, a duplicate attachment, or supporting documentation governed differently from the invoice of record. **The distinction matters because migration and disposition decisions depend on context, not merely vocabulary.**

FROM RECOGNITION TO COMPANY SPECIFIC UNDERSTANDING

The objective is not simply to label files. It is to reconstruct enough business context to govern them.

Every company has its own information language. You can see it in document templates, taxonomies, records schedules, metadata models, department names, product codes, customer identifiers, and old naming conventions. Intelligent Migration has to learn that language if the results are going to be useful.

We use the evidence inside and around the document to rebuild the missing context. Depending on what is available, that evidence may include:

01
Text extracted from native files or scanned images

02
Document layout, recurring labels, headings, and form structure

03
Existing filenames, folder paths, dates, owners, and system metadata

04
Company specific acronyms, templates, project names, product names, and process terminology

05
Examples of documents already classified correctly by knowledgeable staff

06
The organization's target taxonomy, metadata requirements, and retention framework

The goal is a richer result

The result should connect a source file to a document type the company actually uses, the metadata that matters, the likely owner, the right destination, and the appropriate governance treatment. Those fields will be different for every customer because the business context is different.

That company specific focus is especially important for proprietary forms, internal reports, historical templates, customer deliverables, and legacy records whose meaning depends on how the company operated when they were created.

THE INTELLIGENT MIGRATION APPROACH

Intelligent Migration creates a bridge between unknown content and a governed destination.



At Risetime, we built Intelligent Migration for scanned documents and network file shares whose contents are no longer understood. We identify what the documents are, extract the metadata the customer needs, and create the structure required to manage them properly.

Stage	Purpose	Representative outcome
1. Discover	Establish what content exists and where it resides.	A defined source population for analysis.
2. Interpret	Analyze document content and available contextual signals.	Readable text, document indicators, and candidate types.
3. Align	Map findings to the company's own taxonomy and information language.	Company specific classification and metadata mapping.
4. Decide	Apply business, records, privacy, and legal rules with appropriate review.	A documented treatment path and exception queue.
5. Act	Move governed content or execute authorized disposition.	Content stored correctly, retained intentionally, or disposed of defensibly.

THE INTELLIGENT MIGRATION APPROACH

A service, not only a classifier

The technology does a large part of the work, but the work starts with understanding the customer. We define meaningful document types, gather representative examples, map the source content to the target structure, identify exceptions, and agree on who has authority to make each decision.

That is why Intelligent Migration is both a product and a service. We are not producing labels for their own sake. We are helping the customer reach a controlled business outcome.

A governed output

Once we understand the content, we can prepare it for a document management system, organize it in a structured repository, retain it under approved rules, route it for review, or identify it for authorized disposition after legal holds and other requirements have been addressed.

The destination is the customer's choice

Intelligent Migration is not tied to OpenText Content Server or any other single platform. We can import the documents and their metadata into Alfresco, FileNet, Documentum, SharePoint, OpenText, or another document management system, provided the destination offers the APIs needed for the import.



If a direct import is not required, we can organize the results in a spreadsheet that lists each document with its respective classification and metadata. The customer can then use that structured output for migration, review, remediation, or disposition..

Intelligent Migration produces governed information. The customer decides whether that information is delivered to a document management system or in a structured spreadsheet.

> The measure of success is not how many files were scanned. It is how much uncertainty was converted into governed, actionable information.

TWO COMMON SOURCES OF UNKNOWN CONTENT

Scanned archives and network file shares create different technical challenges, but the same governance problem.

01

Scanned documents: the image has survived, but the context has not

Scanning preserves access to paper, but it does not automatically preserve meaning. Large scanning projects may produce images grouped by box, batch, date, or barcode. If indexing was limited, the organization may have millions of readable pages without reliable document boundaries, types, dates, owners, or business identifiers.

Even when OCR is available, the extracted text may be imperfect because of handwriting, stamps, skewed pages, low contrast, historical fonts, or degraded originals. Classification must account for uncertainty and may require targeted human review.

Scanning solves the paper problem. It does not solve the information problem. The archive becomes manageable only after its contents are identified and connected to the company's classification and retention framework.

02

Network file shares: context hidden in paths and habits

Network file shares often grow organically. Employees create folders for clients, projects, years, departments, and personal working files. Some structures are disciplined; others reflect individual preferences. Access rights may be inherited over many years, and duplicated folders may exist because teams copied information instead of moving it.

