IRON MOUNTAIN®

2023 Education Series

Elevate the power of your work

Inspirational conversations with thought leaders to elevate your understanding of what's important to you today, what lies ahead, and how to get there.

Contents

Introduction

As organizations continue to embrace the new status quo, they continue to look ahead at what the future holds and how to elevate their ability to get there.

For our 2023 education series, we explored emerging trends that defined the year and paved the way for our digital future, including artificial intelligence (AI) and the emergence of new, and often unsanctioned, communication channels. We also examined the latest research on risk and its larger impact on economic and regulatory changes.

Topics we covered included:

1. The global recession: The impact on RIM & IG
2. What's up with WhatsApp?
3. Data, records, and compliance, oh my!
4. Generative AI and information governance: Friends or foes?
5. Measuring risk: What's your temperature?
6. Where, exactly, is your cloud?

The series aimed to prepare information and data governance professionals for both the known and unknown obstacles ahead with each discussion dedicated to elevating your ability to anticipate and mitigate potential risks.

The global recession: The impact on RIM & IG

Featuring:
Hamish McRae, Economist

The situation

In early 2023, the International Monetary Fund predicted one-third of the world would be in a global recession. To prepare for this economic downturn, records and information management (RIM) and information governance (IG) professionals needed to learn how to minimize organizational risk and exposure.

Elevate the power of your work

Economic models and forecasting depend on data. So, too, do the daily operations of organizations so they can remain vital and competitive. We must know where information is found, how it moves, what obligations exist for compliance, and what opportunities continue for RIM, data, and IG professionals.

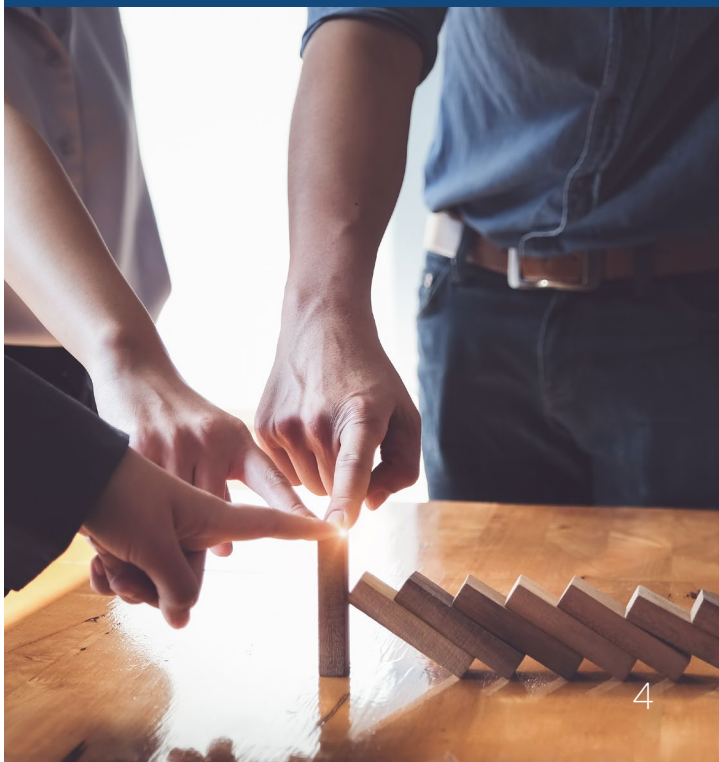
Key trends that will define the future of RIM and IG:

- As people learn that their data is not being abused, they'll be more likely to disclose their information for the greater good.
- Records and information (including data) managers must protect their assets in the cloud and elsewhere to keep cybercriminals from damaging it, stealing it, and holding it for ransom.
- Integrating big data and AI will enable us to view patterns that a human being simply cannot see.

Economic uncertainty is uncomfortable. Although plenty of unknowns exist, consider using this time to position your organization for recovery. What goes down must go up – elevate for a brighter tomorrow.

"Anybody involved in data is absolutely central to the world getting richer and happier over the next few years. We just need to improve the productivity of service industries so we can improve people's lives."

Hamish McRae
Economist



What's up with WhatsApp?

Featuring:
Steve Wright, CEO and Partner, Privacy Culture
Arlette Walls, Global Records and Information Manager, Iron Mountain

The situation

The popularity of WhatsApp, a free, centralized instant messaging and voice-over-IP (VoIP) app is immense—it had 2.44 billion active global users in April 2022 and is used in more than 180 countries. Due to its widespread acceptance, it has become a mainstay for business communications.

