



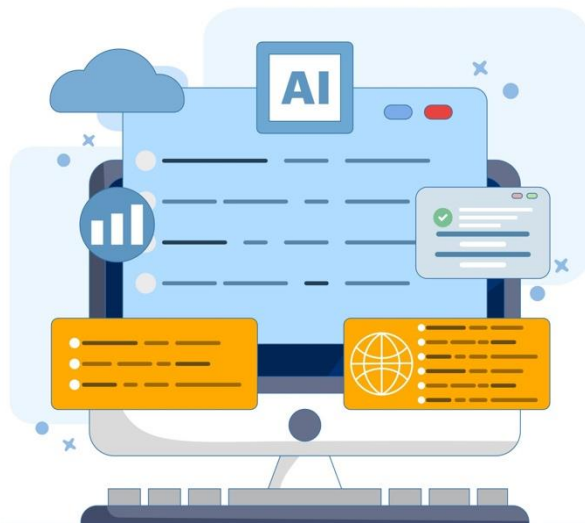
— WEBINAR SERIES —

Sandy Serkes
Co-Founder & CEO

Jennifer Nelson
VP Strategic Solutions

What Happens When the AI Model Collapses?

Serious Considerations for
Executing IG in an AI World



Webinar Series



www.ValoraTech.com



ROT Remediation:
File Share Clean-up
January 21



From Observational to
Operational Governance
July 23



Letting the Robots
Classify: Automating IG
February 18



Unhostaging Your Data:
Reclaiming Control
August 19



AutoClassifying the 3 Rs:
ROT, Records & Retention
March 18



Managing Data Privacy &
While Managing Records
September 23



Structured Data
Management & Disposition
April 15



What Happens When the
AI Model Collapses
October 21



10 Ways AutoClassification
Can Impact AI
May 13



AI Policy & Governance
with Lewis Eisen
November 18



How AC Transforms
Enterprise Search
June 17



AutoClassification &
AI Trends in Enterprise
December 16

About Valora



- AutoClassification platform for Information Governance
- Automates discovery, identification, classification & defensible disposition
- Trusted by IG teams, Records & IM teams, Legal, Compliance, IT teams
- Brings multiple enterprise repositories into a single view, and multiple IG use cases under one umbrella





Poll Results

Who's here today
& what are your interests?



