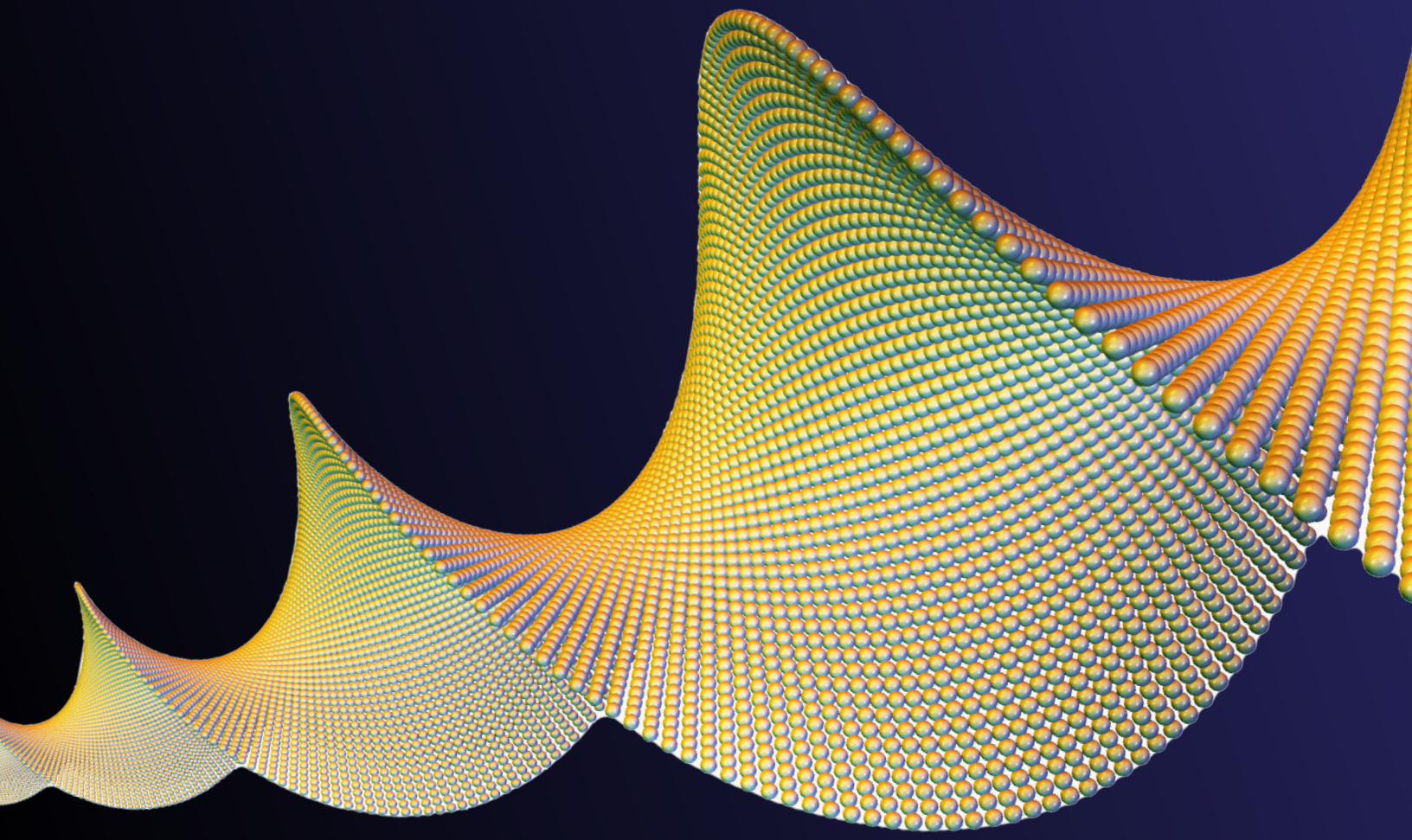
RICOH

THE AI DILEMMA

INFORMATION GOVERNANCE CONSIDERATIONS IN DEPLOYING GENERATIVE AI



ABSTRACT

The adoption of generative AI comes with unparalleled opportunities and risks. Establishing a robust Information Governance program before deployment is essential to ensure safety, compliance and optimal performance.

