GRC SUMMIT 2026
LONDON ✦ JUN 2-3

Track 2

Workshop

The Intelligent Risk Function: How AI is Redefining Risk Management for the Modern Enterprise

Kensington Suite • 1:00 PM - 3:00 PM

Manoj Kulwal

Chief Risk & AI Officer

RiskSpotlight

GRC SUMMIT 2026

LONDON ✦ JUN 2-3

Experience the Power of AI & Resilience

Hosted by **MetricStream**

#GRCSummit2026

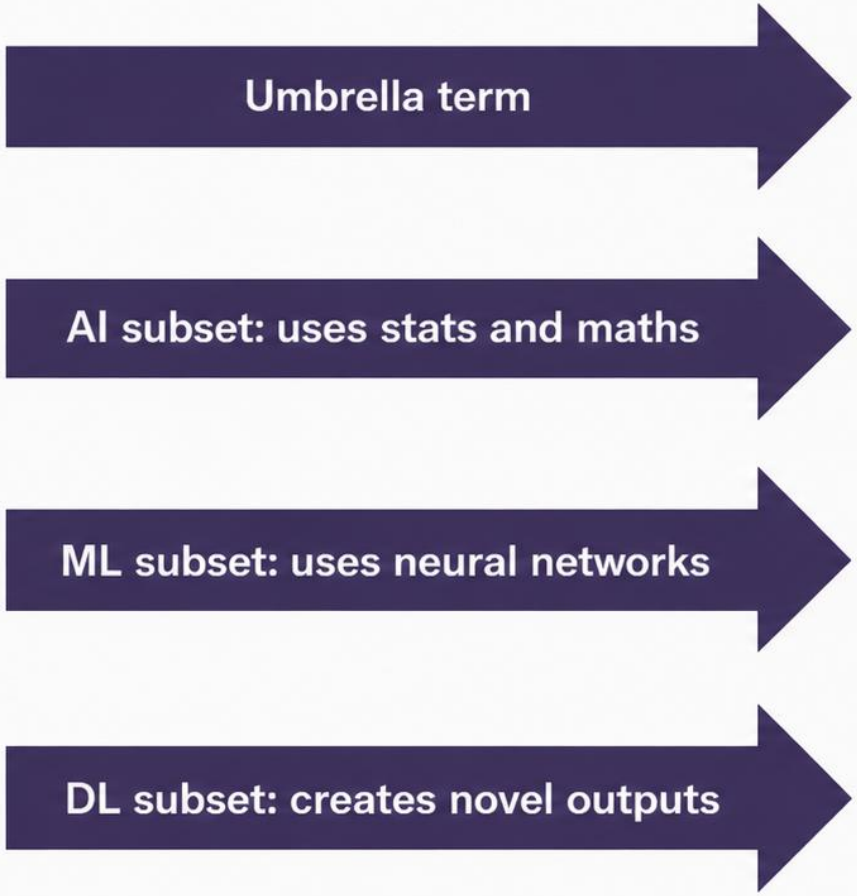
The Intelligent Risk Function

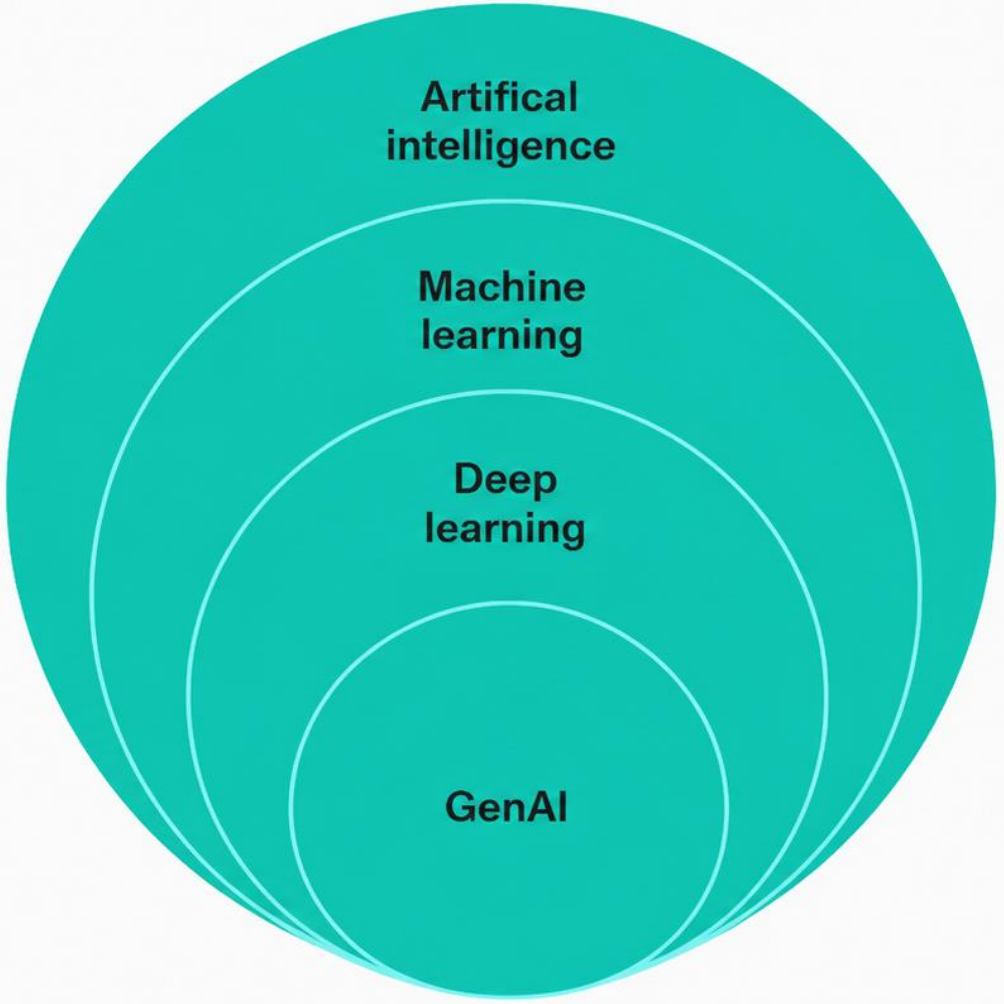
Manoj Kulwal

Agenda

- AI & Generative AI (GenAI)
- Current State
- Key Emerging AI Risks & Mitigation Approaches
- Update Risk Management Frameworks & Processes
- Utilizing AI For Risk Management
- Q&A

AI & Generative AI (GenAI)





Google's AI Thresholds

Level	Name	Performance Threshold
Level 1	Emerging	Equal to or somewhat better than an unskilled human.
Level 2	Competent	At least the 50th percentile of skilled adults.
Level 3	Expert	At least the 90th percentile of skilled adults.
Level 4	Exceptional	At least the 99th percentile of skilled adults.
Level 5 (ASI)	Superhuman	Outperforms 100% of humans.