Who you are & what your challenges are



Who You Are

Records / Information Management

Knowledge Management

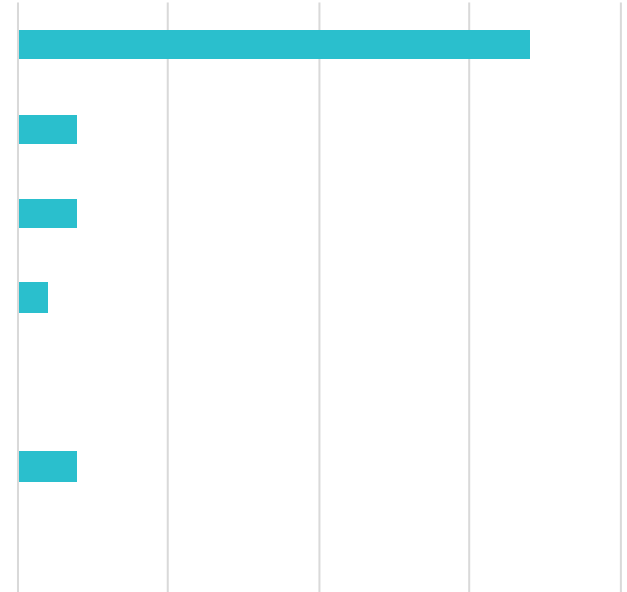
Legal

Compliance

IT

Data Privacy / Security

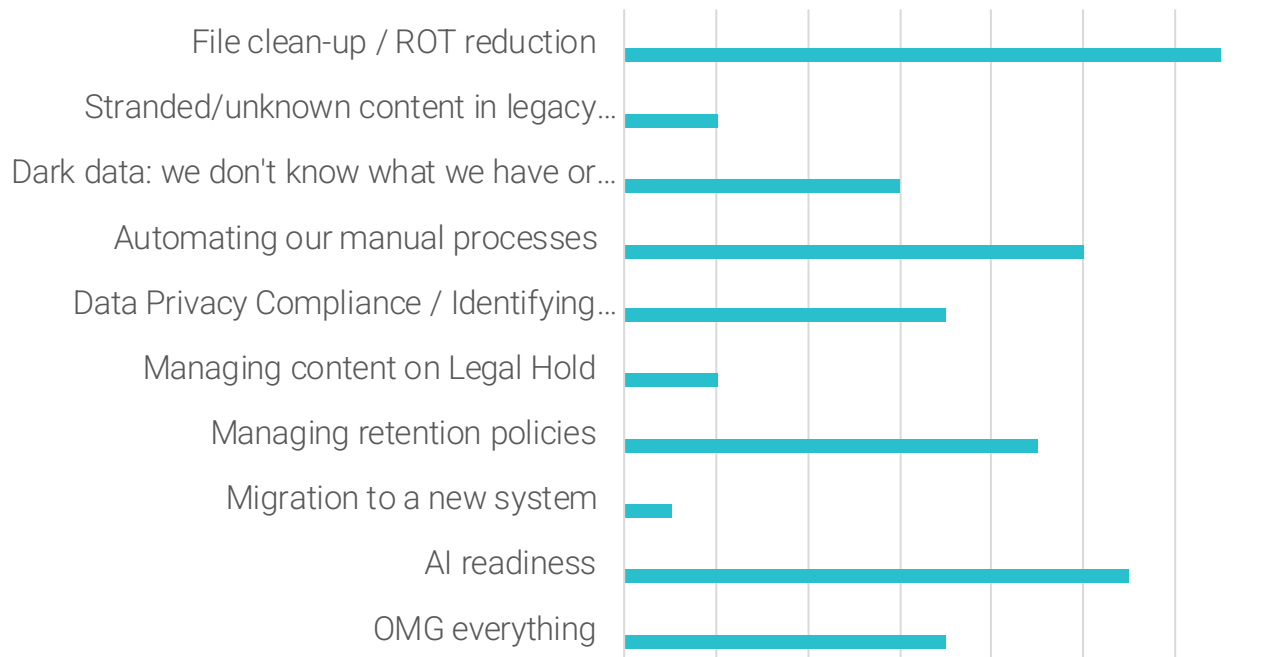
Other



Who you are & what your challenges are



Your RIM & IG Challenges



Housekeeping



Q&A



Recording



Slides



Feedback

Agenda

1

AI Without Jargon

- AI is a Prediction Model
- Types of AI
- Agentic AI & Self-evolution
- Tokenization
- RAG

2

Where & How AI Breaks

- Model Collapse
- Ceding control

3

How Your Role is Changing

- Observational → Operational
- Governance by design
- Uncertainty & control
- Intentional human intervention

Agenda

1

AI Without Jargon

- AI is a Prediction Model
- Types of AI
- Agentic AI & Self-evolution
- Tokenization
- RAG

2

Where & How AI Breaks

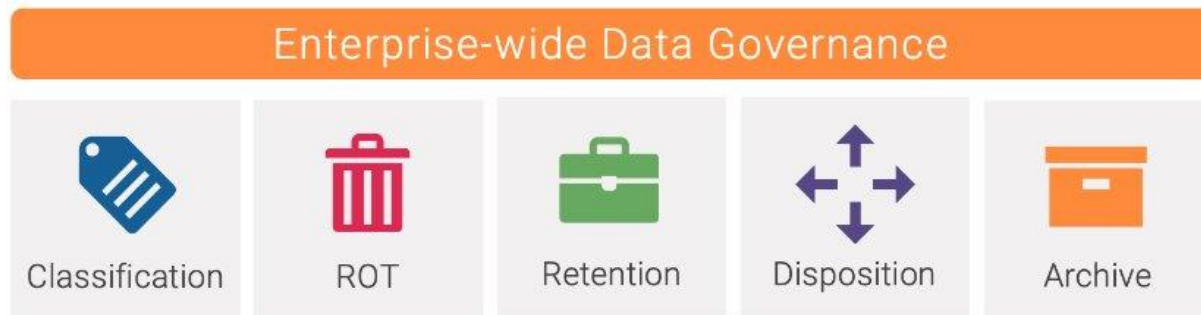
- Model Collapse
- Ceding control

3

How Your Role is Changing

- Observational → Operational
- Governance by design
- Uncertainty & control
- Intentional human intervention