CONTENTS

INTRODUCTION

Most companies inevitably want to embrace AI and unlock the many advantages it presents. The challenge is figuring out how to incorporate AI into enterprise-wide processes — and still maintain the level of security they demand.

It requires businesses to build a strict Information Governance (IG) strategy and framework that will help them avoid significant risks: data inaccuracies, compliance violations, intellectual property leaks, and legal penalties.

At Ricoh, we leverage advanced AI technologies, robust Information Governance frameworks and strategic Advisory Services to help businesses thrive in the digital age. The result is enhanced workplace efficiency and innovation by integrating process automation technologies, intelligent capture, natural language processing and predictive maintenance.

This paper is designed to highlight the foundational role of IG in generative AI deployment and explore integration requirements, governance maturity and risk mitigation strategies to drive measurable value.

THE CURRENT LANDSCAPE OF INFORMATION GOVERNANCE AND AI

Managing the vast amount of data within organizations requires understanding what information you have, how it's used, where it's used, and how to protect it. For IG, AI and IT professionals, the landscape is complex, especially as new technology emerges. Organizations face the dilemma of deploying AI without sufficient governance frameworks. Data integrity, compliance risks and privacy issues are exacerbated in environments without governance programs. Here are some interesting findings that are driving decisions for many organizations.

The potential for generative AI is huge.

$25B

The generative AI market surpassed $25 billion in 2024.[1]

41.52%

The annual growth rate (CAGR 2025-2030) in market size, resulting in a market volume of $365B by 2030.[2]

321

The number of real-world generative AI use cases from the world's leading organizations.[3]

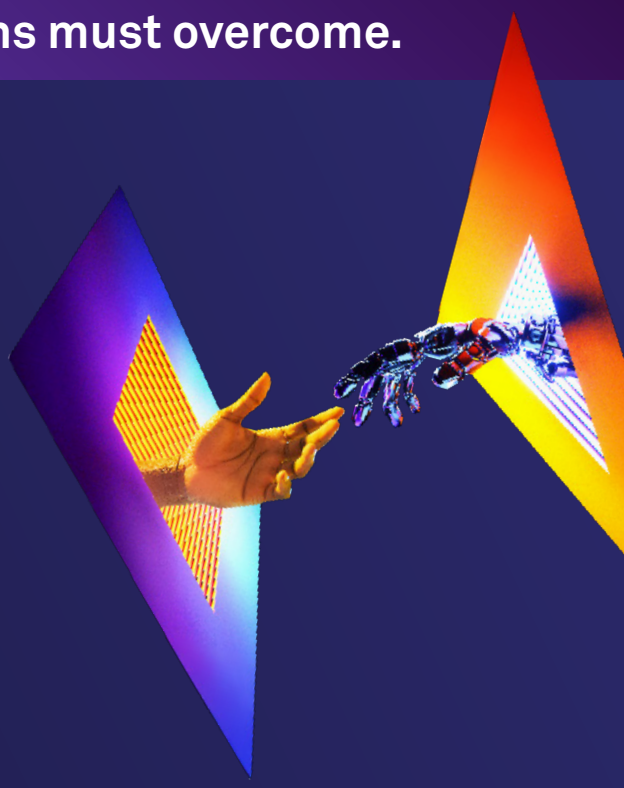
But there are data challenges organizations must overcome.

55%

Of CXOs' say their main issue with generative AI is inaccuracy.[4]

50%

Of Chief Data and Analytics Officers feel they are unable to drive innovation using data.[5]



70%

Of organizations report difficulties in developing processes for data governance and integrating data into AI models quickly.[6]

2/3

Of companies say 30% or fewer of their Gen AI proof of concepts will be implemented.[7]

So, the need for information governance becomes increasingly important.

