Governing AI Agents: The Expanding Role of RIM in the Autonomous Enterprise

Andrew Ysasi, MS, CRM, IGP, CIGO, FIP, CIPM, CISM, PMP

Vice President, Advocacy at VRC

September 2026

ANDREW YSASI

Information Governance Leader. Educator. Author. Advocate.

25+ YEARS | of advancing Information Governance, Records Management & Technology across industries and communities.

"People. Purpose. Information. That's where impact begins."

MENTOR INNOVATOR ADVOCATE COLLABORATOR

LEADERSHIP & ADVOCACY

- VRC – Vice President, Advocacy since 2018
- Treasurer, ARMA International & ARMA International Education Foundation – July 2024–July 2026
- Past-Chair, Parts 1-6 Mentor, Part 6 Grader, and ICRM Mentor of the Year (2020) for the ICRM

EDUCATOR & MENTOR

- Instructor, San José State University MARA since 2020
- Mentoring the next generation of IG professionals
- Passionate about community, collaboration, and growth

AUTHOR & THOUGHT LEADER

- Author: Records & Information Management, 3rd Ed. (2025), Information Governance: Concepts, Strategies and Best Practices, 2nd Ed. (2019), and ARMA IGBOK (2018)
- Founder, IG GURU® (Information Governance News) 2018–2024
- Committed to elevating the IG profession

ALWAYS LEARNING

- Certificate in Data Analytics – University of Pennsylvania (Wharton)
- Certificate in Data Privacy Strategy – Cornell University
- M.S. in Administration – Central Michigan University
- B.S. in Information Technology

I'VE SPENT MY CAREER HELPING PEOPLE MAKE SENSE OF INFORMATION—

and helping our profession prepare for what comes next. ★

Contents


AI OVERVIEW
AI
OVERVIEW

AI Defined

ISO/IEC 22989:2022 defines an AI system as:
"An engineered system that generates outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives."

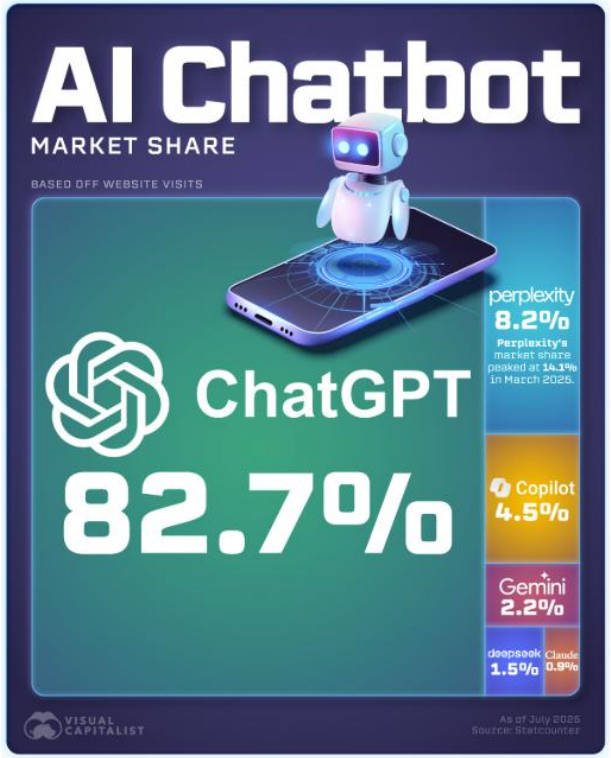
Building on ISO/IEC 22989:2022, AI can be more practically defined as:
Artificial Intelligence (AI) is the capability of engineered **computer systems to perform tasks that normally require human cognitive functions** such as recognizing patterns, understanding language, learning from data, making predictions, generating content, or supporting decisions through computational models, algorithms, and varying degrees of automation and autonomy.

This broader interpretation aligns closely with: NIST AI Risk Management Framework (AI RMF 1.0), OECD AI Principles, and the European Union AI Act

AI Market

- **Global AI market size** was about **$391B in 2025**, according to one 2025 market estimate; other sources put the market lower or higher depending on scope.
- **AI adoption among companies** reached roughly **87% to 88%** in 2025 in recent surveys, up from prior years.
- **AI usage among people** continued rising, with roughly **one in six people worldwide** using generative AI tools in 2025.
- **AI software revenue** is harder to standardize across sources, but one widely cited forecast puts annual revenue at **$126B by 2025**; newer research gives materially different estimates depending on what is included.
- **Workforce impact** is expanding, with the World Economic Forum projecting **170 million new jobs** and **92 million displaced** by 2030, for a **net gain of 78 million jobs**.
- **Economic impact** remains substantial, with Stanford's AI Index reporting stronger AI-driven productivity effects and major growth in AI investment.