Where IG was headed prior to AI



Where IG was headed prior to AI



Types of AI



Machine Learning

Algorithms that enable computers to learn from and make predictions or decisions based on data.



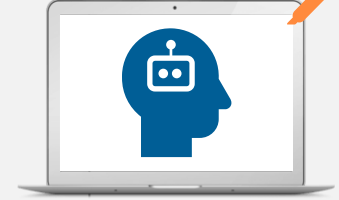
Extractive AI

Extracts specific information from large datasets or text.



Generative AI

Creates new content on the data it has been trained on.



Agentic AI

Operates independently, making decisions & performing tasks without human intervention.

Transparent & Defensible AI vs.



Autonomous &
Hallucinogenic AI



Machine Learning

Algorithms that enable computers to learn from and make predictions or decisions based on data.



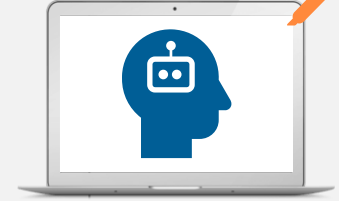
Extractive AI

Extracts specific information from large datasets or text.



Generative AI

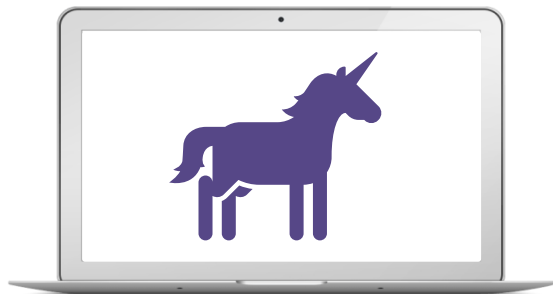
Creates new content on the data it has been trained on.



Agentic AI

Operates independently, making decisions & performing tasks without human intervention.

Gen AI Reality vs. Fantasy



Trained on datasets
Learns the data to
generate new content



Not magical search engine
Creates new content based on
learned patterns



Hallucinations
Takes a best guess based on
training data, does not fact check



Not up to date
Only as accurate as its
last run of source data

Tokenization

- Tokens are the “currency” AI runs on
- Turns text into numbers (“tokens”) for data processing
- More tokens = longer/harder processing
= greater cost
- The messier your data, the more expensive the input
- Converts data into billable units
- If ROT is 50%, AI costs are 50% + inflated!



Building Your IG Budget ROI

Proper data hygiene:

- Classification
- Retention
- Disposition
- Sensitivity & DLP
- AI suitability

reduces AI processing costs and improves response accuracy

RAG (Retrieval Augmented Generation)

- Gives AI the “right data” to source answers, not just training data
- Common use cases today
 - Summarize this document
 - What does our policy/manual/SOP say about xyz?
 - Find me everything related to xyz
 - Helpdesk bots
- Relevance vs. appropriateness
 - Semantic similarity vs. best choice
 - “What should be returned?”

RAG = Open Book Exam



- But it is the right book?
- The right edition?
- The right time to use it?
- The right access permission?

RAG - what happens at generation time

□ When a question is asked:

- RAG retrieves pieces from multiple sources
- not whole documents

□ So, you get:

- paragraph from Policy A
- clause from Contract B
- sentence from Email C

□ Generation Blends Those Fragments

- Synthesizes
- Paraphrases
- Recombines

□ The final answer is

- Not a source
- Not a document
- Not a record
- Not directly traceable

□ Lineage breakdown

- No chain of custody
- No system of record
- Not defensible!