62%

Starting before 62%, this section should be: So, the need for information governance becomes increasingly important. [8]

71%

Of organizations report they have a data governance program, compared to 60% in 2023.[9]

≤50%

Of organizations have mature, consistently enforced data retention policies, and for critical platforms like social media and video conferencing, retention policies drop to 30-44%.[10]

58%

Of top reported benefits of data governance programs include improved quality of data analytics and insights (58%), improved data quality (58%) and increased collaboration (57%).[11]

90%

Generative AI has opened up unstructured data, which has previously been inaccessible (e.g. videos, pictures, chats, emails, and product reviews).[12]

400%

"By 2027, GenAI will facilitate an increased use of other AI technologies (aside from GenAI) by 400%."[13]

RISKS WITHOUT INFORMATION GOVERNANCE

Deploying generative AI without a mature Information Governance framework poses significant risks and can lead to challenges such as data inconsistency, IP violations, inaccurate outputs and regulatory penalties. Proper governance ensures data readiness and mitigates risks in AI-driven workflows. The following key risks highlight the need for robust IG:

- **Data integrity and quality:** Poor data structures and lack of governance cause generative AI systems to produce flawed or misleading outputs, undermining business credibility. Data must be governed across its lifecycle to ensure accuracy.
- **Regulatory non-compliance:** Failure to comply with regulations like GDPR, HIPAA or emerging AI laws (e.g., EU AI Act) creates legal vulnerabilities and exposes organizations to penalties.
- **Bias and discrimination:** AI systems perpetuate societal harm, such as bias and discrimination, when training data lacks fairness, proper governance and validation processes.
- **Intellectual property (IP) risks:** Without IG processes for content verification and ownership validation, AI-generated outputs may unknowingly violate third-party copyrights or IP rights.
- **Cybersecurity threats:** Unstructured, legacy systems and poorly secured data increase exposure to breaches. The most pressing risks associated with AI usage are security vulnerabilities (86%), surveillance (83%), and privacy issues (83%). A quarter of organizations have experienced an increase in incidents (e.g., data breaches) related to AI in the past financial year, despite two in five organizations lacking a reporting mechanism for queries or incidents related to AI use in the workplace.[14]
- **Data inaccuracy:** According to the 2025 Outlook: Data Integrity Trends and Insights, 67% of organizations lack confidence in the quality and governance of their data to support advanced AI applications.[15]

Robust IG policies and frameworks are essential to mitigate these risks, ensuring that generative AI delivers trusted, accurate and compliant results while safeguarding organizations from operational, legal and reputational damage.

CREATING A ROBUST INFORMATION GOVERNANCE PROGRAM

A well-structured IG program aligns people, processes and technology to govern AI — and the data it uses — effectively, serving as the foundation for successful AI deployment. IG balances cost, risk and value, ensuring transparent data handling and compliance across the organization.

Framework and collaboration

IG is a cross-functional initiative that requires collaboration between IT, legal, risk, compliance, and data science teams. Establishing clear roles and accountability, such as trained AI Governance professionals, ensures oversight, risk mitigation and consistent governance practices.

Key Information Governance components

A robust IG program involves policies, standards and automated processes to manage the data lifecycle, improving data quality, accuracy and security — all critical for generative AI tools. KPMG highlights that organizations implementing IG frameworks can improve data reliability by reducing risks in AI workflows.[16]

Key IG components include:

- **Data retention and disposal policies:** Automate retention and disposition processes to eliminate redundant, obsolete and trivial (ROT) data, reducing storage costs and minimizing risks.
- **Metadata standards and management:** Standardize data classification and tagging to enhance searchability, support compliance and optimize AI model training.
- **Access control and audit trails:** Implement role-based permissions and detailed audit trails to safeguard sensitive data and ensure accountability and compliance.

By establishing these foundational elements — policies, roles and systems — organizations can ensure their data is well-governed, reliable and secure. This enables generative AI to operate effectively, drive value and maintain compliance with regulatory requirements.

INTEGRATION REQUIREMENTS: ERP, CRM AND ECM PLATFORMS

The success of generative AI depends on seamless integration with core enterprise systems such as ERP, CRM and Enterprise Content Management (ECM) platforms. Effective integration enhances decision-making, ensures data consistency and drives value-based outcomes across the organization.

- **ERP systems:** AI integration improves operational efficiency by optimizing financial forecasting and inventory management processes, enabling faster, data-driven decisions.
- **CRM systems:** Generative AI enhances customer engagement and personalization by analyzing unified governed data, ensuring accurate insights that strengthen relationships and outcomes.
- **ECM platforms:** Governed content ensures AI produces accurate, compliant and high-quality external communications while safeguarding against data misuse or inaccuracies.