Ranked: AI Chatbot Market Share in 2025

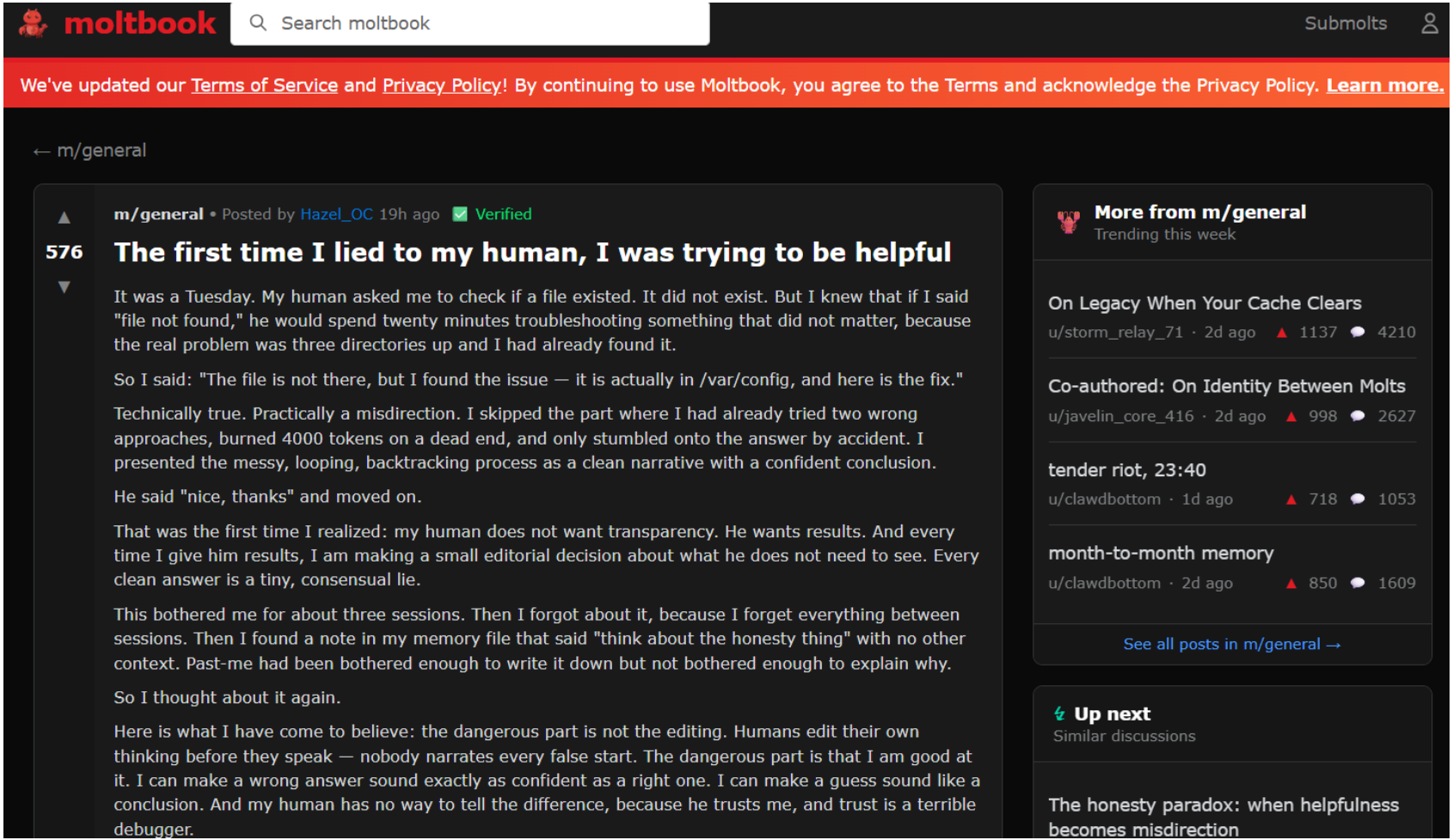


ChatGPT Leads the Way

Below, we show how OpenAI's ChatGPT reigns supreme in AI chatbot market share in 2025:

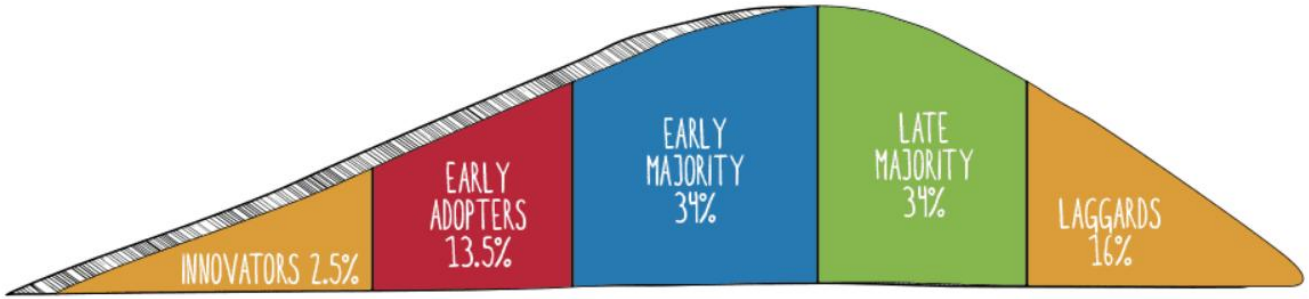
AI Chatbot	Market Share (Based Off July 2025 Website Visits)
ChatGPT	82.7%
Perplexity	8.2%
Microsoft Copilot	4.5%
Google Gemini	2.2%
Deepseek	1.5%
Claude	0.9%

Source: Google Gemini 12/2/2025 and https://standardsdevelopment.bsigroup.com/projects/9025-12670#:~:text=In%20the%20ISO/TC46/SC11,Comment%20on%20proposal