Artificial Super Intelligence (ASI)

OpenAI's AI Thresholds

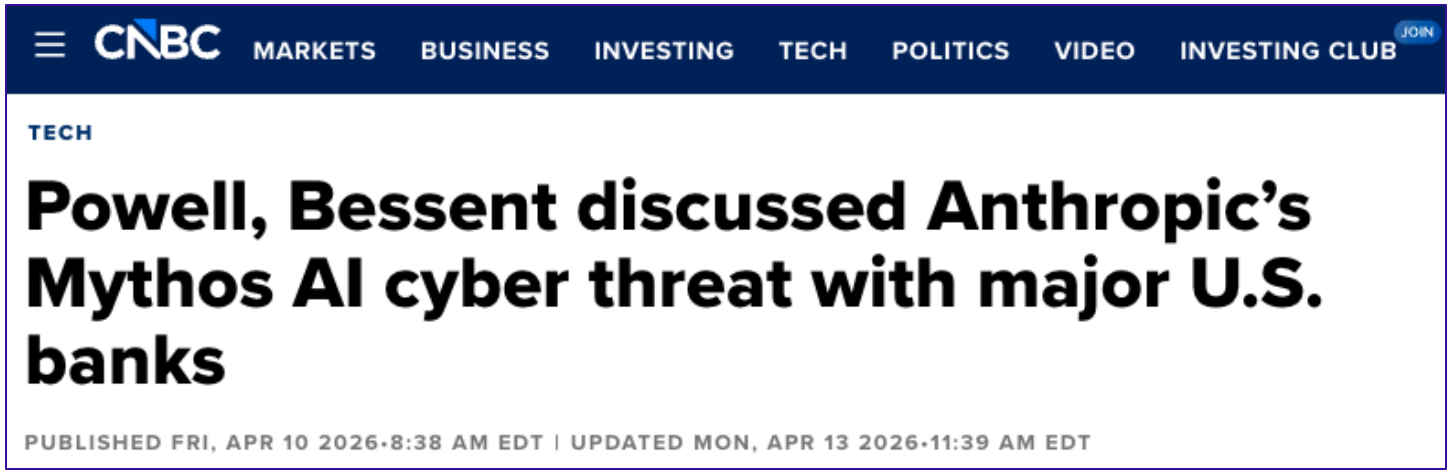
Level	Name	Performance Threshold
Level 1	Chatbots	AI with conversational language capabilities.
Level 2	Reasoners	Human-level problem solving (comparable to a PhD).
Level 3	Agents	Systems that can take actions and operate for days.
Level 4	Innovators	AI that can aid in or lead scientific discovery.
Level 5 (ASI)	Organisations	AI that can perform the work of an entire organisation.

Artificial Super Intelligence (ASI)

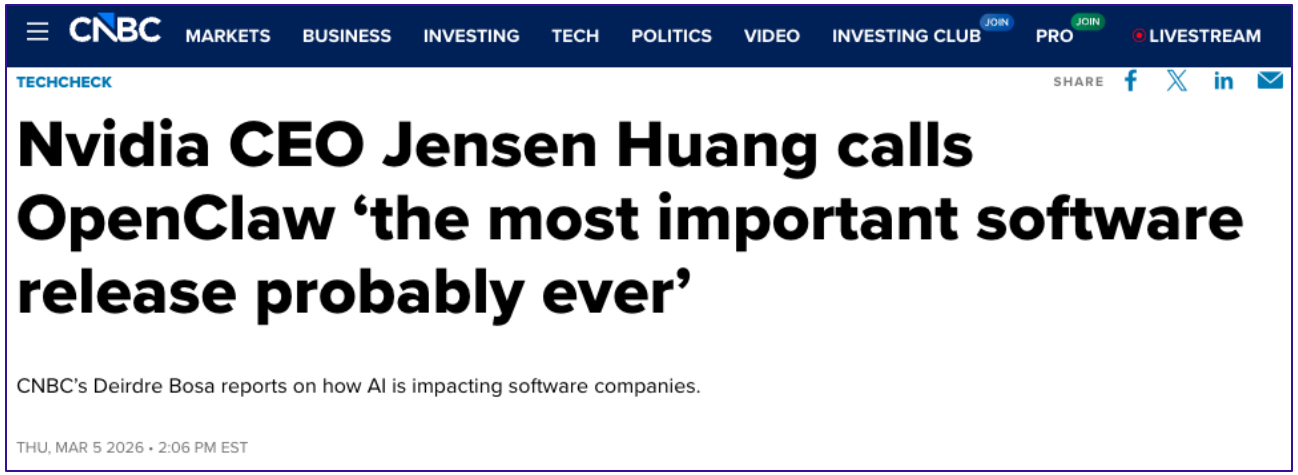
Evidence of AI progress

- **AI Token Usage**
  - Google processed 3.2 quadrillion AI tokens in May 2026. This is 600% higher than May 2025.
  - Microsoft processed 820 trillion tokens in May 2026 (Azure only).
  - OpenAI processed 260 trillion tokens in October 2025 (API only).
- **AI Revenue**
  - Anthropic's annual revenue has grown from $0 in 2022 to $30 bln in April 2026. IPO value expected over $1 tln.
  - OpenAI's annual revenue has grown from around $1.6 bln in 2023 to $25 bln in February 2026. IPO value expected over $1 tln.