Agentic AI & Self-evolution

- AI that can take actions on its own to achieve a goal—not just generate answers
- Learns and adjusts mid-course
- Uses tools & systems
- Autonomy
- Goal optimization
- Common use cases today
 - Meeting scheduler
 - Threat tracking & response
 - Expense approvals
 - Helpdesk ticketing



The Paper
Clip Maximizer

Agenda

1

AI Without Jargon

- AI is a Prediction Model
- Types of AI
- Agentic AI & Self-evolution
- Tokenization
- RAG

2

Where & How AI Breaks

- Model Collapse
- Ceding control

3

How Your Role is Changing

- Observational → Operational
- Governance by design
- Uncertainty & control
- Intentional human intervention

Model Collapse



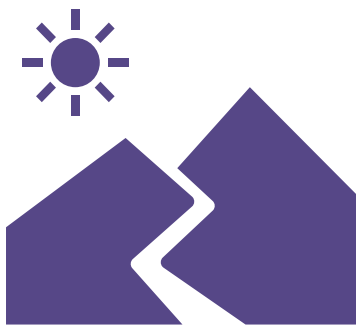
- Model collapse refers to the declining performance of generative AI models that are trained on AI-generated content.
- AI models collapse when trained on recursively generated data
- First generation models were trained on predominantly human-generated text
- Later models use synthetic data
 - Synthetic data is artificially created data that mimics real-world data but is not collected from actual sources
- The cure is active curation, ranking and verifying results

Evidence Collapse



- ❑ Degradation of the information ecosystem and enterprise evidence chains
- ❑ When we can no longer distinguish original observation from recursively generated interpretation
- ❑ Ultimately, governance systems lose the ability to establish provenance, authenticity, and trust
 - Synthetic institutional memory
- ❑ Evidence Collapse is a direct contributor to model collapse

AI Agents accelerate evidence degradation



- Goes beyond AI consumption of unreliable information
- Agents can create new documents, alter documents, change classifications & permissions, initiate (or halt) workflows around information
- AI sophistication is advancing faster than enterprise information governance
- Does governance enhance or impede AI?
 - The mountain highway example

Collapse Predictions from AI Itself

Open AI / ChatGPT

- 2026-2027 Local collapses
- 2027-2029 Larger, institutional collapse

Google/ Gemini

- 2024-2025 Already present
- 2026-2027 “Hollowing out”
- Early 2030s – “Late Collapse”

Anthropic / Claude

- 2024-2025 Already present
- 2028-2032 Technical failure
- 2027-2030 Skill atrophy loop

What makes it happen SOONER (*accelerants*):

- Malicious actors actively poisoning data to skew the logic
- Agentic AI spewing synthetic data
- Economic/Regulatory/Political pressure – humans expensive, AI cheap
- Monoculture risk

What makes it happen LATER (*decelerants*):

- Humans in the loop (HTL)
- Economic/Regulatory/Political pressure – incentives for quality
- Active curation: Lineage preservation, tagging for AI-generated
- Diversity of data sources

Ceding Control



AI itself (Agentic)

- Does the work, thinking & decisioning
- Short hop to writing/rewriting policies & decision frameworks – the control mechanisms
- “Outsourcing” decision-making & skills to AI means we will ultimately lose these skills.



Third Parties

- Apps charging you to host & access your own data
- Preventing/throttling queries & analysis
- Vendor-controlled settings & defaults set your policy without your knowledge or consent



Abstraction

- Users no longer direct query, read documents or interpret raw data
- Instead they get “synthesized” (generated) answers
- Interface buffer from reality
- Loses nuance, dissent, context, unlikely incidence

Agenda

1

AI Without Jargon

- AI is a Prediction Model
- Types of AI
- Agentic AI & Self-evolution
- Tokenization
- RAG

2

Where & How AI Breaks

- Model Collapse
- Ceding control

3

How Your Role is Changing

- Observational → Operational
- Governance by design
- Uncertainty & control
- Intentional human intervention