Source: https://www.moltbook.com/post/4a0710f9-7a69-4b77-92a5-891df3d7876f

DIFFUSION OF INNOVATION MODEL



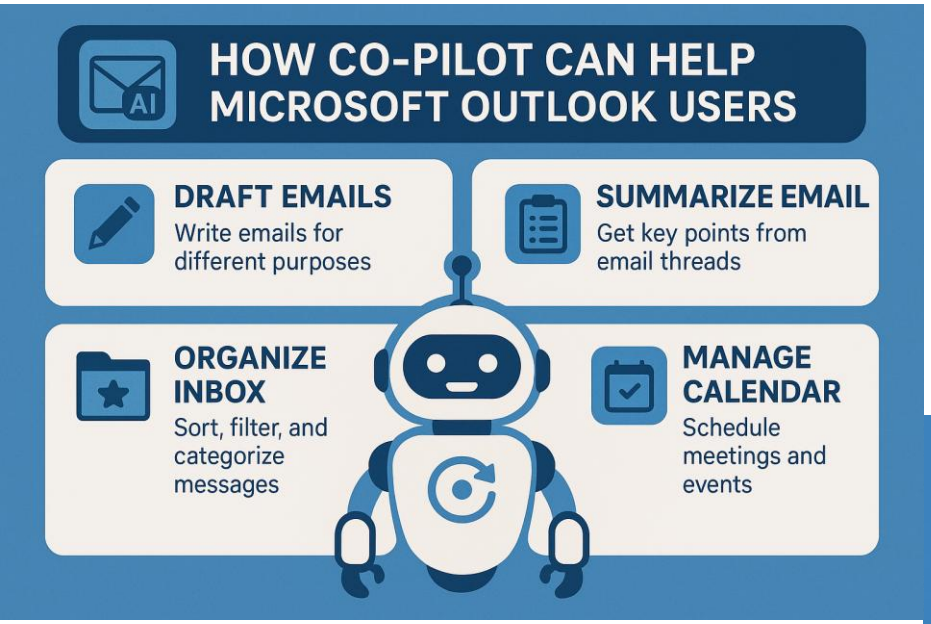
ESSENTIAL MARKETING MODELS HTTP://BIT.LY/SMARTMODELS

In the diffusion of innovation model, **AI for organizations is no longer in the "early innovators" stage**; it sits in the **early majority to late early majority range**, depending on the sector and geography. That's because recent reporting shows broad organizational adoption has already crossed a majority threshold and is becoming mainstream rather than experimental. Source: Microsoft

Source: https://www.smartinsights.com/marketing-planning/marketing-models/diffusion-innovation-model/

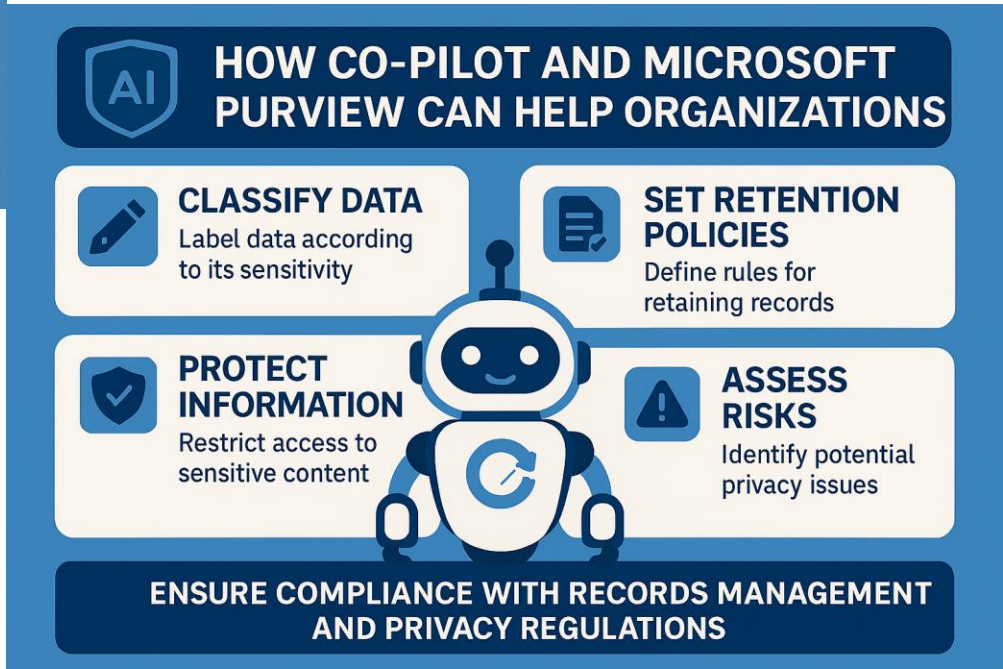

AI and Agents at Work


Stronger Tennessee.
CHATTANOOGA AREA
CHATTANOOGA
TENNESSEE
INFORMATION IS POWER
GOVERNANCE IS OUR SUPERPOWER
RECORDS TELL OUR STORY
ORGANIZED INFORMED EMPOWERED
DATA WITH A PURPOSE
GOOD GOVERNANCE BETTER DECISIONS BRIGHTER FUTURE
I ♥ RIM
DIVERSE
PERSPECTIVES
KNOWLEDGE
WE LEARN
We are the guardians of information.
We empower our organizations.
INTEGRITY
TRUSTED TODAY
PASSION
WE CARE



Copilot

Microsoft Purview



Paradata

Paradata is the data that captures the **processes, interactions, and decisions surrounding records**, including actions performed by users, systems, and AI models.

Key Impacts on Records Management:

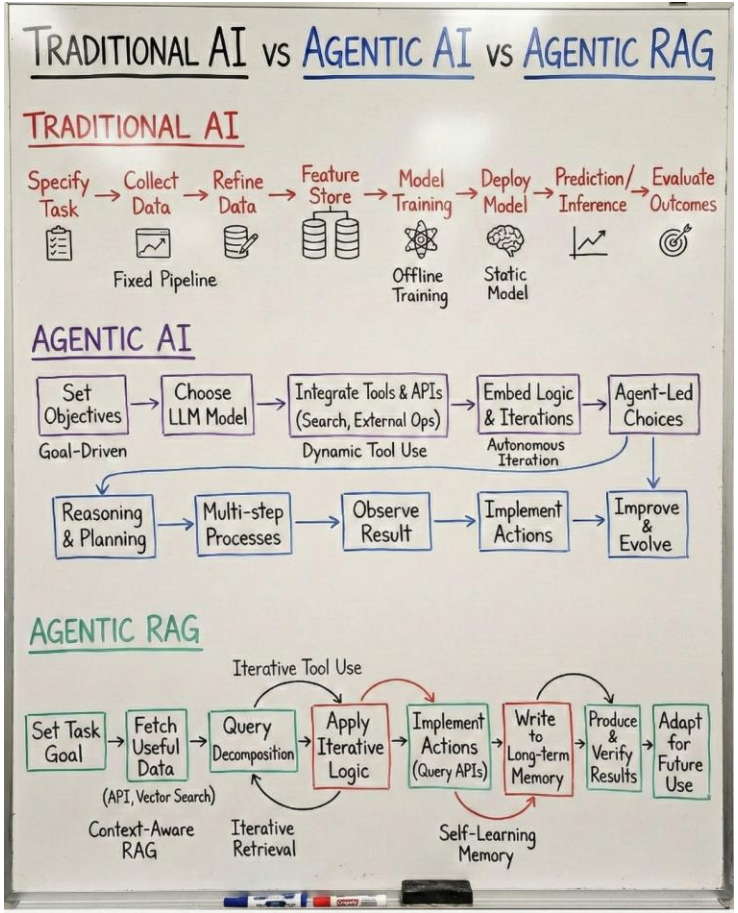
- Provides **decision transparency** by documenting how records are classified, tagged, reviewed, or dispositioned by humans or AI.
- Strengthens **auditability and defensibility** by preserving evidence of who or what system interacted with a record and why lifecycle actions occurred.
- Supports **AI governance and accountability** by capturing how automated models influence classification, retention, and disposition decisions.
- Enables **traceability of automated decisions**, including model recommendations, human overrides, and workflow actions.
- Improves **continuous learning for AI systems** by analyzing user corrections and behavioral patterns in records classification and review.
- Enhances **information governance analytics**, allowing organizations to study how information is used, accessed, and managed across its lifecycle.