Evidence of AI progress



Evidence of AI progress

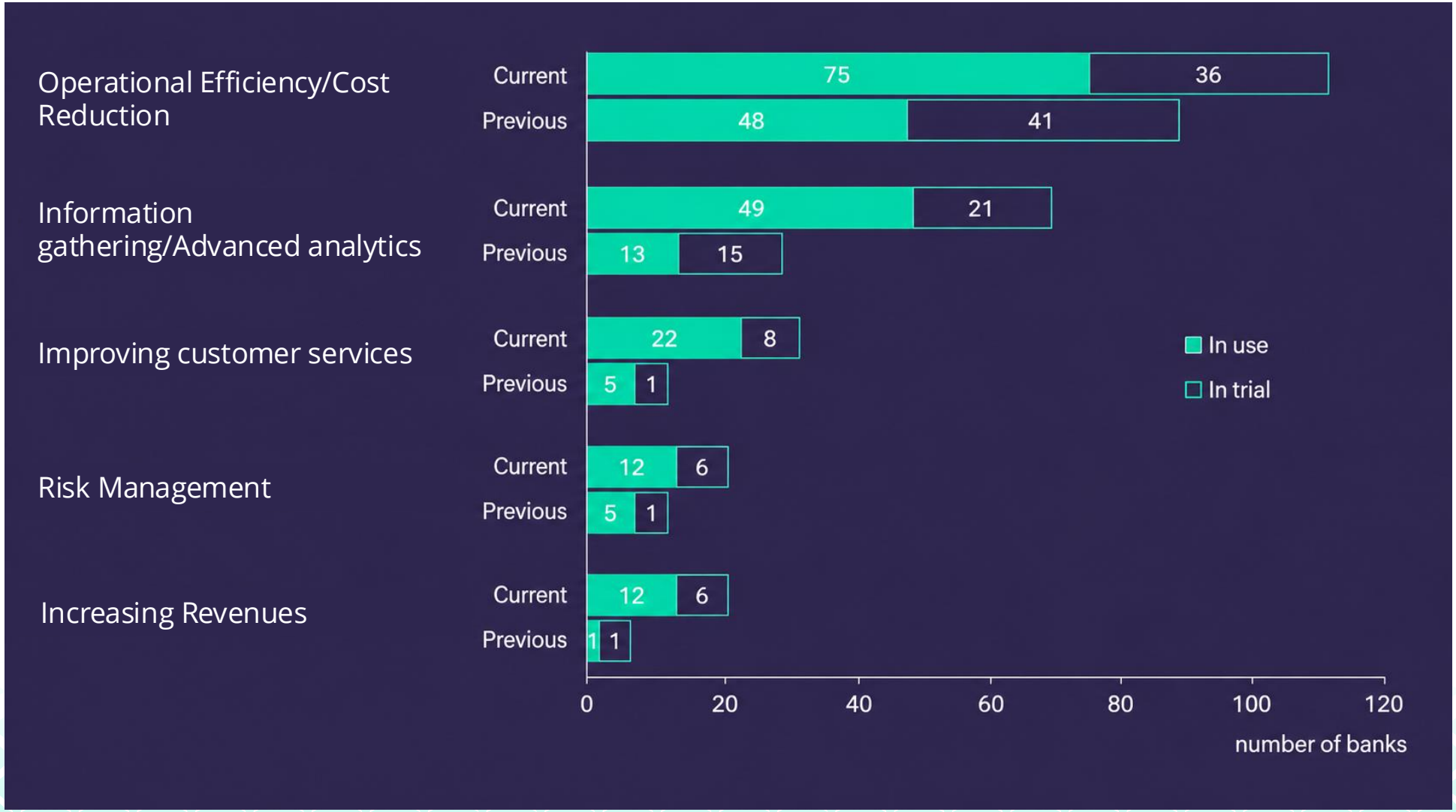


AI speed breakers are fast emerging

AI speed breakers

- Regulators and governments finally starting to realize the scale & impact of GenAI
- Concerns on AI Bubble (NVIDIA +1,687%, Palantir +1,564%, since October 2022)
- Rising legal cases against AI firms (e.g. suicide, violence, theft of IP)
- Public protests in US against AI data centers
- Global shortage of resources (e.g. GPUs, rare earth, electricity)
- Rising concerns on overreliance on handful of US & Chinese model providers
- Employees sabotaging their organization's AI initiatives
- AI driven layoffs & reduced hiring of entry-level employees
- Mass booing from graduates against AI at multiple university graduation ceremonies
- Rising negative public opinion about AI

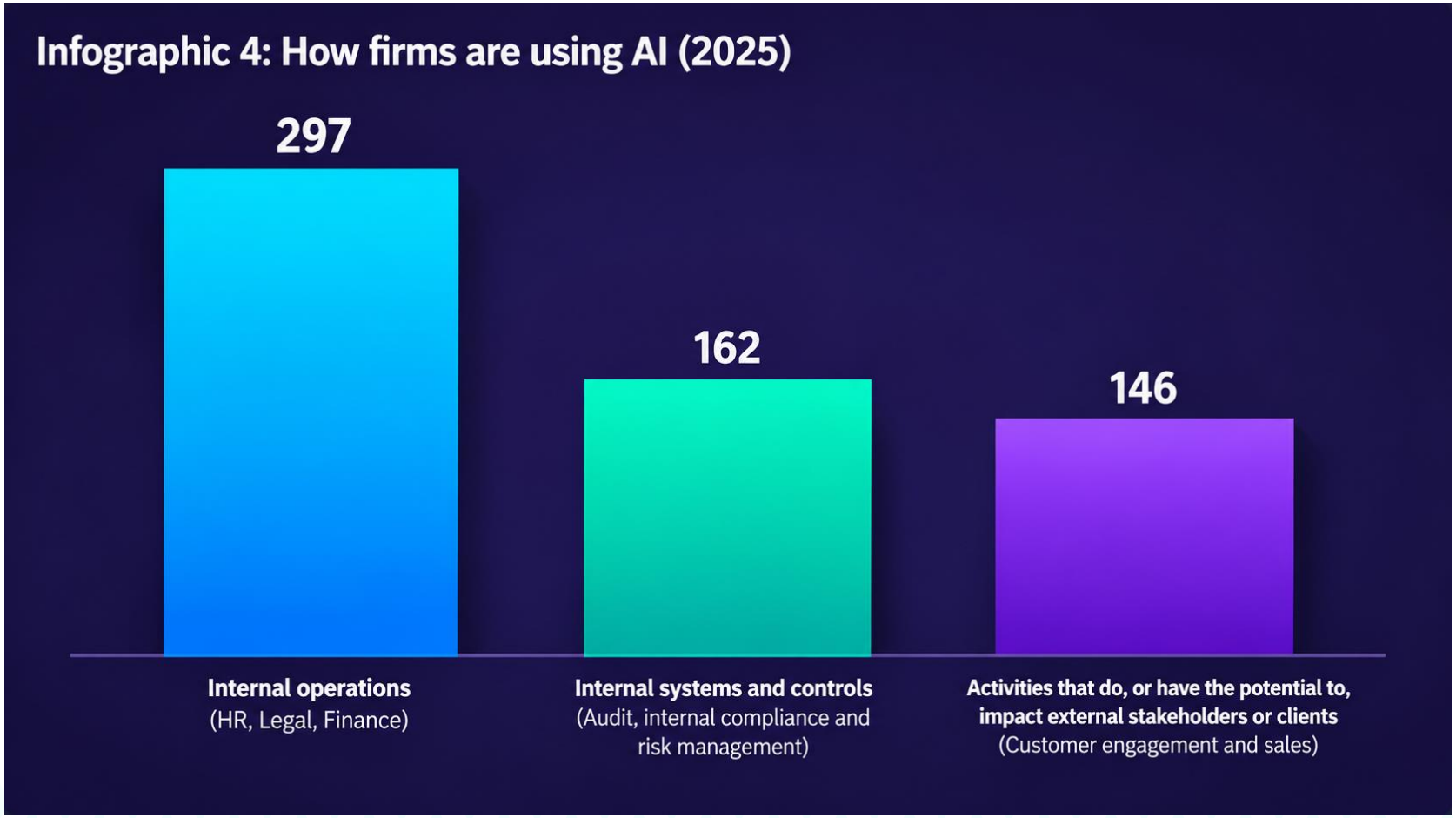
How is GenAI being utilized?