The path itself can contain useful context, but it can also mislead. A file stored in a "Contracts" folder may be a draft, a template, correspondence, or supporting material. A file named "final" may have been superseded years ago. Content analysis must therefore be combined with contextual evidence rather than relying on the filename or location alone.

A shared governance challenge

In both environments, the organization needs to answer the same questions: What is this? Does it still matter? Who is responsible for it? Is it sensitive? How should it be classified? Where should it live? How long should it remain?

CASE STUDY: TWO MILLION INHERITED DOCUMENTS

A global transportation company turned an acquisition era document mystery into governed information.

One of our global transportation customers acquired another business and inherited approximately two million documents. The documents came across in the transaction, but the knowledge behind them did not. None of the employees who came with the acquisition could reliably explain what the documents were, which metadata mattered, or how long they needed to be retained.

Simply moving two million unidentified documents into a new repository would have moved the problem, not solved it. Deleting them without understanding their content and retention requirements was not a responsible option either.

Teaching the model the organization's document language

We started with several exemplar documents that represented the acquired company's document types. Those examples taught the AI the customer's real document language, including its terminology, structure, and recurring patterns. We were not asking the system to recognize a broad transportation category. We were teaching it to recognize the documents this company actually used.

> **Using company specific exemplars, Intelligent Migration achieved 98% classification accuracy across the evaluated document population.**

A controlled exception path

Intelligent Migration classified the evaluated population with 98% accuracy. We did not force the remaining documents into a category. Our librarians reviewed those exceptions and assigned the correct classifications manually. This allowed the technology to do the work at scale while our experts concentrated on the documents that genuinely needed judgment.

From classification to governed lifecycle management

After identifying the documents, we extracted the metadata required for each type and imported the documents into OpenText Content Server. We also assigned the appropriate Records Management classification so each document could enter a controlled lifecycle.

OpenText Content Server was the destination selected for this project. Intelligent Migration was not dependent on OpenText; the same classified documents and metadata could have been delivered to another document management system with suitable APIs or provided in a structured spreadsheet for the customer to use. The customer did more than complete a bulk import. It turned two million inherited documents into information that could be found, managed, retained for the correct period, and eventually destroyed through an authorized records management process.

> **The project replaced inherited uncertainty with company specific classification, usable metadata, and a governed path to eventual disposition.**

CASE STUDY: MORE THAN TEN MILLION PAPER AND NETWORK DOCUMENTS

A manufacturing company unified decades of paper and network content in a governed digital repository.

Another customer, a manufacturing company, had several closets filled with paper and a network file share containing material dating to the late 1990s. Together, those sources held more than ten million documents. The company did not just need scanning and file transfer. It needed to know what it had and bring the documents under records management.

Bringing paper into the same classification process

We worked with a scanning vendor that digitized the paper files and transferred the images to us by FTP. We then ran those images through Intelligent Migration to classify them and extract the required metadata.

The document types known at the beginning represented approximately 85% of the scanned population. Within that group, Intelligent Migration achieved 96% classification accuracy. Put simply, the system was highly accurate on the types it had been taught, and those types covered most, but not all, of the collection.

> **Initial scanned document results: 96% classification accuracy across the known document types, which represented approximately 85% of the scanned population.**

Using librarians to resolve exceptions and expand coverage

Our librarians reviewed the remaining documents. When they found a recurring type the system had not seen before, they classified examples and used them to teach the AI. We could then run that newly learned type across the collection and identify similar documents in bulk.

That learning loop is important. The technology handles recognized documents at scale, while our librarians resolve exceptions and expand what the system understands about the customer.

Applying the same process to the network file share

We ran the network files through the same classification, review, and metadata extraction process. When we found scanned images that had never been processed with OCR, we added that step so the text could be analyzed.

From ten million documents to one governed repository

We loaded the classified documents and their metadata into OpenText Content Server and assigned the appropriate Records Management classifications. The content could finally move through a controlled lifecycle instead of sitting indefinitely in closets and on a file share.

CASE STUDY: MORE THAN TEN MILLION PAPER AND NETWORK DOCUMENTS

OpenText Content Server was the customer's chosen repository in this case. The classification and metadata output was portable and could have been imported into another document management system with suitable APIs or delivered as a structured spreadsheet.

One year after the migration, the customer destroyed the physical source files and removed the migrated documents from the network file share. More than ten million documents were now searchable, structured, and governed in OpenText Content Server.

> **The outcome was not simply digitization. It was the retirement of physical and network file sources after their content had been identified, enriched, migrated, and brought under records management.**

FROM IDENTIFICATION TO DEFENSIBLE ACTION

Classification creates value only when it supports a controlled decision.