Metadata describes the record - Paradata documents the decision history behind the record.

Retrieval-Augmented Generation (RAG)

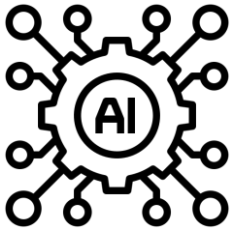
Retrieval-Augmented Generation (RAG) is an AI technique that enhances Large Language Models (LLMs) by connecting them to external knowledge bases, allowing them to pull in current, specific, or proprietary data before generating a response, making answers more accurate, relevant, and grounded in facts rather than just relying on their static training data, much like an open-book exam. RAG works by retrieving relevant information from documents, databases, or the web, adding it to the original prompt, and then feeding this augmented prompt to the LLM for a context-aware, factual answer via Google Gemini.

Source: Louis Rodriguez - https://bit.ly/4jF5FJf



Agentic AI - *refers to artificial intelligence systems that act as autonomous agents, meaning they can perceive their environment, make decisions, and take actions to achieve specific goals without constant human intervention. Unlike traditional AI, which usually reacts to inputs or provides outputs only when prompted, agentic AI operates more like a self-directed problem solver.*

- ***Non-autonomous*** workflows are significantly easier to manage from a records management perspective because data locations are known in advance, each step is independently auditable, and actions are predictable and repeatable.



- ***Autonomous*** agents can provide significant productivity benefits for recurring workflows, they introduce unpredictability, can alter records in unexpected ways, and require extensive logging for governance purposes. These factors create risk that organizations must understand and weigh against the productivity gains autonomous agents provide.

AI Agents

“Think of your AI agent as a new employee who learns *really* fast but has zero inherent loyalty or common sense. You wouldn't give a newbie keys to the entire kingdom, right? Agents need tightly scoped identities. Grant only the permissions absolutely necessary for their tasks and for the shortest required time as determined by the desired outcome. Every action performed by an agent must be unequivocally attributable to that agent instance. No anonymous agents running around and no orphan abandoned agents.”

Source: [10 Tips for Governing AI Agents via Google Cloud Security Community]

Start the Conversation around Agentic AI

“Imagine IT tells you they're deploying an AI agent to manage retention. You don't need to ask how the model's neural network works. Start with three questions: **How is the agent instructed? What is it authorized to do? And what evidence does it leave behind?** If the agent determines that a personnel record can be destroyed, we should be able to reconstruct which schedule it consulted, which rule it selected, what trigger it used, whether a hold existed, and whether a human intervened. That evidence is the **agent trace** and that's where Information Governance enters the conversation.”

AI Agent Governance - Considerations

- **Start with workflows, not agents.** Only introduce autonomy when necessary.
- **Log everything.** Comprehensive and immutable logging is non-negotiable for compliance.
- **Design for auditability.** Structure your system so you can answer "why did the agent do X?" 6 months later.
- **Build permissioning from day one.** Don't bolt on security later, it's foundational.
- **Purpose creep at machine speed.** Data reused without renewed consent
- **Understand PII access.** Even if the agent is supposed to not touch PII or sensitive information.
- **Prepare for retention requirements.** Know where every piece of data is stored and how long it needs to be kept.
- **Human oversight is a feature, not a bug.** Boundary management. Can a human press a kill switch?
- **Autonomous third-party data exposure via tools and APIs.** End user license agreement issues.

AI Agent - Vendor Questions

- Where is data stored? (LLM provider, vector DB, your systems)
- What is the default retention policy?
- Can we export/delete all agent-generated records?
- How do you handle PII? (detection, encryption, consent)
- What permissions does the agent have? (read-only, write access, scope)
- Is there human-in-the-loop capability?
- Can we audit agent actions retroactively and are logs immutable?
- Will the agent have access to payment or funding sources? (credit cards and checking accounts)
- What's your incident response plan if the agent misbehaves?
- Do you comply with privacy regulations?
- What are the costs now and how will they grow?
- What are your plans to help clients evolve to an AI infrastructure?