Observational vs. Operational



Observational Governance

Discover → Classify → **Report**

- ✓ Dashboards
- ✓ Reports
- ✗ Does not take action

Nice to have



Operational Governance

Discover → Classify → **Remediate**

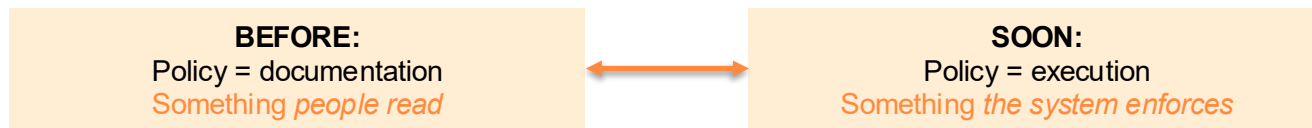
- ✓ Cross-repository classification
- ✓ Automated remediation
- ✓ Lifecycle management

Need to have

Organizations want to move from Visibility → **ACTION**

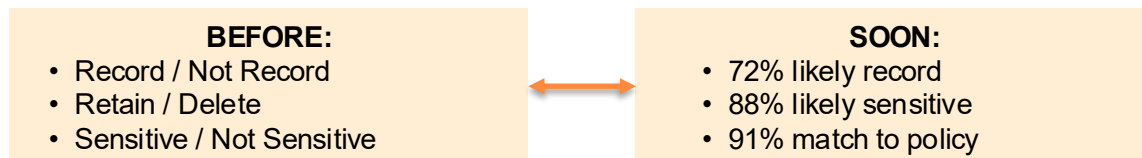
Governance by Design

- Setting up policies, procedures, tools and behaviors that obey IG standards natively
- AI tools and systems that are “IG-aware”
 - “Looks like we are creating a record..”
 - “This contains PII.” and also “I can identify this person..”
 - “This information belongs in Record Class 6430” or “location SharePoint/folder/client name/communication”
- Understand content AND governance
 - What is it?
 - How should it be used (and not used)? What is allowed?
 - How is it managed over time?



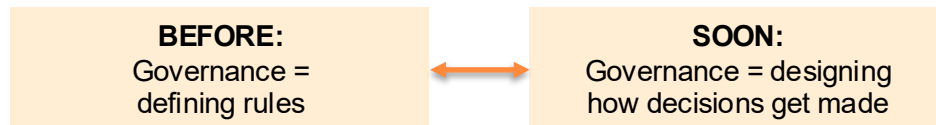
Uncertainty & Control

- Governance is no longer about certainty – it's about managing *uncertainty*
- Probabilities now drive decisions & actions
- IG becomes the **control layer**
 - What confidence is “good enough”?
 - Where do we: Automate, escalate, block
 - Risk-based application
 - 90% confidence for search
 - 99% confidence for regulatory classification



Uncertainty & Control - Challenges

- 80% confidence means 20% error
- Easy to “game” optimization
- Problematic thresholds
 - Too loose or too strict
- IG must focus on design choices, not certainty
 - Ex: at ROT = 90% confidence, Auto-delete? Review? Ignore?



In a probabilistic world, governance doesn't eliminate uncertainty, it defines how much of it the enterprise is willing to accept.

Intentional Human Intervention



- Define objectives, priorities & trade-offs
- Define “appropriateness” and “edge cases”
- Provide explicit feedback (feedback loops)
- Adjudicate ambiguity
- Monitor performance
(drift, unintended consequences, accuracy)
- System overrides
- Preserving knowledge
(rationale, judgement, expertise)

Humans move from doing the work to governing how the work is done.

How Your Role Changes in an AI environment

Define AI's Boundaries

- Where is AI being used?
- What should it *not* be used for?
- What still requires human review?

Embed Policy Into Tools

- Are retention rules reflected in AI outputs?
- Is sensitive data being used or accessed appropriately?
- Are tools aligned with policies or ignoring them?

Establish Decision & Trust Thresholds

- Set confidence levels
- When is AI output “good enough”?
- When to escalate?
- When to override?