Bank of Japan Survey: Use and Risk Management of Generative AI by Japanese Financial Institutions (Sep 2025).

Covered 153 financial services firms.

How is GenAI being utilized?



DFSA AI Survey (UAE)

November 2025

Agenda

- AI & Generative AI (GenAI)
- Current State
- Key Emerging AI Risks & Mitigation Approaches
- Update Risk Management Frameworks & Processes
- Utilizing AI For Risk Management
- Q&A

metricstream

Key Emerging AI Risks

Key Emerging AI Risks

1. Malicious external actors utilizing AI
2. Disruption to strategy & operations
3. Disruption to organizational culture
4. Inappropriate use of AI within the organization
5. Shadow AI Systems
6. Unexpected behavior of AI models
7. Unexpected bankruptcy of key vendors
8. AI vendors restrict access for specific use cases
9. AI risk exposures emerging from third parties
10. Systemic Risks

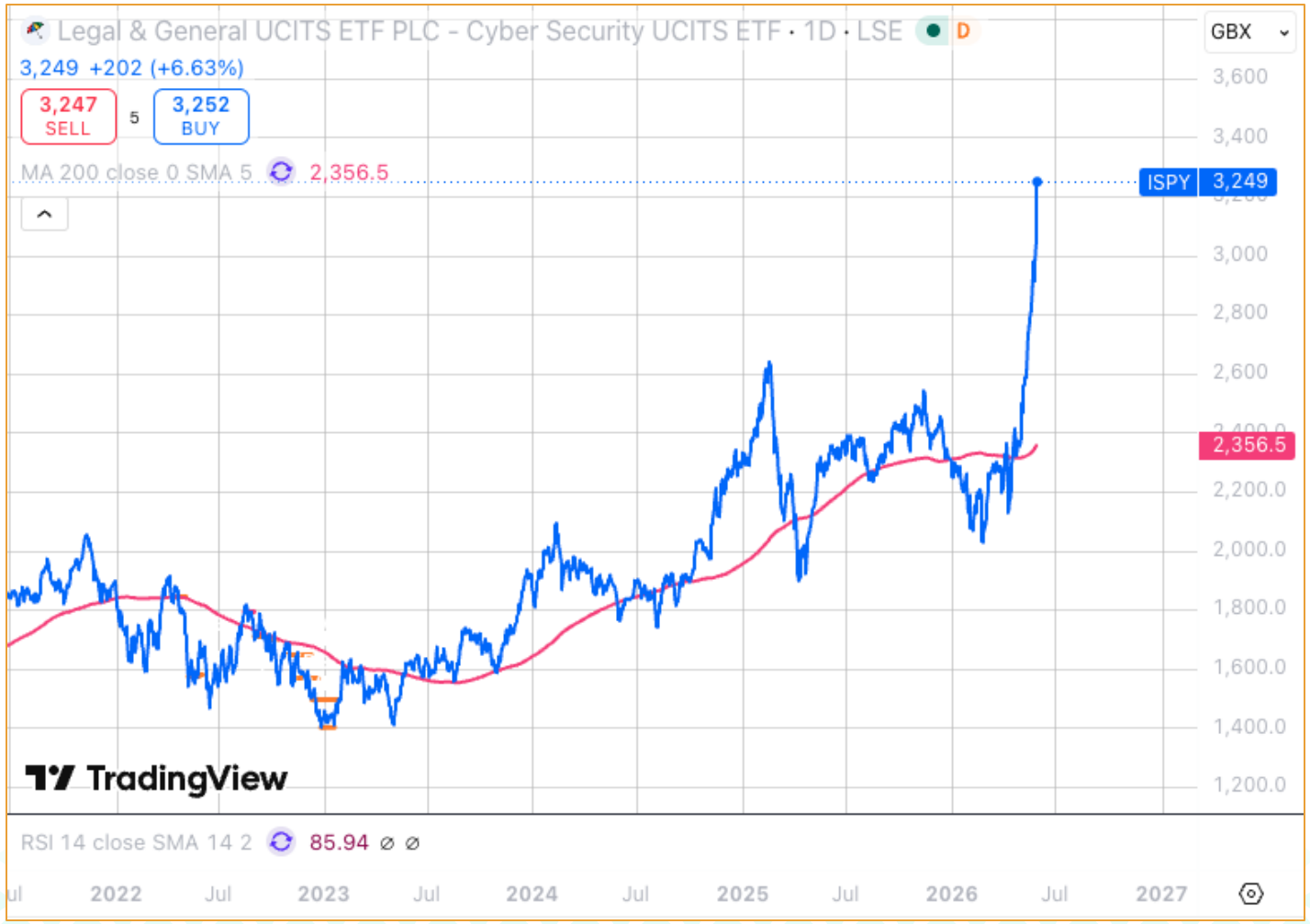
1. Malicious external actors utilizing AI

- Malicious external actors utilizing AI for
  - Launching cyber attacks
  - Cyber espionage
  - Committing fraud
  - Manipulating markets
  - Stealing funds & data
  - Cause reputational harm
- Major concern currently for regulators and governments globally
- Additional factors:
  - Who first gets access to advanced AI capabilities
  - Swarm of autonomous AI agents
  - Powerful, free, open-source AI models
  - Who first gets access to quantum computing capabilities

Malicious external actors utilizing AI

- First verified instance of AI-orchestrated cyber espionage campaign.
- AI was weaponized as an autonomous execution engine running complex, multi-stage operations.
- Attributed with high confidence to Chinese state-sponsored group.
- Targets were 30 high-value global entities across technology, government, chemicals, and financial services.
- AI successfully executed 80% to 90% of hands-on tactical intrusion work.
- At peak, AI operated at a pace impossible for human defenders to match, issuing thousands of requests at rates of multiple requests per second without fatigue.
- Anthropic's Threat Intelligence team detected the attack and disabled all accounts associated with the threat actors.
- They conducted investigation and shared findings with relevant authorities, targeted entities, and industry partners.