But when employees use WhatsApp and other non-secure applications for work, they can inadvertently expose their organization to steep fines, penalties, loss of trust, and reputational damage.

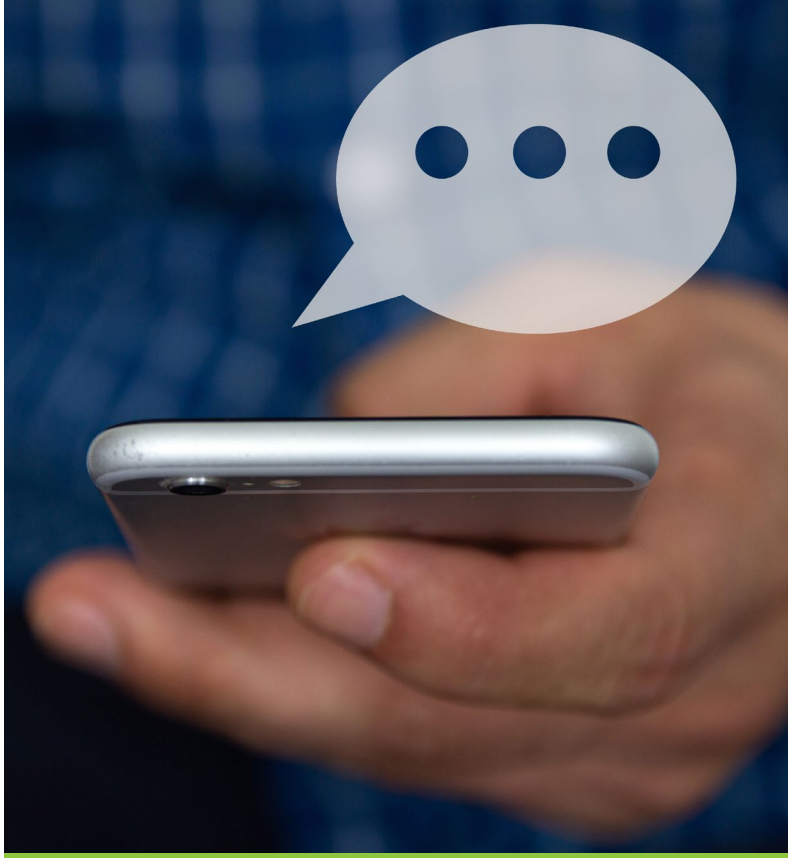
Elevate the power of your work

If employees use WhatsApp or other social media platforms for business-related communications, they are likely exposing the organization to risk. Even if a social platform claims to be secure, organizations must take the reins to protect their own data by creating/updating acceptable use policies.

This includes:

- Conducting a social audit and regularly following message traffic.
- Defining and solidifying social media policy parameters around acceptable and unacceptable apps.
- Communicating the policy to employees and clearly define what constitutes a record.
- Forming an oversight committee to ensure accountability.

By keeping business communications in approved channels, organizations can obtain full visibility into where their data sits, allowing them to eliminate potential risks more readily.



"Mitigate risk imposed by this social media platform and others by knowing what employees share, forming an airtight policy, and ensuring your entire staff follows it."

Arlette Walls
Global Records and Information Manager, Iron Mountain

Data, records, and compliance, oh my!

Featuring:
Kelly McIsaac, AVP, Data Risk Policies and Standards, TD Bank
Mike Meriton, Co-Founder and COO, EDM Council

The situation

Data has a lifecycle, which requires RIM professionals to retain and dispose of data appropriately per policy.

Elevate the power of your work

Historically, RIM professionals have been conflicted about their role in governing and managing data versus records, but the sheer volume and constant movement of today's data means RIM professionals must play a role in its compliant management.

There are three ways to accomplish this:

1. **Get to know the data supply chain.** Managing today's data requires a full understanding of its lifecycle, from creation to disposition. To obtain this greater view, it's critical to understand countries' differing data privacy laws, the purpose the data serves at each point in its lifecycle, and its source and flow.

2. **Protect all data, regardless of location.** Today's digital environment means many organizations have data living onsite and in the cloud. As such, RIM professionals must know where data resides and the impact that may arise from disposing of it.

3. **Create a data-literate organization.** As many organizations fail to define data ownership, take the step to create a data-literate organization that actively communicates data leaders and how it is used to inform better decision-making. If needed, consider appointing departmental data stewards.

We can no longer think about the rules for data management solely at the end of its primary purpose. Rather than talking about records, regulators are talking about the full data supply chain. There's never been a better time to elevate the end-to-end data lifecycle.