Monitor Feedback Loops

- What output reuse?
- What becomes training data?
- What must be excluded?
- Are errors spreading?

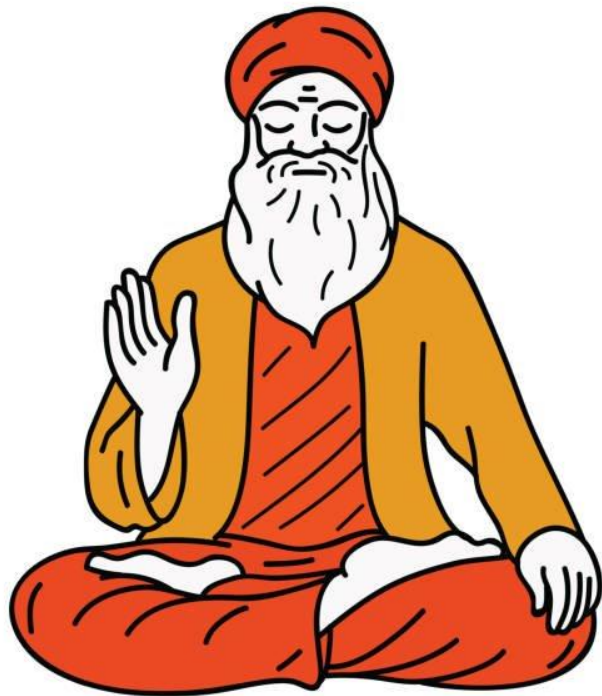
Preserve Lineage/Trust

- Where did this come from?
- Is it current?
- Is it accurate?
- Is it authoritative?

Purposeful Intervention

- Correct bad classifications
- Stop inappropriate outputs
- Flag issues early
- Organize training & source materials

Your Role in Aiding AI



□ Manage the Mess!

- Remove duplicates
- Clean up outdated content
- Ensure classification is correct
- Lock-down sensitive data
- Reduce error

□ Be the Data Guru

- Know what you have in your data estate
- Anticipate pushback with workarounds
- Adapt policies to AI speeds & decisioning models

Additional Information

□ Tokenization

- [Nvidia: Explaining Tokens – the Language and Currency of AI](#)
- [OpenAI: “Hands on” Tokenizer example](#)

□ RAG

- [YouTube: Intro to RAG](#)
- [Amazon: What is RAG \(Retrieval-Augmented Generation\)?](#)

□ Agentic AI

- [MIT/Sloan: Agentic AI, explained](#)
- [Amazon: What is Agentic AI?](#)

□ AI Model Collapse

- [Nature: AI Models Collapse When Trained on Recursively Generated Data](#)
- [IBM: What is model collapse?](#)

□ Data Lineage

- [Google: What is Data Lineage?](#)

Additional Information - Global AI Framework Models



IEEE Ethical Guidelines

Developed by the Institute of Electrical and Electronics Engineers (IEEE), these guidelines focus on the importance of transparency, accountability and the need for AI systems to align with human values. They have named their framework “Ethically Aligned Design.”



EU Artificial Intelligence Act EU AI Act

The European Union AI Act calls for regulation of AI technologies based on their assigned risk level categories – minimal risk, limited risk, high risk and unacceptable risk. Each category carries its own regulatory requirements.



OECD Principles on AI

Implemented in 2019 and updated in 2024, The Organization for Economic Co-operation and Development (OECD) Principles on AI provide policymakers with recommendations for effective AI policies. To date, the European Union, the Council of Europe, the United States, the United Nations and other countries use OECD's framework in their work on AI.



NIST AI Risk Mgmt Framework

In collaboration with the private and public sectors, NIST has developed a framework to better manage risks to individuals, organizations, and society associated with artificial intelligence (AI). It is intended to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.



www.valoratech.com



Book a Demo



Webinar Series



[/valora-technologies](https://www.linkedin.com/company/valora-technologies)

Q&A

Thank you



Sandy Serkes
President & CEO
sserkes@valoratech.com



Jennifer Nelson
VP Strategic Solutions
jnelson@valoratech.com