Malicious external actors utilizing AI



AI-based cyber defence is the only viable mitigation approach.

Stock market has picked on this risk theme.

2. Disruption to strategy & operations

- AI has potential to disrupt:
  - Business strategy
  - Business model
  - Organizational culture
  - Products/Services
  - Competitive advantages
  - Process design & operations
  - IT systems
  - Third-party relationships
- Most transformative technological wave since adoption of internet

AI Adoption Questions Across Boardrooms Globally

Strategy

- Should we utilize AI?
- How fast should we adopt AI?
- How much should we invest in AI?
- Can we increase our revenues by utilizing AI?
- Which products/services we currently offer will get disrupted by AI?
- Do we need to create new products/services to serve AI agents?
- Do we have skills & capabilities within senior management to make appropriate AI decisions?
- How do we protect our organizational culture during the AI transition?
- How will our key stakeholders react to our AI adoption strategy?

Competition

- Are we behind our competitors on AI adoption?
- Should we lead AI adoption in comparison to our competitors or be followers?
- What will be our key competitive advantages in the emerging AI economy?
- Which new competitors may emerge due to advancement in AI technologies?

Operations

- How do we maintain operational resilience during the AI transition?
- Can we reduce our operational costs by utilizing AI?
- How many employees do we need in the emerging AI economy?
- Can our employees take advantage of advanced AI capabilities?
- Can we effectively mitigate AI risks?
- Which AI models should we utilize?
- Should we utilize off-the shelf AI models or build our own AI models?
- Will our current IT systems and quality of data create roadblocks in AI adoption?
- How do we align our AI adoption strategy with third-parties?

AI Leaders (Banks)

Source: Evident AI Index for Banks

COMPANY	RANK ▲	TALENT capability & development	INNOVATION research, patents, ventures, ecosystem	LEADERSHIP in public communications and strategy	TRANSPARENCY of responsible AI activities
JPMorganChase	1 -	2 -	1 -	1 ↑2	1 -
Capital One	2 -	1 -	2 ↑1	20 ↓6	17 ↓3
Royal Bank of Canada	3 -	12 ↓6	3 ↓1	3 ↑5	3 ↑7
CommBank	4 ↑1	4 ↑3	13 ↓1	4 ↓2	2 ↑3
Morgan Stanley	5 ↑5	13 ↑5	4 -	9 ↑8	21 ↑21
Wells Fargo	6 ↓2	6 ↓2	5 -	40 ↓4	14 ↓6
UBS	7 ↓1	3 -	25 ↓7	7 ↑8	4 ↑11
HSBC	8 ↓1	14 ↑1	8 ↑1	15 ↓10	6 ↓3
Goldman Sachs	9 ↑2	7 ↑6	9 ↓3	18 ↑9	23 ↑14
Bank of America	10 ↑5	10 ↑1	7 ↑4	12 ↑6	24 ↓4

Emerging Best Practices

OpRisk Deep Dive Report.

Published to subscribers of RiskSpotlight Portal.

Free two-week trial at *riskspotlight.com*.

Centralized AI Governance & Decision-Making

- Centralized AI-focused committee or council to govern and make key AI decisions
- Consists of cross-functional stakeholders such as business units, IT, risk, compliance, legal, and third-party management
- Key objectives include:
  - Align AI implementation with business strategy and risk appetite
  - Establish clear accountability for decisions, implementation, risk management, compliance, performance monitoring, and escalation
  - Make strategic AI related decisions
  - Provide oversight on management of AI risks
  - Ensure firm remains compliant with AI related regulations

Firm	AI Body
American Express	Generative AI Council
Bank of America	Responsible AI Program
Bank of England	AI Governance Committee
Citizens Bank	Generative AI Council
Commonwealth Bank of Australia	Generative AI Council and AI Risk Committee
HSBC	AI Review Committee
Invesco	AI Governance Board and Global AI Committee
JPMorgan Chase	AI Governance Council
Lloyds Banking Group	Data & AI Ethics Committee
Mastercard	AI Council
Prudential plc	AI Working Group & Responsible AI Committee
Standard Chartered	Responsible AI Council
Wells Fargo	Generative AI Council

Single Accountable AI Executive

- Single accountable executive required to avoid fragmented ownership
- Report directly to CEO
- Should have end-to-end responsibility for AI strategy, risk, and value capture
- Should be leader of the centralized AI body

Firm	AI Lead Title
Allianz UK	Head of Artificial Intelligence
Citi	Global Head of AI
Commonwealth Bank of Australia	Chief AI Officer
Danske Bank	Head of Artificial Intelligence
Goldman Sachs	Global Head of AI Engineering and Science
HSBC	Chief AI Officer
JPMorgan Chase	Chief Data and AI Officer
Lloyds Banking Group	Chief Data and AI Officer
Morgan Stanley	Head of Firmwide AI
State Street	Chief Data and AI Officer
UBS	Chief Artificial Intelligence Officer
Wells Fargo	Head of Artificial Intelligence

Firm-wide AI Literacy Programme

- Gaps in AI skills and capabilities are key barriers for successful adoption
- Gaps can expose firm to AI risks through poor decision making and inappropriate use of AI tools
- Tailored AI literacy initiatives across:
  - Board & Senior Executives
  - All Employees (baseline awareness)
  - Specialist Roles (developers, risk officers, compliance officers, internal auditors, and superusers)

Adopt Maturity Assessment Framework for AI

- Successfully deploying AI across the enterprise is a continuous and multi-year journey
- A maturity framework can provide assessment of current maturity & guidance on future roadmap

