

JSK OVERSEAS INC. — OPERATIONAL RISK MANAGEMENT

## CASE STUDY

# Protecting Sensitive Records in a Complex Divestiture

*How a Multinational Financial Services Group Managed Records Governance, Retention Scheduling, and Secure Segregation During a High-Stakes Corporate Transaction*

**Service Area:** Operational Risk Management — Records Governance & Divestiture Compliance

**Industry:** Financial Services — Banking, Consumer Finance, Insurance, Asset Management

*Prepared by JSK Overseas Inc. | Business & Risk Management Consulting | Canada & United States*

## Engagement Snapshot

<b>Client Profile</b>	Large multinational financial services conglomerate — banking, consumer finance, insurance, and asset management
<b>Annual Revenue</b>	Multi-billion dollar revenue across diversified financial business lines
<b>Challenge</b>	Records segregation, retention schedule creation, and secure divestiture of sensitive records from a 30–40 year archive held at a third-party facility
<b>Third-Party Vendor</b>	Iron Mountain — physical and electronic records storage provider
<b>Stakeholders</b>	Chief Risk Officer (CRO), Legal Counsel, Law Firm Partner, Records Management Team, HR, Compliance, and Buyer Representatives
<b>Service Delivered</b>	Operational Risk Management — Records Governance & Divestiture Compliance
<b>Outcome</b>	Two structured retention schedules, full records segregation, secure destruction program, and governance framework compliant with multi-jurisdictional legislation

## Executive Summary

When a large multinational financial services group — spanning banking, consumer finance, insurance, and asset management — undertook a complex corporate divestiture, its Chief Risk

Officer (CRO) was confronted with one of the most operationally sensitive challenges a records governance program can face: how to protect decades of accumulated physical and electronic records from reaching the hands of a buyer who had no legal right to them.

With 30 to 40 years of records stored at Iron Mountain — the group's third-party records management facility — the organisation faced an immediate and multi-dimensional operational risk. The records had been accumulated by hundreds of employees across multiple business lines, in multiple jurisdictions, over multiple decades. They ranged from routine administrative files to highly sensitive personal data, regulated financial records, privileged legal correspondence, and proprietary business intelligence.

JSK Overseas Inc. was engaged to support the CRO in designing and executing a comprehensive records governance strategy that would protect sensitive information, ensure regulatory compliance, and give the organisation a defensible, auditable framework for managing both retained and divested records throughout the transaction and beyond.

***The central challenge was not simply what to keep — it was what to destroy, what to share, what to withhold, and how to do all of it legally, swiftly, and without exposing the organisation to regulatory sanction or litigation.***

## Background — The Organisation and Its Records Challenge

XYZ Group (name anonymised) was a large, publicly listed multinational financial services conglomerate with operations across Canada, the United States, and multiple international markets. Its diversified business model encompassed retail banking, corporate banking, consumer finance, life and general insurance, and asset management — each with its own regulatory obligations, client data environments, and internal records management practices.

Over the course of three to four decades, employees across all business lines had generated and submitted physical and electronic records to Iron Mountain for long-term storage. The cost of this storage was borne centrally by XYZ Group, and while individual business lines had nominal responsibility for their own records, there was no unified group-wide retention schedule, no standardised destruction policy, and no single inventory that accurately reflected what was held, where, and under what retention obligation.

When XYZ Group entered into a divestiture transaction — selling one or more of its core business units to a third-party buyer — the records situation became immediately critical:

- **The buyer demanded access to records.** As part of due diligence and transition planning, the buyer sought access to a broad range of business records held by XYZ Group, including records held at Iron Mountain. Not all of these records could be lawfully or safely shared.
- **Sensitive records needed to be protected.** Records containing privileged legal advice, personal data of clients and former employees, proprietary risk models, regulatory correspondence, and commercially sensitive business intelligence could not be transferred to the buyer without creating material legal, regulatory, and reputational exposure.
- **No defensible retention schedule existed.** The absence of a formalised, jurisdiction-compliant retention schedule meant XYZ Group could neither defend its current records holdings nor safely destroy records without risking regulatory breach or spoliation of evidence in potential future litigation.
- **Iron Mountain costs were ongoing and escalating.** With records accumulating over 30 to 40 years and no structured destruction program in place, Iron Mountain storage

costs represented a significant and growing financial liability — one that the remaining entity had no obligation to continue bearing for records belonging to divested business units.