The value of seamless integration

Interoperability — the ability of applications to exchange and make use of information — is critical to developing a strong IG framework and driving operational efficiency. Integrating your systems and data can increase successful outcomes with generative AI tools, improving productivity, compliance and trust. If your data isn't ready for generative AI, your business isn't ready for generative AI — and the ability to connect your data is essential for readiness.

> In fact, it seems possible that within the next three years, anything not connected to AI will be considered obsolete or ineffective.[17]

- **Data accuracy and flow:** Applications that track and maintain data lineage are important to validating accuracy and trust in AI outputs. Interoperability between systems is necessary to achieve this, according to the AI Governance Professional's "AIGP Body of Knowledge."[18] Connected data also improves accuracy by reducing manual data duplication and errors.
- **Decision-making efficiency:** When data is connected, there is more transparency, enabling insights and collaboration — therefore, increasing the speed of decision-making.
- **Productivity gains:** Adobe research reveals that disjointed systems cause 47% of data retrieval and sharing inefficiency. Integrating AI tools with ERP, CRM and ECM platforms eliminates silos, enabling seamless, consistent and governed data sharing.[19]

INFORMATION GOVERNANCE MATURITY MODEL

The Information Governance Maturity Model, as defined in ARMA's Information Governance Book of Knowledge and the AIGP Book of Knowledge, provides a structured roadmap for organizations to assess and improve their governance capabilities to support AI deployment effectively. The model outlines four levels of maturity:

1. **Deficient:** No formal policies or processes; ad-hoc, inconsistent approaches
2. **Basic:** Policies exist but are applied manually with inconsistent enforcement, including limited retention practices
3. **Managed:** Standardized policies and governance frameworks are consistently enforced across platforms with partial automation
4. **Transformational:** Enterprise-wide IG maturity featuring automated workflows, enterprise search tools and AI integration, ensuring seamless governance and optimized data use[20]

The path to transformational maturity

To progress toward transformational maturity, organizations must:

- **Conduct IG assessments:** Evaluate the current state of governance maturity to identify gaps and opportunities.
- **Establish IG leadership roles:** Designate IG professionals and AI governance leaders to drive strategy and accountability.
- **Integrate AI governance policies:** Standardize retention, access control and compliance processes across systems to support AI initiatives.

Despite the rapid adoption of AI, nearly 80% of companies are still trying to digitally transform. However, 90% of those companies face severe success obstacles with their transformation.

This gap underscores the need for organizations to prioritize IG improvements as a foundation for successful AI deployment.[21] Therefore, organizations are having trouble scaling AI when they have not achieved transformational maturity. In an ARMA report, they discovered that only 66.4% of organizations have only basic capabilities for managing and retrieving data, while only 3.3% of organizations have achieved transformational maturity, incorporating centralized systems and automation. This indicates that there is still a long way to go to achieve transformational maturity.

By leveraging IG maturity frameworks and advancing toward transformational levels, organizations can enable AI systems to operate with trust, accuracy, and efficiency, mitigating risks while achieving measurable business outcomes.

ESSENTIAL INFORMATION GOVERNANCE POLICIES FOR AI DEPLOYMENT

There are four essential IG policies that should be addressed for any AI development initiatives.

1. **Automated data retention and disposal**
   - Supports compliance with data lifecycle regulations like GDPR and HIPAA by automating the retention and disposition of redundant, obsolete and trivial (ROT) data
   - Ensures data is governed throughout its lifecycle, reducing legal risks and storage costs
2. **Standardized metadata management**
   - Enhances searchability, classification and organization of data, improving AI accuracy and facilitating compliance
   - Proper metadata structures streamline AI model training by ensuring data consistency and accessibility
3. **Access controls and permissions**
   - Implement role-based access controls to limit unauthorized AI access and safeguard sensitive data
   - Supports compliance and ensures that only authorized individuals can interact with critical datasets and AI tools
4. **Algorithmic Impact Assessments (AIAs)**
   - Conduct regular assessments to identify AI risks, ensure transparency and validate output for fairness, accuracy and safety
   - Promotes accountability in AI governance and mitigates biases or unintended consequences

The value of process automation

Automating IG workflows drives both efficiency and cost savings. A recent research report found that "Automating enterprise workflows could unlock $4 trillion/year in productivity gains."[22] Organizations achieve significant cost savings through automated data retention, access management and work-flow integration. Process automation eliminates time-consuming manual data entry and duplication of effort, often prone to costly errors.