Not every document should have the same destination. Active, valuable, or regulated documents may belong in a modern document management system. Others may belong in a governed archive. Some need their access or metadata corrected. Some have met their retention requirements and may be eligible for disposition.

A practical decision framework includes the following outcomes:

Migrate
Move active or valuable content into the appropriate managed platform with useful metadata.

Retain
Preserve content for the required period in a governed location with appropriate protection.

Remediate
Correct access, metadata, format, ownership, or other governance problems.

Review
Send uncertain or high risk content to a knowledgeable person for resolution.

Hold
Move active or valuable content into the appropriate managed platform with useful metadata.

Migrate
Move active or valuable content into the appropriate managed platform with useful metadata.

Retention schedules require classification

A retention schedule connects record categories to retention periods and disposition instructions. It works only when a document can be mapped to the correct category. NARA's federal guidance illustrates the principle clearly: an approved schedule provides legal authority for the disposition of covered federal records. Private organizations work under different authorities and requirements, but the practical dependency is the same. The record must be identified before the correct rule can be applied. [4]

Disposition must be coordinated

Intelligent Migration supports the decision. It does not replace the people accountable for it. Records management, legal, privacy, security, technology, and the business may all have a role. Before acting, the organization should agree on who approves classification rules, how legal holds suspend routine deletion, which exceptions require review, and how disposition will be documented.

Intelligent Migration turns "we are afraid to delete it" into "we understand it well enough to govern it."

HUMAN OVERSIGHT, CONFIDENCE, AND TRUST

Automation should reduce the volume of manual work while keeping consequential decisions visible and reviewable.

Not every document will be clear. Some are incomplete, corrupted, handwritten, mislabeled, or genuinely ambiguous. Two document types may look nearly identical but follow different retention rules. We treat that uncertainty as part of the work, not as something to hide.

Designing the review model

Review rules should reflect business risk, not only a confidence score. A routine duplicate does not require the same scrutiny as a document containing health information, trade secrets, regulated records, or evidence related to pending litigation.

A practical review model can separate content into three broad paths:

01 High confidence, lower risk content that can proceed through an approved automated or streamlined workflow.

02 Content that requires validation because the classification is uncertain or the consequences are significant.

03 Exceptions that cannot be classified reliably and must be isolated for specialist review or preserved pending a decision.

Trust through transparency

People trust the process when they can see how document types were defined, how samples were validated, what happened to exceptions, and who approved the decisions. Intelligent Migration should be repeatable and explainable. It should never be treated as an unquestionable black box.

NIST security and privacy guidance connects information handling and retention with broader security and privacy controls and encourages coordination with records management functions. Although specific obligations differ by organization, the underlying principle is useful: retention, security, privacy, and records management should operate as one lifecycle rather than separate projects. [5]

BUILDING THE BUSINESS CASE

The value of Intelligent Migration appears in avoided cost, reduced exposure, and better use of information.

If the business case is based only on storage savings, it will miss most of the value. The larger return often comes from avoiding repeated migrations, reducing manual review, retiring old systems, and lowering the amount of unknown information that must be protected or reviewed later.

Potential value categories

- Smaller migration populations and fewer unnecessary files to transfer and validate
- Reduced dependency on manual document by document review
- Improved metadata and findability in the target document management system
- More consistent application of retention and disposition policies
- Reduced security and privacy exposure from forgotten sensitive content
- Better readiness for legal holds, investigations, audits, and discovery
- Retirement of legacy repositories that persist only because their contents are unknown
- Preservation of business knowledge that would otherwise disappear as experienced employees leave

A practical cost model

Start with more than terabytes. Count repositories and files. Look at duplication, age, access activity, backup footprint, migration effort, manual review time, security administration, and legal discovery volume. That baseline lets the organization compare the cost of continued uncertainty with the cost of classification and governed action.

I would state the benefits carefully. An initial assessment may produce ranges instead of exact savings, and age alone does not make a document disposable. A credible business case separates verified results from estimates and makes every assumption visible.

Questions executives should ask

01
How much content do we possess that no current employee can confidently explain?

02
How many times have we migrated that content without improving its classification?

03
What sensitive information may exist in repositories with outdated access models?

04
What does it cost to preserve, search, and review this content during litigation or an investigation?

05
Which legacy systems could be retired if their useful content were identified and moved?

06
Can we demonstrate that our retention schedule is being applied consistently to unstructured content?

A PRACTICAL ROADMAP

Begin with a representative problem, validate the company specific model, and scale with governance in place.