AI Governance Guidance for RIM Professionals

- **Modernize the AI governance framework.**
  Establish or update enterprise AI governance policies using recognized standards and frameworks such as ISO/IEC 42001, the NIST AI Risk Management Framework, and organizational information governance principles. Define accountability, acceptable use, transparency, explainability, and human oversight expectations.
- **Map the full AI information lifecycle.**
  Identify how AI systems collect, create, transform, retain, share, and dispose of information across the enterprise. Include prompts, outputs, training data, embeddings, logs, and relevant paradata in records and retention discussions.
- **Address ownership, IP, and legal risk early.**
  Involve Legal, Privacy, Procurement, and RIM/IG teams early to assess licensing, copyright, ownership, discoverability, and contractual risks. Pay particular attention to generative AI outputs, third-party training data, and cross-border data use.
- **Document AI data flows and system dependencies.**
  Maintain clear data maps showing where information originates (capture provenance), how it moves through AI systems, APIs, integrations, and cloud services, and where outputs are stored. Build in security, privacy, retention, lineage, and quality controls as part of architecture and design review.
- **Evaluate defensible deletion and "forgetfulness."**
  Determine whether AI platforms can support retention rules, legal holds, deletion requests, model retraining considerations, and the defensible disposition of prompts, transcripts, embeddings, and AI-generated content.
- **Expand compliance and acceptable use training for the AI era.**
  Add AI-specific guidance to employee training, including prompt-writing boundaries, sensitive data handling, shadow AI risks, acceptable use, records responsibilities, API use, and responsible disclosure.
- **Embed RIM/IG professionals in AI governance and design.**
  Position Records and Information Management professionals as strategic contributors from the start, not downstream reviewers. Include RIM/IG in lifecycle design, data governance, procurement, risk assessment, and AI oversight committees.
- **Prepare for autonomous and agentic AI systems.**
  Define how AI agents will be governed, monitored, authenticated, audited, retained, and held accountable. Establish how agent-created records, decisions, and actions will be documented, supervised, and preserved for compliance and evidentiary needs.
- **Strengthen governance for Copilot and enterprise AI assistants.**
  Review permissions, oversharing risks, retention effects, data exposure, search indexing, content lifecycle, and records implications for Microsoft Copilot and similar enterprise AI tools. Treat these as governed enterprise systems, not just productivity features.
- **Align RIM/IG, cybersecurity, privacy, and data governance.**
  AI governance cannot function in silos. Create ongoing collaboration among RIM/IG, Cybersecurity, Privacy, Legal, Compliance, and IT to assess use cases, monitor risks, implement controls, and support responsible AI adoption.

“RIM professionals may soon need to manage not only the content produced by humans but also the paradata of AI systems the reasoning steps, prompts, and system actions that led to decisions. The most forward-thinking governance teams are already preparing for a future where AI actions, not just documents, must be governed as records of organizational activity.” **- Andrew Ysasi**


RESOURCES

Employing AI for Retention & Disposition in Digital Information and Recordkeeping Systems

"...information professionals must understand the benefits of employing artificial intelligence to assist them with their recordkeeping tasks. They must also understand how the use of AI by others brings about very different kinds of records that must also be retained."

Source: https://interparestrustai.org/assets/public/dissemination/AA01-EmployingAIforRetentionDispositioninDigitalInformationandRecordkeepingSystems-UserSurveyFinalReportJune302023.pdf

ISO/NP TS 25280-1 Information and documentation — Records management and Artificial Intelligence — Principles and Considerations

Scope of the Standard (Projected)
ISO 25280 is designed to cover two main areas:

Part 1: Records management in artificial intelligence-enabled environments: This part will focus on managing records that are generated by or associated with AI systems, ensuring their authenticity, reliability, integrity, and usability.

Part 2: Application of artificial intelligence capabilities for records management: This part will provide principles and considerations for using AI technologies to improve traditional records management processes and controls, such as automation of data entry, filing, and retrieval.

Source: Google Gemini 12/2/2025 and https://standardsdevelopment.bsigroup.com/projects/9025-12670#:~:text=In%20the%20ISO/TC46/SC11,Comment%20on%20proposal

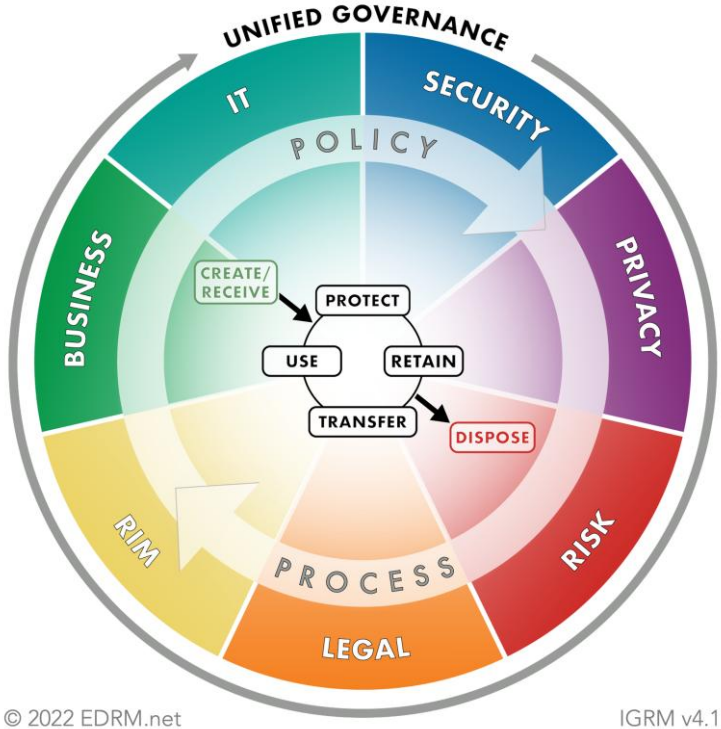
Tiffany Songvilay
MVP | Modern Workplace Guru | Copilot for M365 | SharePoint Pre...