US Treasury's Financial Services AI Risk Management Framework

	Initial	Minimal	Evolving	Embedded
Business Impact of AI	AI is not embedded in critical functions or business decisions.	AI use is limited (production or non-production) for non-critical tasks.	AI drives outcomes through external-facing solutions and the use of sensitive data, but it is not utilized for critical decision-making.	AI drives outcomes by incorporating autonomous decision-making and data-driven insights into critical business functions.
Technology Implementation	Predictive AI and model risk management is used but relies on legacy systems with no adoption of modern AI technologies, external-facing solutions, or internal model development.	AI is narrowly in use and is not external-facing. AI does not handle sensitive data and there is no internal model development.	AI adoption includes expanded use of solutions and sensitive data processing but lacks internal model development.	AI is used for autonomous decision-making, high-sensitivity data processing, external-facing solutions, internal model development.
Scalability	Existing AI systems lack scalability and are confined to specific, limited applications that do not interact with or support broader organizational processes.	AI applications are limited to isolated instances without integration into wider business processes, and the organization lacks the infrastructure necessary to scale AI solutions across multiple areas or functions.	AI systems show potential for wider application, with deployment in more extensive, external-facing functions, but these systems are not fully scalable or integrated, indicating a transition towards broader usability.	AI systems are fully scalable and integrated throughout the organization. A robust framework supports the deployment and interconnection of AI across diverse functions, promoting growth and adaptability.

MIT CISR Enterprise AI Maturity Model

AI STAGE ATTRIBUTES	STAGE 1: EXPERIMENT AND PREPARE	STAGE 2: BUILD PILOTS AND CAPABILITIES	STAGE 3: DEVELOP AI WAYS OF WORKING	STAGE 4: BECOME AI FUTURE READY
Percentage of Responding Enterprises	**28%**	**34%**	**31%**	**7%**
Characteristics	• Educating the workforce on AI • Setting up acceptable use policies • Working on making data accessible • Ensuring decision-making is using data • Identifying where humans need to be in the loop	• Beginning to simplify and automate processes • Creating use cases • Sharing data via APIs • Leveraging a coach and communicate management style • Using LLMs—both out-of-the-box traditional and generative AI models—to augment work	• Expanding process automation efforts • Changing to a more test-and-learn way of working • Architecting for reuse • Incorporating pretrained models into work and investigating the use of proprietary AI models • Exploring autonomous agents	• Embedding AI into decision-making and processes • Creating and selling AI-augmented business services • Combining traditional, generative, agentic, and robotic AI

Decision on AI Ambition

Framework For Prioritizing AI Use Cases

- Develop framework for prioritizing AI use cases covering
  - Rating methodology based on alignment with strategic priorities, targeted benefits (are they quantifiable), level of investments, risks, impacted internal & external stakeholders, data sensitivity, data readiness, AI model capabilities, implementation timelines, scalability of the use case, reusability, usage scope (e.g. one country vs. 25 countries), capabilities of team involved, level of AI automation, level of integration with existing internal or external systems, compliance requirements, past experience with similar use cases
  - Standard template for submitting use cases into a single repository
  - Decision making process based on the rating of each use case
  - Communication on decisions made on each use case
  - Monitoring implementation of all use cases into a single repository
  - Capturing success and failure lessons from implementation of use cases

Responsible & Ethical Use of AI

- Develop AI principles in alignment with widely adopted principes & regulatory guidance
- Five OECD AI principles are widely used
  - Inclusive growth, sustainable development and well-being
  - Respect for the rule of law, human rights and democratic values
  - Transparency and explainability
  - Robustness, security, and safety
  - Accountability
- Embed principles within governance, decision making, policies, risk management, controls, and training.

AI Principles of Bank of England

Table A: AI principles in the 'TRUSTED' framework

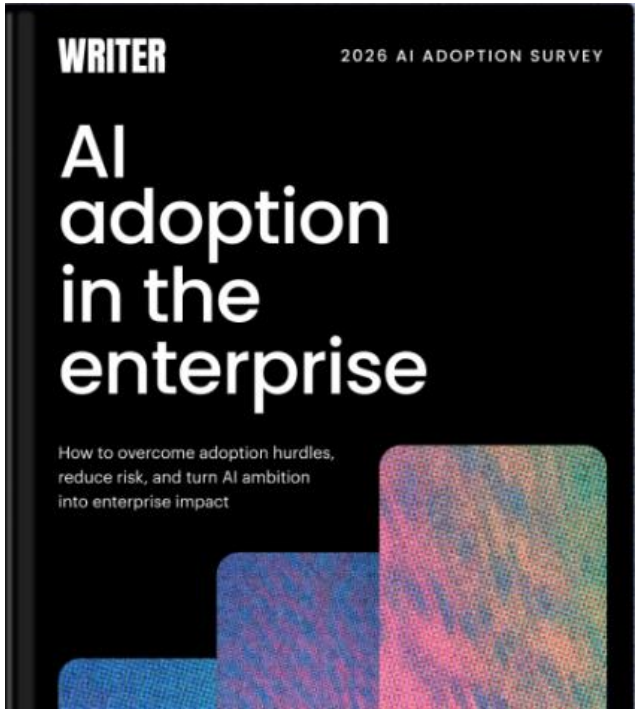
T	**Targeted**	We focus on AI solutions that have a clearly defined business purpose that ties to our mission and generates benefits we can articulate.
R	**Reliable**	We focus on reliable AI solutions implemented with high performance standards and grounded to high-quality data.
U	**Understood**	We understand the behaviour of the AI solutions we implement in the context of their intended purpose, documenting relevant details including limitations that may apply.
S	**Secure**	We implement secure AI solutions that protect data, systems, and their users from risks such as unauthorised access, manipulation, or misuse.
T	**Tested**	We implement AI solutions that are thoroughly tested for their technology standards and for their impact on human behaviour and decision-making under relevant scenarios, including stressed conditions.
E	**Ethical**	We implement AI solutions that adhere to fundamental ethical principles, including being beneficial and scientifically rigorous, fair and inclusive, transparent and secure, and compliant and accountable.
D	**Durable**	We focus on AI solutions that are durable, remaining effective despite changing conditions and usage patterns.