## The Risk Landscape — What Was at Stake

The CRO's risk assessment identified the following interconnected operational, legal, regulatory, and reputational risks requiring immediate structured management:

Risk Identified	Inherent Risk Level	Potential Impact
Unauthorised buyer access to sensitive records	High	Catastrophic — regulatory sanction, litigation, reputational damage
Records destruction without legal authorisation	High	Severe — regulatory breach, contempt of court, fines
Incomplete inventory at Iron Mountain	High	Material — inability to demonstrate compliance during divestiture audit
Privacy breach — personal data of former employees/clients	High	Severe — PIPEDA / GDPR / state privacy law violation
Prolonged Iron Mountain storage costs post-divestiture	Medium	Financial — unnecessary ongoing liability for the remaining entity
Failure to segregate divested entity records from retained entity	High	Operational — legal ambiguity over ownership and access rights
Non-compliance with multi-jurisdictional retention laws	High	Regulatory — varying requirements across Canada, US, and international markets
Employee non-compliance with destruction policy	Medium	Operational — incomplete execution of governance framework

*Records management in the context of a corporate divestiture is not a back-office administrative function. It is a first-order operational risk — one that sits at the intersection of legal privilege, regulatory compliance, personal data protection, and commercial confidentiality. Getting it wrong exposes the organisation to consequences that no indemnity clause can fully absorb.*

## The JSK Approach — A Risk Resilience Framework for Records Governance

JSK Overseas Inc. approached this engagement through the lens of our core risk resilience methodology: diagnose the full risk landscape, design a structured and defensible framework, and deliver an implementation roadmap that the organisation's own people can execute with confidence. The engagement was structured across four sequential phases.

### Phase 1 — Records Inventory and Classification

The first and most foundational task was establishing a complete, accurate inventory of all records held at Iron Mountain on behalf of XYZ Group. This involved:

- Engaging directly with Iron Mountain to obtain a full manifest of all physical and electronic records held under XYZ Group's storage agreement, categorised by business unit, record type, date range, and physical location.
- Cross-referencing the Iron Mountain manifest against internal records management systems to identify discrepancies, unclassified boxes, and orphaned records with no clear business unit ownership.
- Classifying all records into one of three categories: records belonging exclusively to divested entities; records belonging exclusively to retained entities; and shared or commingled records requiring further legal review to determine ownership and transferability.
- Flagging records containing personal data (client, employee, or third-party), legally privileged communications, regulatory correspondence, and commercially sensitive proprietary information — each requiring a distinct treatment protocol.

This inventory phase produced the foundational data set upon which every subsequent decision in the engagement was made. Without it, no defensible retention schedule, destruction program, or segregation protocol could be constructed.

### Phase 2 — Dual Retention Schedule Development

With a complete and classified inventory in hand, JSK Overseas Inc. — working in close collaboration with the organisation's appointed external law firm — developed two distinct and legally compliant retention schedules tailored to the divergent needs of the retained and divested entity populations.

#### Retention Schedule 1 — Retained Entities (Compliance-Driven)

The retention schedule for the entities remaining under XYZ Group's post-divestiture ownership was designed to be fully compliant with all applicable legislation in every jurisdiction in which those entities operated. This included:

- Federal and provincial financial services regulations in Canada, including OSFI guidelines on record retention for regulated financial institutions.
- US federal and state banking, insurance, and consumer finance regulations, including requirements under the Bank Secrecy Act, Gramm-Leach-Bliley Act, and applicable state insurance codes.
- Privacy legislation obligations under PIPEDA (Canada), applicable US state privacy frameworks, and any applicable international data protection standards.
- Litigation hold obligations, ensuring that records subject to actual or reasonably anticipated legal proceedings were quarantined from the destruction schedule pending legal clearance.

This schedule established minimum and maximum retention periods for each record category, clearly defined the triggering events for retention (such as the closing date of a contract,

termination of employment, or last date of client relationship), and specified approved destruction methods for each record type.

### Retention Schedule 2 — Divested Entities (Accelerated Destruction)

The retention schedule for divested entities was deliberately more aggressive in its destruction timelines — reflecting the reality that XYZ Group had no ongoing operational, regulatory, or legal reason to retain records belonging to businesses it no longer owned, beyond the minimum legally mandated periods. This schedule was designed with three primary objectives:

- **Eliminate ongoing financial liability.** Ceasing Iron Mountain storage costs for records that served no legitimate retention purpose for the remaining organisation.
- **Eliminate the risk surface.** Reducing the volume of sensitive records that could become the subject of buyer demands, litigation discovery, or regulatory inquiry.
- **Ensure defensibility.** Ensuring that every destruction decision was legally authorised, formally documented, and executed in a manner that could withstand scrutiny in any future regulatory or legal proceeding.