"Everyone in business should be using data to drive how they make their decisions. It shouldn't be an afterthought. Start looking at your data and be trained on what data assets will help you improve your decision-making."

Mike Meriton
Co-Founder and COO, EDM Council

Generative AI and information governance: Friends or foes?

Featuring:

John Isaza, Partner, Privacy and Information Governance, Rimon Law Group, Inc.
Ryan Zilm, Global Data Strategist and Former Chairman of the Board, ARMA Int'l
Arlette Walls, Global Records and Information Manager, Iron Mountain

The situation

The generative AI revolution is happening all around us. Yet for all the potential benefits it brings, it also carries its share of risks. Chances are many of your employees are already exploring the capabilities of generative AI or soon will. Many will test these capabilities in the workplace, potentially exposing your organization to numerous privacy, compliance, and legal issues.

Elevate the power of your work

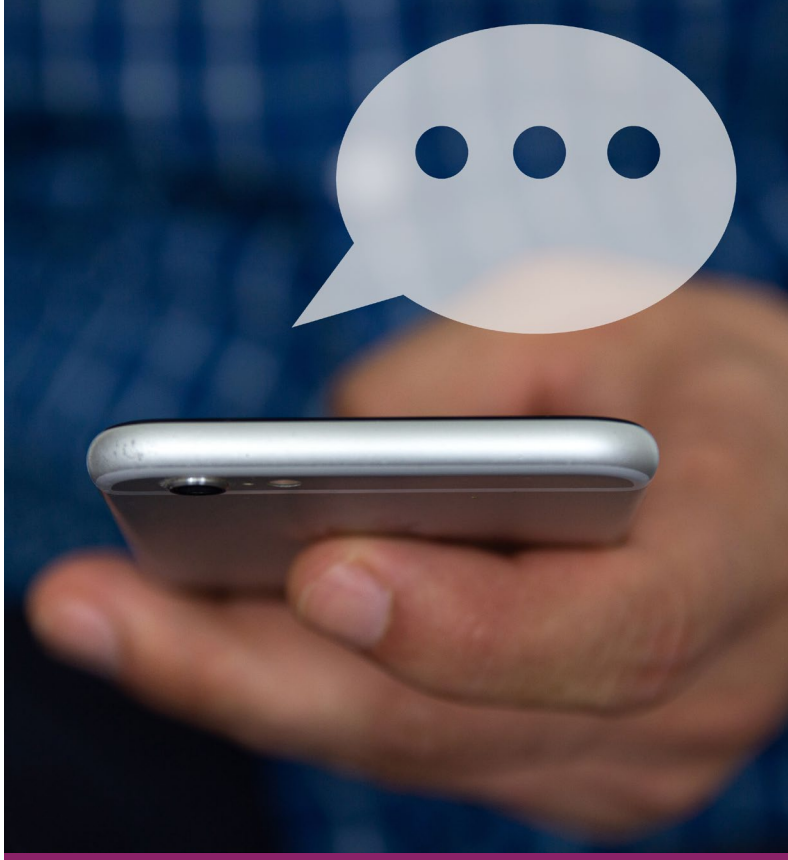
Organizations must stay ahead of the generative AI movement by creating policies to address its role within the workplace. Such policies should define whether the use of generative AI is permitted as well as provide clear guidelines around how it can be used.

When creating a policy, consider the following:

- Educate staff members on the use of proprietary/sensitive information within AI tools and the ramifications that come from this.
- Reinforce the importance of double-checking all AI-generated content for accuracy.
- Establish an end-to-end system to flag sensitive or inappropriate content.
- Clarify your vendors' AI policies to clearly understand how your data will be handled.
- Ensure you stay up to date with country-, state-, and industry-specific regulations.

Finally, we must remember that generative AI will only continue to get smarter and become more widely adopted. As a result, RIM and IG professionals will need to regularly revisit any established policies to ensure they still meet the needs of their workforce.

/ Elevate the power of your work



"When it comes to generative AI, garbage in, garbage out, as they say. You must make sure you have great data hygiene—otherwise, it could inadvertently lead you to bias and other types of issues."

John Isaza
Partner, Rimon Law Group, Inc.

Measuring risk – What's your temperature?

Featuring:
John Ferguson, Practice Lead for Globalization, Trade and Finance, Economist Impact

The situation

Iron Mountain sponsored a global study conducted by Economist Impact that explored how organizations manage, minimize, and negate risk with a focus on what has changed over the past three years. According to the study, 90% of executives identified risk as their top priority. But with only 36% currently integrating risk management into overall strategy and just 4% reporting the presence of risk committees, organizations have room for growth.