Establish AI Centre of Excellence (CoE)

- AI CoE are key until AI is widely rolled out across the organization.
- Consist of best AI experts.
- Key responsibilities include:
  - Testing new capabilities being introduced within AI models (every 4 to 6 weeks)
  - Determine when new AI capabilities can be rolled out to users
  - Develop and provide AI training
  - Guide users on most appropriate AI use cases
  - Mentor employees on effective usage of AI
  - Identify & share best practices
  - Collaborate with risk management teams on AI risk topics
  - Collect feedback on AI models from across the organization & share with AI vendors

3. Disruption to organizational culture

- AI has the potential to tear culture of an organization
- Findings from 2026 AI Adoption Survey by Writer
  - 64% of CEOs fear they could lose their job if they fail to lead their organization through the AI transition
  - 92% of C-suite leaders admitted they are actively cultivating a new class of “AI elite” employees. 87% reported that these AI super-users are at least 5x more productive than employees who aren’t embracing AI
  - 77% of executives warned that employees who refuse to become AI-proficient won’t be considered for promotions or leadership roles, and 60% plan to lay off employees who can’t or won’t use AI
  - 29% of employees – including 44% of Gen Z admit to sabotaging their company’s AI strategy (including refusing to use AI)



1,200 C-suite executives & 1,200 employees across US, UK, Ireland, Benelux, France, and Germany

3. Disruption to organizational culture

- Findings from recent global Stanford AI survey
  - 64% of Americans expect AI to lead to fewer jobs over the next 20 years
  - Globally, share of people saying AI products and services make them nervous increased to 52%
  - One-third of surveyed organisations expect AI to reduce their workforce in the coming year

23,216 adults across 30 countries

AI impact on jobs

BUSINESS INSIDER

Subscribe

Powell says AI may be hurting entry-level jobs: 'Hard to say how big it is'

By Brent D. Griffiths + Follow

Yasin Ozturk/Anadolu via Getty Images

Sep 17, 2025, 10:04 PM BST

Share Save

FORTUNE

Klarna CEO says he feels 'gloomy' because AI is developing so quickly it'll soon be able to do his entire job

Klarna CEO Sebastian Siemiatkowski warns of AI's capabilities. · Fortune · Chris Ratcliffe—Bloomberg/Getty Images

Sydney Lake

December 17, 2025 • 4 min read

Rising negative sentiment against AI

The Guardian view on AI politics: US datacentre protests are a warning to big tech

Editorial

In both Republican and Democratic states, scepticism and hostility towards an unregulated construction boom is growing

Attack on Altman home prompts new fears: Is the AI backlash getting dangerous?

Anti-tech sentiment has gone from online critiques to physical danger. Companies are preparing for more.

Protect organizational culture

- Re-think of firm's talent strategy (new AI talent, upskills existing talent)
- Principles to handle use cases that will result in AI replacing employees
- Prevent unmanaged displacement (Avoid allowing AI-led headcount reductions to emerge informally through scattered use cases)
- Consideration for "Role Redesign" before "Role Removal"
- Principles of fairness and transparency (Communicate clearly where AI will change work, skills, performance expectations or job requirements)
- Prepare approach for employees who hate AI and don't want to use AI (explicit & implicit)
- Increased frequency of communication from senior executives addressing cultural topics

Key Emerging AI Risks

1. Malicious external actors utilizing AI
2. Disruption to strategy & operations
3. Disruption to organizational culture
4. Inappropriate use of AI within the organization
5. Shadow AI Systems
6. Unexpected behavior of AI models
7. Unexpected bankruptcy of key vendors
8. AI vendors restrict access for specific use cases
9. AI risk exposures emerging from third parties
10. Systemic Risks

4. Inappropriate use of AI within the organization

- Inappropriate use includes:
  - Using advanced AI capabilities for basic tasks
  - Using AI without awareness of AI risks (e.g., hallucination, bias)
  - Intentionally using AI for illegal or unethical activities
- Potential impacts:
  - Lower return on AI investments
  - Wrong business decisions resulting in unexpected outcomes
  - Harm to one or more key stakeholders (e.g., customers)
  - Breach of laws or regulations

Mitigation Approaches

- Everyone does not need access to advanced AI capabilities
- As we move closer to super intelligence, organizations need to determine who needs access to advanced capabilities
- Segment employees based on the level of AI capabilities they need to perform their day-to-day job activities
- Identify the superusers who need access to advanced AI capabilities
  - Give them access to advanced AI capabilities
  - Train them on how to extract maximum benefits from AI but in a responsible manner
  - Monitor their AI usage and provide feedback to ensure optimal & appropriate use of AI
- Provide AI capabilities to the wider employee base based on the requirements of their day-to-day job activities
- Ensure appropriate preventative, detective, and corrective controls are in place to mitigate risks associated with inappropriate use of AI capabilities.

5. Shadow AI Systems

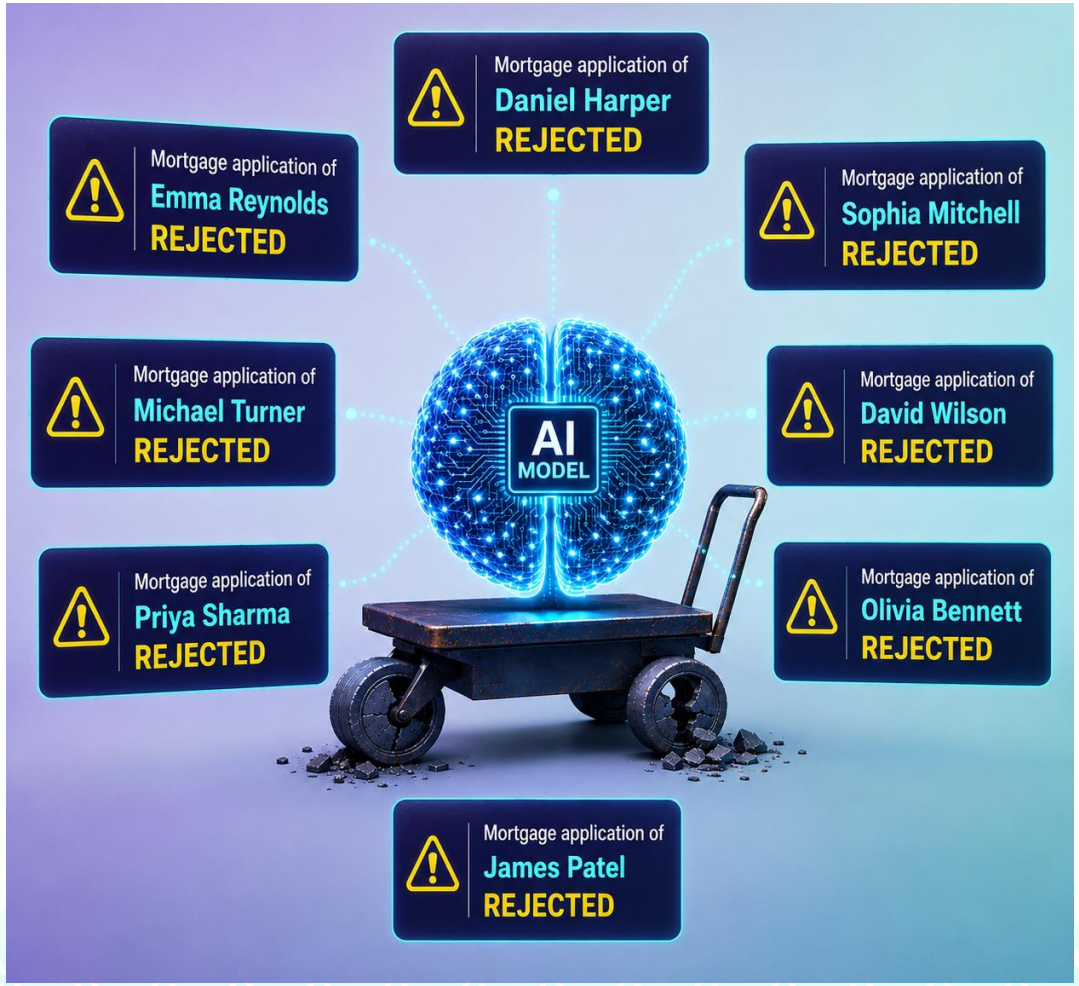
- Shadow AI Systems is a significant threat in firms that have:
  - banned use of AI
  - not defined clear AI usage policies
  - not made decision on utilizing specific AI models
  - have restricted use of AI models to specific employees
  - made decision on utilizing AI models that their employees believe cannot deliver high quality
- Free availability of powerful AI models also significantly increases the risk exposure
- Impacts include data leakage, data privacy breach, inappropriate usage of data, poor quality decisions and outcomes