The accelerated schedule was reviewed and endorsed by the external law firm, which provided a written legal opinion confirming that the proposed destruction timelines were compliant with all applicable retention obligations. This opinion formed a critical part of the governance documentation supporting the destruction program.

### Phase 3 — Records Segregation and Buyer Access Management

Parallel to the retention schedule development, JSK Overseas Inc. led the operational process of physically and electronically segregating records at Iron Mountain to prevent any unauthorised buyer access.

- A formal access control protocol was established with Iron Mountain, restricting all retrieval and access requests to a designated authorised list of XYZ Group personnel — removing any possibility of the buyer or its advisors accessing records through existing access credentials or relationships.
- Records identified as belonging exclusively to divested entities were physically quarantined within Iron Mountain's facility — clearly labelled, access-restricted, and placed on a destruction schedule in accordance with Schedule 2.
- Records that the buyer had a legitimate right to access — such as operational records directly relating to the transferred business — were identified through the classification process, reviewed by legal counsel for any privileged or sensitive content, and transferred to the buyer in a structured, documented handover process.
- A formal records transfer agreement was drafted by the external law firm, governing the terms under which transferred records were delivered to the buyer, including confidentiality obligations, permitted uses, and the buyer's obligation to comply with applicable retention and destruction obligations from the date of transfer.
- Commingled records — those containing data relating to both retained and divested entities — were subject to a bespoke review process, with redaction applied where necessary before any transfer to the buyer was authorised.

***The segregation process was not merely a logistical exercise. It was a legal and risk management imperative — ensuring that every record transferred to the buyer had been individually reviewed, approved by counsel, and formally documented in the chain of custody.***

### Phase 4 — Governance Framework, Policy, and Employee Compliance

The final phase of the engagement focused on embedding the new records governance framework into the organisation's ongoing operations — ensuring that the retained entity's employees understood their obligations, had the tools to comply with them, and were operating within a governance structure that would remain defensible long after the divestiture transaction closed.

- **Policy and SOP Development.** Working with the external law firm, JSK Overseas Inc. supported the development of a comprehensive Records Management Policy and accompanying Standard Operating Procedure (SOP) for records destruction. These documents defined authorised destruction methods for physical records (cross-cut shredding for paper; certified electronic erasure for digital media); the approval chain required before any destruction could proceed; the documentation requirements for destruction certificates; and the process for managing litigation holds that might suspend a destruction event.
- **Governance Structure.** A records governance committee was established, comprising representatives from Legal, Compliance, Risk, and Operations — with clear accountability for reviewing and approving destruction batches, escalating disputes, and reporting to the CRO on program progress. The law firm served in an advisory capacity to the committee throughout the program's execution.
- **Employee Training and Awareness.** A targeted awareness program was delivered to all employees of the retained entities, covering their obligations under the new retention schedule, the process for submitting records for destruction approval, the prohibition on sending new records to Iron Mountain without prior classification and retention review, and the consequences of non-compliance.
- **Ongoing Iron Mountain Management.** A formal protocol was established for the ongoing management of the Iron Mountain relationship — including regular inventory audits, a defined process for authorising new records submissions, and a quarterly destruction review cycle to ensure the accelerated schedule for divested entity records was being executed on time.

## Results — What Was Achieved

Outcome Area	Specific Achievement	Business Impact
<b>Records Segregated from Iron Mountain</b>	100% completion across all business lines	Buyer received only pre-approved, legally cleared record sets
<b>Retention Schedules Created</b>	Two distinct schedules — retained entity and divested entity	Full multi-jurisdictional regulatory compliance achieved
<b>Sensitive Records Protected</b>	Zero unauthorised disclosures to buyer during divestiture	CRO confirmed no material breach of confidentiality obligations
<b>Records Destroyed</b>	Aggressive destruction schedule for divested entity — legally authorised	Storage cost liability eliminated for non-retained records

<b>Governance Framework</b>	Policy, SOP, and law firm-endorsed destruction authorisation	Auditable paper trail established for all destruction activities
<b>Employee Compliance</b>	Training and awareness program completed across retained entities	Risk-aware records culture embedded in post-divestiture organisation

Beyond the specific operational outcomes, the engagement delivered three strategically significant results for XYZ Group's post-divestiture leadership:

- **CRO Confidence.** The CRO was able to close the divestiture transaction with documented assurance that no material sensitive information had been transferred to the buyer without legal authorisation — a critical requirement for regulatory sign-off on the transaction in multiple jurisdictions.
- **Regulatory Readiness.** In the event of any future regulatory inquiry into the transaction or the records management practices of XYZ Group, the organisation now had a complete, auditable documentation trail covering every material decision made about records during the divestiture — including the legal opinion supporting the accelerated destruction schedule.
- **Sustainable Records Culture.** Perhaps the most enduring outcome was the shift in organisational culture. Records management moved from a low-visibility administrative function to a board-visible risk management discipline — one that the retained entity's leadership now understood to be a material component of its operational risk framework.

## The JSK Risk Resilience Lens — What Made This Engagement Work

This engagement succeeded because it was approached as an operational risk management challenge — not a filing project. The following principles from JSK Overseas Inc.'s risk resilience framework were central to the outcome:

- **Diagnose before designing.** No retention schedule, destruction policy, or segregation protocol was developed until a complete and accurate inventory of the records landscape was in hand. Decisions built on incomplete information would have created, not eliminated, risk.
- **Legal and risk expertise in parallel.** The external law firm and JSK Overseas Inc. worked in parallel — not sequentially. Legal counsel provided the jurisdictional compliance framework; JSK provided the operational risk architecture. Neither could have delivered the outcome alone.
- **Governance as a risk control.** The records governance committee, the approval chain for destruction, and the documentation requirements were not bureaucratic formalities. They were risk controls — designed to ensure that no single individual could make a material records decision without oversight, and that every decision was defensible.
- **Speed with precision.** The divestiture transaction imposed non-negotiable deadlines. The program was designed to move quickly — but never at the expense of accuracy, legal compliance, or defensibility. Speed without precision in a records governance context creates the very risks it was designed to eliminate.
- **Embedding, not just delivering.** The engagement did not end when the transaction closed. The training program, the governance committee, the Iron Mountain management protocol, and the ongoing destruction schedule ensured that the

framework became part of the organisation's operating model — not just a project deliverable.

## Lessons Learned — What Every CRO Should Take From This Case

This engagement offers several lessons of direct relevance to any Chief Risk Officer or senior leader managing records governance in the context of a corporate transaction or significant organisational change:

- **Records governance is a divestiture risk, not an afterthought.** The absence of a formalised retention schedule at the outset of the divestiture significantly compressed the organisation's decision-making timeline and increased the complexity — and cost — of the governance program. Organisations undergoing any form of M&A activity should conduct a records governance readiness assessment before the transaction enters its critical path.
- **Third-party storage creates third-party risk.** Iron Mountain held decades of records under XYZ Group's name — but with limited visibility into what was held, who owned it, and what obligations applied to it. Any organisation using third-party records storage should maintain an up-to-date, classified inventory and a current retention schedule as a matter of standard operational risk hygiene.
- **Commingled records are a material legal risk.** Records that contain data relating to both retained and divested entities do not have a clean ownership answer. Identifying and managing them early — before the buyer begins making access demands — is essential to protecting legal privilege and commercial confidentiality.
- **Destruction is a legal act, not just an operational one.** Every destruction event in this program was legally authorised, formally approved, and documented with a destruction certificate. In any future litigation or regulatory inquiry, that documentation is the difference between a defensible position and an indefensible one.
- **Culture is the last line of defence.** The most sophisticated retention schedule and governance framework will fail if the people responsible for executing it do not understand why it matters. Employee awareness is not a soft deliverable — it is a hard risk control.

## Why JSK Overseas Inc. for Operational Risk Management

JSK Overseas Inc. is a Canada-wide business and risk management consulting firm specialising in helping small and medium-sized enterprises — and their senior leadership — navigate complex operational, governance, and compliance challenges through a risk resilience lens.

Our Operational Risk Management practice covers the full spectrum of risk exposures embedded in day-to-day business operations — from records governance and third-party risk to change management, regulatory compliance, and financial crime risk. We deliver practical, implementation-ready frameworks that your team can own and operate with confidence.

***This case demonstrates that operational risk management at the highest level is not about managing processes — it is about protecting the organisation when it is most vulnerable. That is the standard JSK Overseas Inc. brings to every engagement.***

**JSK Overseas Inc.**

*Business & Risk Management Consulting | Canada & United States*  
**Redefining Strategic Business Decisions Through Risk Resilience**  
*www.jskoverseasinc.com | Confidential — For Illustrative Purposes Only*