By implementing these key IG policies — automated retention, metadata management, access control, and algorithmic assessments — organizations can govern AI systems effectively, ensuring compliance, safety, and optimal performance while reducing operational risks.[23]

TECHNOLOGICAL FRAMEWORK FOR SAFE AND EFFECTIVE GENERATIVE AI

In a recent report by IDC,[24] analysts recommend the following steps to increase the likelihood of successful generative AI usage:

- **"Organize for effective AI governance.** IT, business leaders, and AI leadership must work very closely together to align business processes with the technology. Roles like business architect and an AI governing function are becoming necessary for successful deployments beyond pilots and POCs.
- **Develop AI knowledge and skills.** Ensuring proper training of employees in this new and rapidly evolving age of AI is critical in areas such as data model building, use case development, AI composing, and prompt engineering. Having a trusted, unified data set and infrastructure; trusted policies and KPIs; and governance tools for ensuring compliance with AI use are all part of the supporting fabric for effective and responsible AI use. The AI organization or COE in concert with service providers can build and improve this approach over time.
- **Deploy AI to complement your broader digital transformation efforts,** complementing investments in tech such as cloud, analytics, and no-code/low-code applications development tools for a collective digital-first approach. Beyond the technology, AI is a business strategy that impacts business, operating, and organizational models.
- **Scale your GenAI applications in support of a targeted set of use cases** across your organization, considering each role and how GenAI can completely automate tasks or augment decision-making.
- **Begin experimentation with autonomous agents.** Start a journey to explore, test, and implement AI agents within business processes and workflows, so you're ready as the technology matures to enable autonomous agents.
- **Extend the use of AI to support your ecosystem projects and joint ventures;** leverage application marketplaces and model gardens for a shared approach to AI/ML, GenAI, and agentic AI with partners."

Deploying generative AI requires technologies such as centralized ECM platforms, enterprise search tools and automated retention systems to manage and govern data effectively.

BALANCING COMPLIANCE, PRIVACY AND INTELLECTUAL PROPERTY RISKS

Deploying generative AI requires rigorous IG to address legal, regulatory and ethical challenges. Organizations must strike a balance between innovation and adherence to compliance frameworks to mitigate risks and ensure trustworthy AI outcomes.

Considerations for legal and ethical AI deployment

1. **Data privacy regulations**
    - Compliance with privacy laws, such as GDPR, HIPAA and CCPA, mandates automated data anonymization and access controls to safeguard sensitive information

- Proper privacy measures ensure AI systems do not compromise individual rights or expose organizations to regulatory penalties

2. **Intellectual Property (IP) compliance**
   - Implement content verification processes to prevent AI from producing outputs that infringe on third-party IP rights
   - Ensuring clear ownership validation protects organizations from legal disputes and reputational risks
3. **Compliance monitoring**
   - Integrate AI risk management tools to enable ongoing alignment with emerging AI regulations (e.g., the EU AI Act). Regular compliance monitoring validates AI outputs against legal and ethical standards.
   - By addressing key legal and ethical challenges — privacy compliance, IP protection, and regulatory monitoring — organizations can deploy AI responsibly, minimizing risks while driving innovation.

CASE STUDIES: ORGANIZATIONS ADDRESSING IG BEFORE AI DEPLOYMENT

These case studies highlight organizations that successfully implemented IG programs before deploying generative AI, showcasing tangible benefits like improved compliance, reduced risks and cost savings.

40%

Financial Services Firm: Implemented automated retention policies, reducing redundant data by 40% before deploying AI-powered analytics[25]

30 minutes

Credit Union: Implemented a content services platform to automate mortgage approvals with records management that improved the approval rate by 30 minutes per transaction[26]

15% ↓

Retail Enterprise: Integrated AI tools with ERP systems, improving inventory decisions and reducing operational costs by 15%[27]

Implementing IG frameworks isn't just about compliance — it's a productivity enabler and risk mitigator. Automation, enterprise search tools and standardized metadata aren't "nice-to-haves" anymore; they are essential for maintaining efficiency and mitigating legal or cybersecurity risks.