01 **Define the outcome**
Select a business problem: a migration, legacy system retirement, scanned archive, file share cleanup, compliance initiative, or discovery readiness need.

02 **Assemble governance**
Identify the business owner and involve records, legal, privacy, security, and technology stakeholders as appropriate.

03 **Select a representative population**
Choose content broad enough to expose real variation but bounded enough to validate efficiently.

04 **Build the company specific vocabulary**
Gather document examples, taxonomies, metadata requirements, records classes, naming conventions, and knowledgeable reviewers.

05 **Analyze and validate**
Classify the sample, examine errors and exceptions, and refine definitions using business feedback.

06 **Define decision paths**
Specify what may be migrated, retained, remediated, reviewed, held, or disposed of and who authorizes each action.

07 **Measure and scale**
Track classification quality, review volume, migration reduction, risk findings, and realized savings before expanding.

A PRACTICAL ROADMAP

What success looks like

A high classification percentage is useful, but it is not the whole definition of success. The classifications must lead to the right destination and the right retention treatment. Exceptions must remain visible. The measures should connect what the technology produced to what the business was able to do.

- Percentage of the source population assigned to an approved company specific document type
- Accuracy confirmed through representative validation samples
- Reduction in files and volume requiring migration
- Reduction in manual review effort
- Number of sensitive, mispermissioned, or otherwise high risk items identified
- Legacy repositories retired or reduced
- Documented disposition actions completed under approved governance

Avoid the big bang trap

Do not begin by trying to solve every repository and every document type at once. A focused pilot will expose the real data issues and give stakeholders something concrete to validate.

Once the classifications and decision authority are working, the program can expand by business unit, repository, document family, or risk priority.

CONCLUSION: GOVERN WHAT YOU KNOW

The unknown document problem is not primarily a storage problem. It is a knowledge problem.

Staff leave. Businesses reorganize. Systems are retired. Over time, the company loses the context that once made its documents understandable. When nobody can say with confidence what a file is or why it matters, the natural response is to keep it.

Keeping everything does not make the risk disappear. The company continues paying to store, protect, back up, migrate, search, and review information that may no longer have value. It also carries that information into every future compliance request, investigation, or lawsuit where it may be relevant.

The answer is not to delete first and ask questions later. It is to understand the content before acting on it.



Intelligent Migration restores the context required to classify information according to the company that owns it so valuable documents can be preserved, governed content can be placed where it belongs, and eligible information can be disposed of defensibly.

When Intelligent Migration learns the company's own document types, orphaned content can become governed information. The company can preserve what matters, dispose of what has reached the end of its lifecycle, and stop moving yesterday's uncertainty into every new system.

A starting conversation

A good place to start is one repository the organization still maintains mainly because nobody knows what it contains. Use it for a focused assessment. Determine what is there, how much can be identified, which company specific document types appear, what risks are present, and what governed outcomes are possible.

The question is no longer simply, "How much data do we have?"

The better question is: "How much of our information do we understand well enough to govern?"

ABOUT INTELLIGENT MIGRATION

We created Intelligent Migration to identify scanned documents and files stored in unstructured environments such as network file shares. It learns more than an industry category. It learns the customer's terminology, taxonomy, business processes, metadata, and governance requirements.

That understanding allows us to migrate content into the customer's chosen document management system with the right structure, apply retention, route exceptions for review, and support authorized disposition when the content reaches the end of its required lifecycle. Intelligent Migration can work with Alfresco, FileNet, Documentum, SharePoint, OpenText, and other platforms that provide suitable APIs. We can also deliver a structured spreadsheet containing the document inventory, classifications, and respective metadata when the customer does not want a direct system import.

For more information, visit www.risetime.com

Important note

This publication provides general information about information governance and migration practices. It is not legal advice. Retention, privacy, discovery, and disposition requirements vary by jurisdiction, industry, organization, and matter. Organizations should involve qualified legal, records management, privacy, security, and business stakeholders when designing policies or authorizing disposition.

Sources and further reading

[1] Federal Trade Commission, Protecting Personal Information: A Guide for Business

[2] UK Information Commissioner's Office, Principle (e): Storage limitation

[3] United States Courts, Federal Rules of Civil Procedure

[4] U.S. National Archives and Records Administration, Scheduling Records

[5] National Institute of Standards and Technology, SP 800 53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations

Draft prepared September 2026. Sources were accessed during drafting and should be revalidated before publication.