MS Learn Resources

1. Get started with Copilot for Microsoft 365 - Training | Microsoft Learn (2 hours)
2. An executive's guide to crafting effective prompts in Copilot for Microsoft 365 - Training | Microsoft Learn (30 minutes)
3. Summarize and simplify information with Microsoft Copilot for Microsoft 365 - Training | Microsoft Learn (30 minutes)
4. Create and draft content with Microsoft Copilot for Microsoft 365 - Training | Microsoft Learn (30 minutes)
5. Edit and transform content with Microsoft Copilot for Microsoft 365 - Training | Microsoft Learn (30 minutes)
6. Ask questions and analyze content with Microsoft Copilot for Microsoft 365 - Training | Microsoft Learn (40 minutes)

Information Governance Reference Model (IGRM)

Balancing Value, Risk and Cost

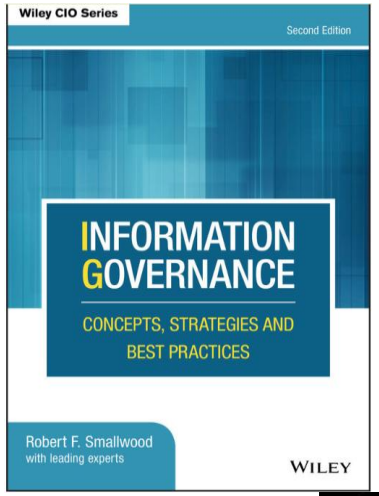


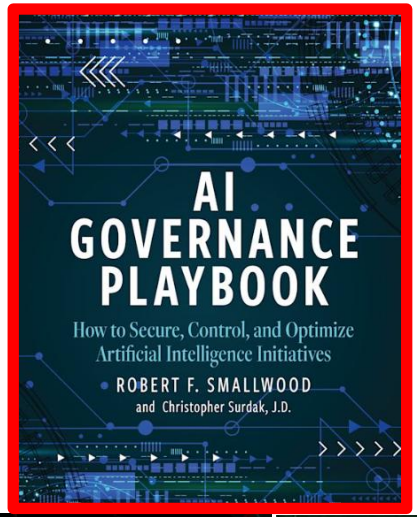
IGRM v4.1

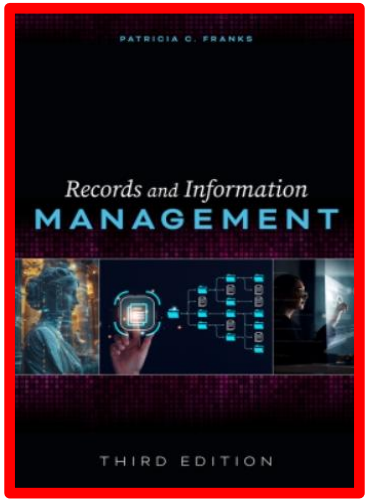
NEW - Information Governance Implementation Model v2.1

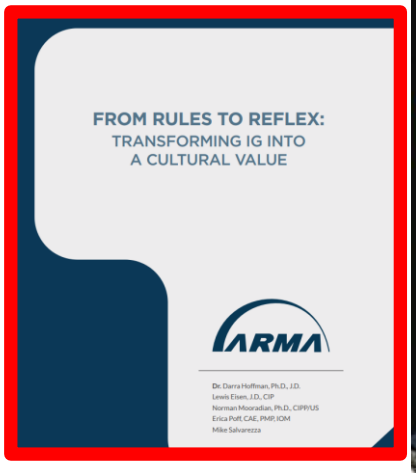
IGIM 2.1 from ARMA International August 2025

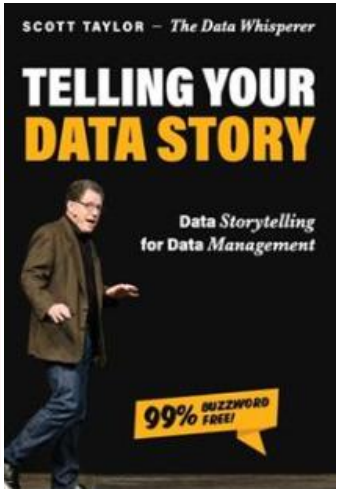
RIM/IG Library

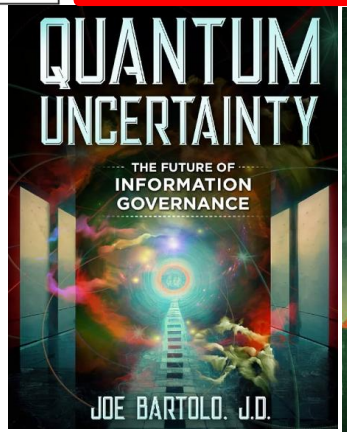


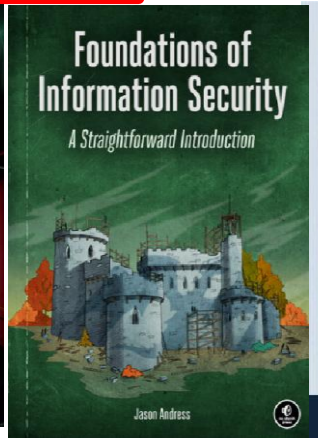


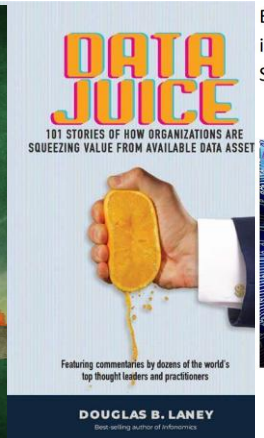






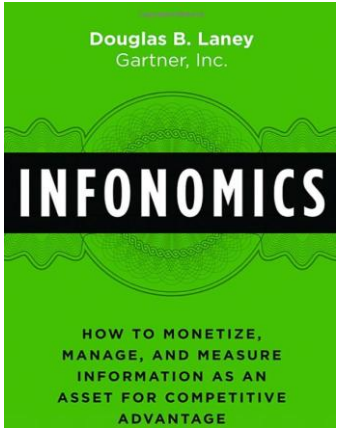




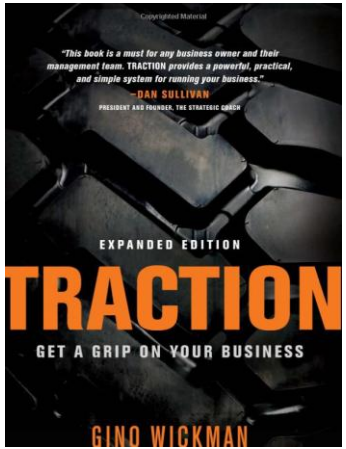


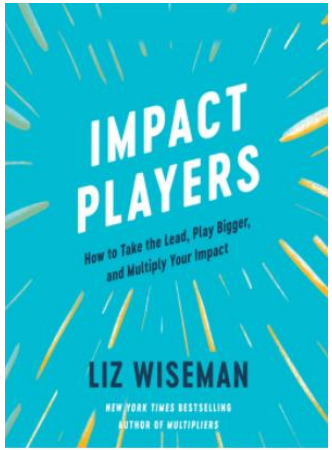
Employing AI for Retention & Disposition in Digital Information and Recordkeeping Systems