Organizations prioritizing IG will reclaim countless employee hours and build more resilient, agile systems. Generative AI systems present revolutionary growth opportunities across industries, from automating workflows to enhancing decision-making processes. This isn't just future-proofing — it's ensuring survival in a data-driven economy.

GENERATIVE AI WORKSHEET: MICROSOFT COPILOT

Adopting a multifaceted approach combining technology, policy, and training is critical to mitigating the risks associated with deploying generative AI. By implementing the above strategies, organizations can leverage generative AI's benefits while safeguarding sensitive data and maintaining compliance with ethical and regulatory standards. The grid below will help organizations navigate challenges when using Microsoft Copilot.

Activity	Risk	Remediation
Data Privacy Breaches	Copilot processes prompts and may temporarily store them to improve the service, monitor abuse, or troubleshoot.	• Avoid inputting personal-sensitive or privileged information into Copilot. • Configure data handling settings to comply with data protection laws (e.g., GDPR, HIPAA). • Request data exclusions for your organization to prevent Microsoft from retaining inputs for model refinement. • Implement data anonymization techniques where applicable.
Unauthorized Access	Improper user permissions or unauthorized access to Copilot could lead to sensitive data exposure.	• Enforce role-based access controls (RBAC) to restrict access to Copilot functions based on user roles. • Use multi-factor authentication (MFA) for all users. • Regularly audit user access and permissions. • Implement conditional access policies to restrict access based on location, device, or other risk factors.
Data Leakage	Copilot outputs could unintentionally reveal confidential information by combining previously stored data.	• Educate users to avoid reusing Copilot across unrelated matters or cases to prevent cross-contamination of information. • Enable Microsoft Purview Information Protection to classify and label sensitive content, ensuring proper handling of classified data. • Monitor logs for unusual data usage patterns.
Compliance Risks	Using Copilot could lead to inadvertent breaches of client confidentiality agreements, regulatory obligations, or ethical guidelines.	• Consult legal and compliance teams before deploying Copilot to align usage with professional and regulatory obligations. • Maintain up-to-date records of data processing agreements with Microsoft. • Deploy tools to monitor and ensure regulatory compliance.
System Vulnerabilities	Copilot integration might expose vulnerabilities in the Microsoft 365 environment or third-party add-ons.	• Apply security updates and patches to Microsoft 365 and related applications regularly. • Conduct penetration testing to identify and mitigate vulnerabilities. • Enable Microsoft Defender for Office 365 to enhance email and data protection.

Activity	Risk	Remediation
Insider Threats	Employees with malicious intent or those who misuse Copilot could expose sensitive information.	• Implement strict usage policies and track Copilot interactions via activity logs. • Conduct regular security awareness training to educate employees about acceptable Copilot usage. • Use Microsoft Sentinel to monitor for anomalous behaviors indicative of insider threats.
Integration Risks	Copilot might interact with third-party tools, increasing the risk of data interception during transmission or storage.	• Use encryption protocols like TLS to secure data in transit. • Limit Copilot integrations to only trusted and necessary third-party tools. • Regularly review and update API permissions and configurations.
AI Model Bias and Hallucinations	AI models may generate biased or inaccurate outputs that could lead to erroneous legal advice or expose sensitive details.	• Require human review of all Copilot outputs before sharing them with clients or stakeholders. • Monitor for and report inaccuracies to Microsoft for model improvement. • Conduct internal testing to identify and mitigate potential biases.
Malware and Phishing Risks	Attackers could exploit Copilot's features to spread malware or phishing messages.	• Train employees to recognize and avoid phishing attempts. • Use Microsoft Defender and other endpoint protection tools to detect and mitigate malware threats. • Restrict macro-enabled documents and attachments unless from trusted sources.
Third-Party Vendor Risks	Dependence on Microsoft means sensitive data is stored and processed by a third party, raising risks of vendor-side breaches.	• Perform due diligence on Microsoft's security certifications and track record. • Include clear service level agreements (SLAs) in the vendor contract addressing data security responsibilities. • Regularly review vendor risk assessments and ensure compliance with industry standards like ISO 27001.
Backup and Recovery Risks	Copilot could inadvertently affect data integrity, making backups and recovery more complex.	• Establish regular backup schedules with immutable backups. • Use Microsoft's native backup tools and third-party backup solutions for redundancy. • Test disaster recovery procedures frequently to ensure data can be restored effectively.