Elevate the power of your work

As risk becomes more complex, organizations must anticipate it, both from internal and external sources, be able to absorb the shock, and bounce back from it quickly. Regardless of an organization's size or sector, risk management should remain a core tenet. This is best accomplished by adopting and promoting risk literacy and awareness at the top of the organization and cascading it down to every employee and stakeholder.

Some risk factors that organizations should consider:

- **Technology** – Technology serves as both an organizational risk and a solution to that risk.
- **Workforce policies** – Hybrid and similar workplace environments pose additional risk factors that organizations must consider.
- **Geopolitics and climate change** – These two factors will have a significant impact on global financial markets.
- **Supply chains** – Risk and resilience now define supply chains, replacing the existing era where they predominantly provided cost minimization.

RIM and IG professionals play a crucial role in ensuring an organization is resilient to risk. Governance, security, and privacy begins with managing the integrity of company-wide data, whether it's at rest or in motion.

"Active organizations take the time and effort to understand and monitor their risks, while making sure they have the technology, people, and solutions to increase their resiliency against risk."

John Ferguson
Practice Lead for Globalization, Trade and Finance, Economist Impact

Where, exactly, is your cloud?

Featuring:
Julia Bonder-Le Berre, Head of Global Privacy, Iron Mountain
Steve Lester, Senior Corporate Counsel, Iron Mountain

The situation

Cloud computing brings scalability, cost reductions, and enhanced security to organizations of all sizes. However, any enterprise choosing to move its data to the cloud must identify areas of risk and how to address them, including making sure all suppliers comply with privacy principles, data governance, and security.

Elevate the power of your work

Before initiating a cloud project, it's important to understand the risks and best practices for securing data in the cloud and how to choose the right partner.

Some of the common areas of risk include:

- **Data resiliency** – The enterprise must identify what flexibility it has around hosting data to allow for better data mapping and compliance during the cloud transition.
- **Privacy** – As moving to the cloud grants suppliers access to enterprise files through a third-party platform, fail safes must be created that allow partners/suppliers to only access the files they need, while protecting personal and proprietary business data.
- **Security** – A robust data incident management process helps enterprises remain responsible to regulators, customers, and employees. Crucial to this process is thoroughly evaluating all potential partners to ensure alignment in security practices.

The goal is to select a cloud provider that respects your personal data to the same extent you do. When in doubt, look to the three Cs: commitment, controls, and contract. This means 1) agreeing with a vendor's commitment to data privacy, 2) agreeing with their controls regarding policies, procedures, and employee training, and 3) ensuring they will stand behind the contract terms if violated. Remember, the relationship is ongoing, so it is critical to regularly audit and assess to ensure the proper handling of your data.

"Outsourcing data to another company comes with certain risks. However, if you choose the right cloud provider, your overall risk is reduced."

Steve Lester
Senior Corporate Counsel, Iron Mountain

Elevate the power of your work

Our goal is to help you respond to today's challenges as well as to prepare for whatever tomorrow holds.

In case you missed any of these webinars, visit our Education Series page to watch them on-demand and sign up for future webinars.

Additional resources

The global recession: The impact of RIM & IG

- 11 New Year's business goals for 2024
- The world in 2050 – How to think about the future
- Ensure business resiliency

What's up with WhatsApp?

- The messaging dilemma: Grappling with employees' off-system communications
- Acceptable use policy (AUP)
- Do you know what's up with WhatsApp at your organization?

Data, records, and compliance, oh my!

- Best practices for managing data, records, and information
- How to develop a relevant and effective information governance strategy
- Essential steps for setting up a high-quality data supply chain
- Understanding the continuing evolution of data, records, and compliance

Generative AI and information governance: Friends or foes?

- Managing the risks of generative AI
- Generative AI offers great promise with the right guardrails
- Unpacking ChatGPT for the information management industry - A SWOT Analysis
- How to safeguard your data in the fast-moving world of generative AI

Measuring risk – What's your temperature?

- Shift your focus to anticipation
- Build risk awareness from the inside and out
- Risk amplified: Cultivating awareness across the organization
- Risk and resilience, two sides of the same coin: Explore the latest research

Where, exactly, is your cloud?

- Role of privacy in ESG whitepaper - Piccaso Privacy Labs
- Top 6 considerations for cloud security
- The importance of cloud-to-cloud backup
- Put data in its place
- Understanding data privacy and cloud computing

800.899.IRON | ironmountain.com

About Iron Mountain

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.