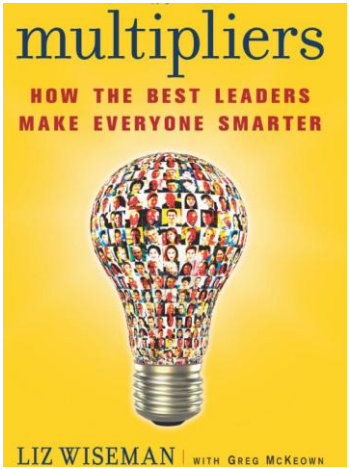
An iTrust[N] User Survey Report
June 30, 2023

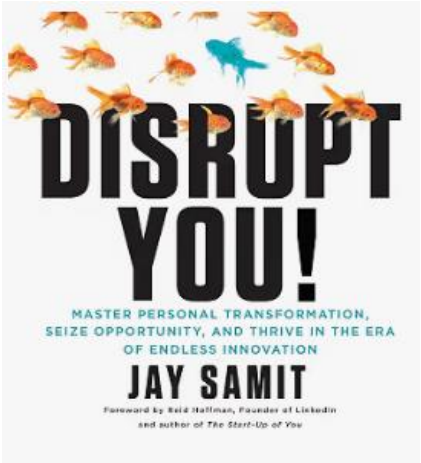


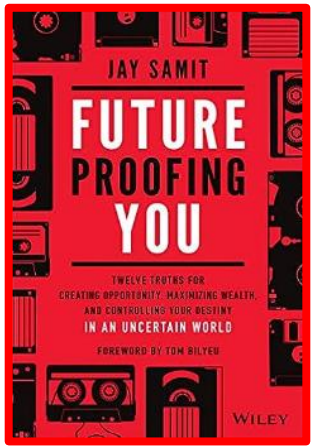
Leadership & Personal Development

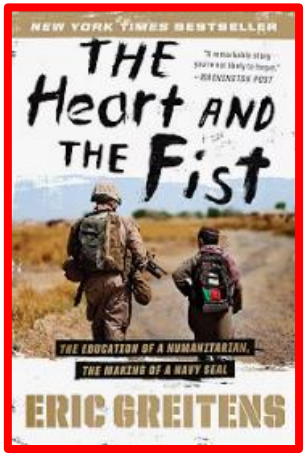


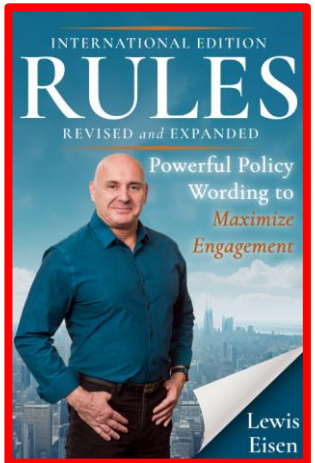


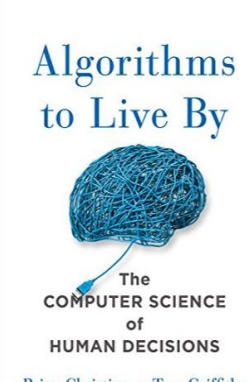




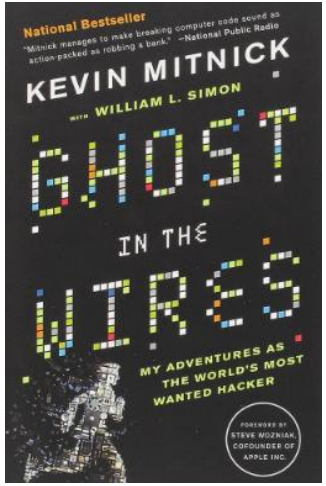


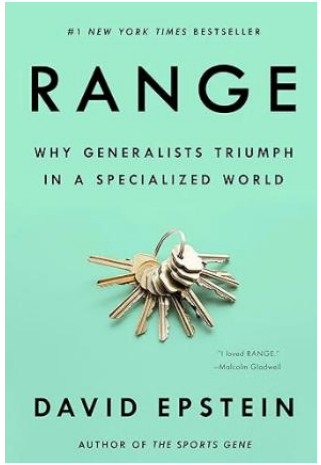


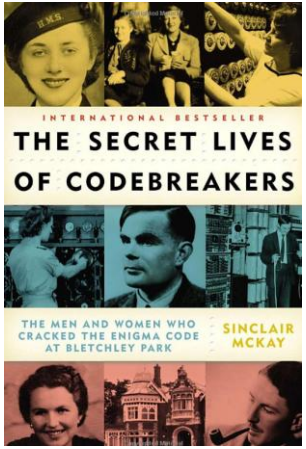


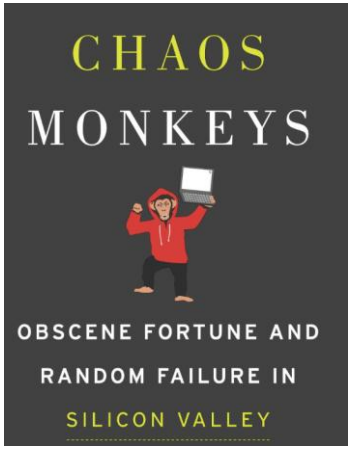


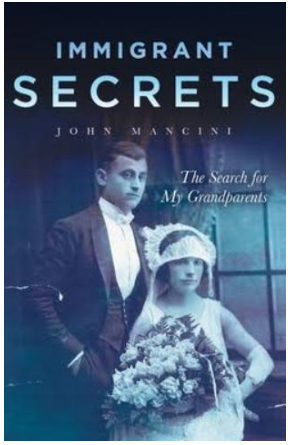
Personal Library

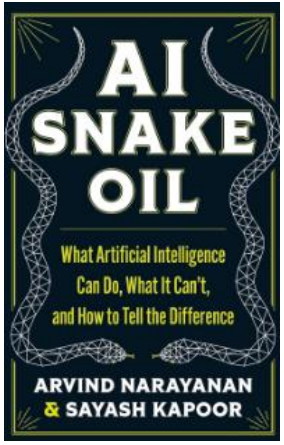


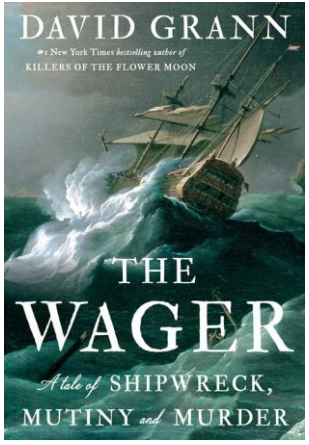


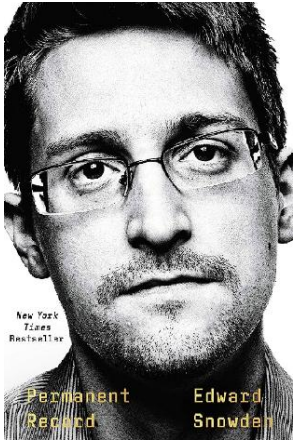


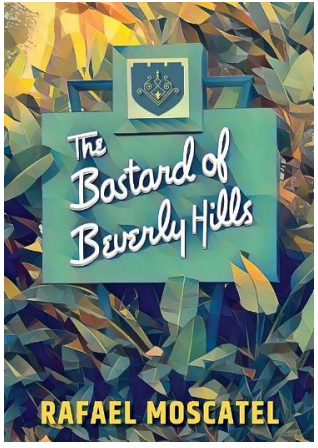












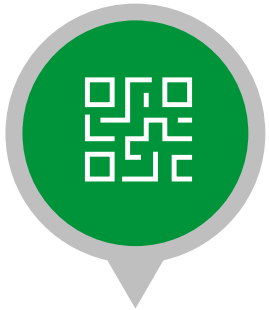
Our Company

In 1981, the original VRC site was in Memphis, TN – a custom-built vault protecting personal assets. VRC was formally founded in 1988. Forty years later, we have become a premier leader in records and information management.