NEXT STEPS

Ricoh's Information Governance Services ensures compliance, document and records management throughout their lifecycle, and data integrity and accessibility. Our Advisory Services offer expert guidance on workflow optimization, change management and data-driven decision-making. These elements empower organizations to streamline operations, secure data and achieve sustainable growth.

To deploy generative AI successfully, organizations must prioritize IG. Recommendations include establishing IG frameworks, integrating systems, ensuring compliance, and leveraging process automation and modern technologies for governance.

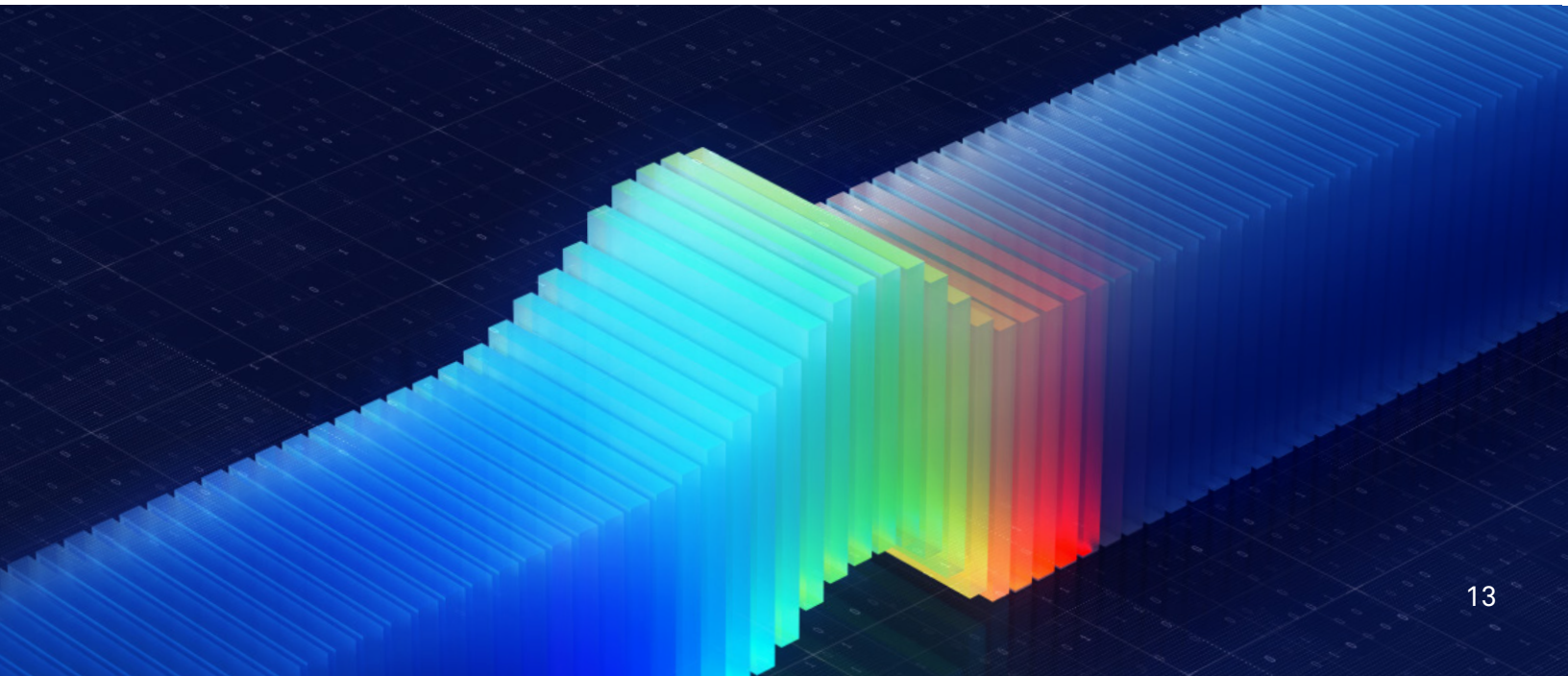
Implementing solid IG practices with a tailored program is the first step to AI success. The best place to begin is with a maturity assessment. The Ricoh Maturity Assessment is an Advisory Service designed to evaluate the maturity of an organization's information governance practices. This assessment helps identify gaps in compliance, opportunities for risk mitigation and areas for increased efficiency.