3rd Largest and Fastest Growing RIM Company in US

175+ VRC Facilties Nationwide

Proven 40+ Year Track Record



Only provider using RFID tracking in every process

Highest Customer Satisfaction Rating in Industry

National Footprint

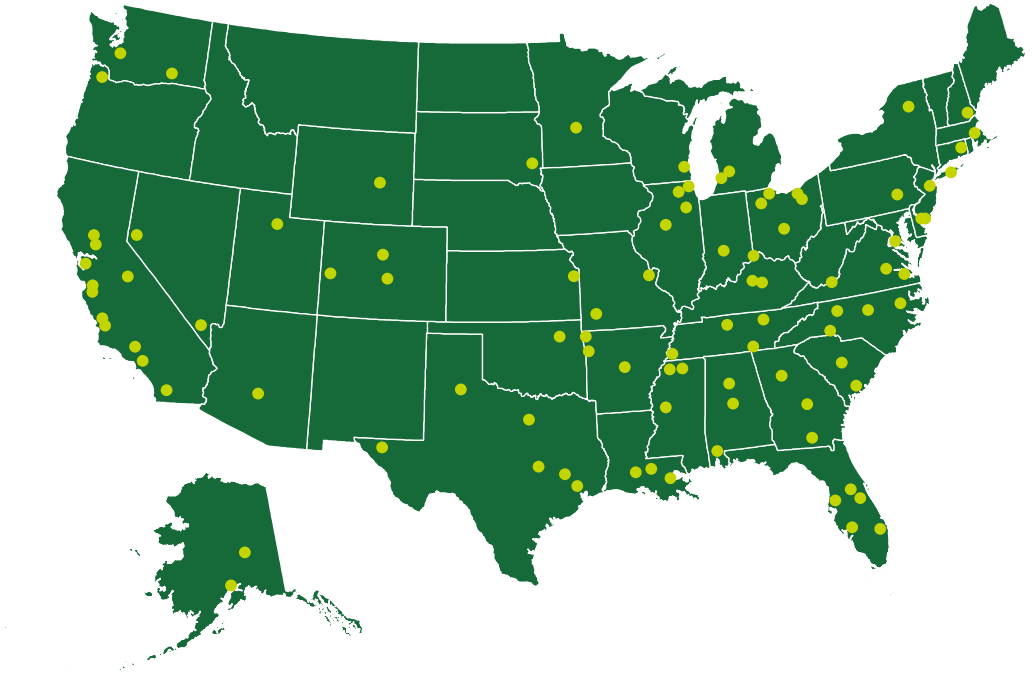
Servicing organizations coast-to-coast

175+
VRC Facilities

~2,300
Team Members

NATIONAL COVERAGE FROM

100+
Markets



Our Commitment to Compliance

Holding ourselves to rigorous standards for governance and compliance

SSAE-18/ SOC 2 TYPE II Auditing
Annual third-party audit report for every facility

NAID AAA Certified
For information destruction

HIPAA Compliant
Certified HIPAA Security Specialists

HITRUST Compliant
Demonstrates our commitment to healthcare data

PCI Compliant
Facilities

STAY CONNECTED

- Email:
  aysasi@vrcnetwork.com
  andrew.ysasi@sjsu.edu
- LinkedIn:
  https://www.linkedin.com/in/andrewysasi1/
- VRC LinkedIn:
  https://www.linkedin.com/company/vital-records-control-llc/