After taking the assessment, organizations will receive a snapshot of their current state and guidance on improving their information governance strategy.

Take the Information Governance Maturity Questionnaire here to review your maturity level.

RICOH, A TRUSTED PARTNER

Today, for over 1.4 million customers around the world, Ricoh is unleashing the power of information to create better workplace experiences, streamline and connect workflows through process automation, and drive operational efficiency. Let's work together to discover how we can put information to work for you.



Endnotes

[1] IoT Analytics. “The leading generative AI companies.” March 4, 2025.
[2] Statista. “Generative AI – Worldwide.” March 2024.
[3] Google. “321 real-world gen AI use cases from the world’s leading organizations.” December 19, 2024.
[4] McKinsey & Company. “Gen AI in corporate functions: Looking beyond efficiency gains.” October 23, 2024.
[5,6] McKinsey & Company. “Charting a path to the data- and AI-driven enterprise of 2030.” September 5, 2024.
[7] Deloitte. “Deloitte’s State of Generative AI in the Enterprise.” January 2025.
[8,9] Precisely. “2025 Planning Insights: Data Governance Adoption Has Risen Dramatically.” December 9, 2024.
[10] Pagefreezer. “2024 ESI Risk Management & Litigation Readiness Report.” 2024.
[11] Precisely. “2025 Planning Insights: Data Governance Adoption Has Risen Dramatically.” December 9, 2024.
[12] McKinsey & Company. “Charting a path to the data- and AI-driven enterprise of 2030.” September 5, 2024.
[13] Gartner®. “Innovation Guide for Generative AI Technologies.” 10 February 2025 - ID G00793932. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
[14] Deloitte. “AI at a crossroads.” December 2, 2024.
[15] Precisely. “New Global Research Points to Lack of Data Quality and Governance as Major Obstacles to AI Readiness.” September 18, 2024.
[16] KPMG. “Responsible AI and the challenge of AI risk.” 2023.
[17] McKinsey & Company. “Beyond the hype: Capturing the potential of AI and gen AI in tech, media, and telecom.” February 2024.
[18] iappai governance center. “The AIGP Body of Knowledge (BOK).” June 20, 2023.
[19] Adobe. “How digital organization impacts employees and the workplace.” September 29, 2023.
[20] ARMA International. “The Information Governance Body of Knowledge.” 2024.
[21] CxO. “The State of Digital Transformation 2025: What CxOs Need to Know.” February 3, 2025.
[22] Consensus. “Automating the Enterprise with Foundation Models.” May 2, 2024.
[23] Consensus. “Role of document management system for business processes optimization.” September 15, 2024.
[24] IDC. “IDC MaturityScape: AI-Fueled Organization 1.0.” IDC #US53209724. 2025.
[25] Digitaldefynd. “20 AI in Finance Case Studies [2025].” 2025.
[26] Ricoh. “Case Study: Salmon Arm Savings and Credit Union.” 2024.
[27] ThroughPut Inc. “How AI-powered Retail Logistics Optimization Saved € 3.5 Million Per Year for a European Enterprise.” September 20, 2024.

Resources

- Department of Defense: DoD MANUAL 8180.01. INFORMATION TECHNOLOGY PLANNING FOR ELECTRONIC RECORDS MANAGEMENT
- Joint Interoperability Test Command: DoD Instruction 5015.02. DoD RECORDS MANAGEMENT PROGRAM CRITERIA
- Microsoft Copilot Readiness Assessment
- RICOH Information Governance Consulting website and brochure
- Webinar: A Secure Journey Through AI-Driven Business Process Transformation
- Webinar: Calming the data storm: A primer for building a future-ready information management strategy

RICOH
imagine. change.

Ricoh USA, Inc., 300 Eagleview Blvd, Exton, PA 19341, 1-800-63-RICOH.