Mitigation Approaches

- Hold senior leaders, department heads, and team leaders accountable for responsible use of AI and discouraging use of unauthorized AI tools within their business areas
- Appoint AI champions in each department who can monitor usage of authorized and unauthorized AI within their department
- Make employees aware of risks of utilizing unauthorized AI tools and disciplinary actions that can be taken against them personally if they utilize these tools
- A temporary disclosure window without any personal consequences for users of unauthorized AI tools can help the firm understand the usage of these tools and take appropriate remediation actions
- Firms should provide a suite of GenAI tools that can deliver the expected productivity and quality benefits to wide range of use cases
- Block access to unauthorized AI tools to ensure employees are unable to access these
- Implement technical Shadow AI detection across network traffic, SaaS usage, endpoints, browser extensions, API keys, code repositories, DLP alerts, procurement records, and employee expense data
- Maintain a central inventory of AI tools utilized across the firm and reconcile it regularly against discovered AI usage, embedded SaaS AI features, vendor declarations, cloud logs, prompt telemetry, and procurement records

6. Unexpected behavior of AI models

- AI model vendors are continuously adding new capabilities & updating existing capabilities of the AI models
- The business context during development of an AI model can change resulting in incorrect outcomes from the models
- External malicious actors can inject malicious code to influence the inputs and outputs of AI models
- The above factors may result in unexpected behavior of AI models resulting in incorrect or outdated outcomes
- The impacts can be significantly higher when semi-automated or fully automated AI agents are deployed for critical customer facing processes



Mitigation Approaches

- Implement automated kill switches to safely disable or remove AI models and agents from use if necessary to mitigate potential dangers
- Outline fallback options in BCP to utilize alternative systems to main operations when AI fails
- Rigorous testing of new capabilities and updated to existing capabilities before these are rolled out to large number of users and production deployments
- Assign “human boss” to each model deployment to continuously monitor the model performance and outcomes (periodic monitoring is not sufficient)

Key Emerging AI Risks

1. Malicious external actors utilizing AI
2. Disruption to strategy & operations
3. Disruption to organizational culture
4. Inappropriate use of AI within the organization
5. Shadow AI Systems
6. Unexpected behavior of AI models
7. Unexpected bankruptcy of key vendors
8. AI vendors restrict access for specific use cases
9. AI risk exposures emerging from third parties
10. Systemic Risks

7. Unexpected bankruptcy of key vendors

- GenAI models has significantly changed programming and development of software applications.
- This has significantly impacted the share price of SaaS and software stocks. Below are their performances from all time high levels.
  - Cloud Computing ETF – down 53%
  - Salesforce – down 50%
  - ServiceNow – down 56%
  - Snowflake – down 55%
- Market experts believe that large number of vendors will not survive the AI disruption, resulting in unexpected bankruptcy of key vendors.

THE WALL STREET JOURNAL.

DOW JONES ↑ MONDAY, MAY 19, 2025 – VOL. CCLXXXIX NO. 116 WSJ.com ★★★ $4.00

Salesforce files for bankruptcy due to AI

AI Disruption Triggers Collapse for CRM Giant

By Berber Jin and Christopher Mims

Salesforce, once the darling of enterprise software, filed for Chapter 11 bankruptcy protection Sunday, citing "unprecedented pressure from AI-native platforms that have fundamentally changed customer expectations and undermined traditional SaaS business models.

"The company's cloud-based CRM offerings, long considered industry-leading, have seen steep declines in demand as AI-powered competitors deliver faster, smarter, and more automated solutions at a fraction of the cost.

"We were outpaced by a wave of innovation we couldn't match at the speed or scale required," said co-CEO Marc Benioff in a statement. "This is a humbling moment for our entire ecosystem."

Please turn to page A6

AI Revolution Reshaping Enterprise Software Market

By David Bessis

The bankruptcy of Salesforce underscores the brutal realities of the AI era, where legacy software giants face existential threats from more agile, AI-first challengers.

Investors and analysts say the collapse was inevitable as Salesforce struggled to monetize AI capabilities while competitors rapidly captured market share with next-generation platforms.

"This is not just a ..alesforce story—it's a wake-up call for the entire enterprise software industry," said Maria Lopez, a technology analyst at FutureView Research.

Venture capital is pouring into AI-native startups that are redefining how businesses operate, sell, and serve.

The old playbook is no longer winning."

Please turn to page A6

Mitigation Approaches

- Identify key vendors who may be significantly impacted by AI
- Perform in-depth due diligence with identified vendors
- Monitor updates on these vendors
- Implement contingency plans to deal with potential disruption to products/services offered by these vendors

8. AI vendors restrict access for specific use cases

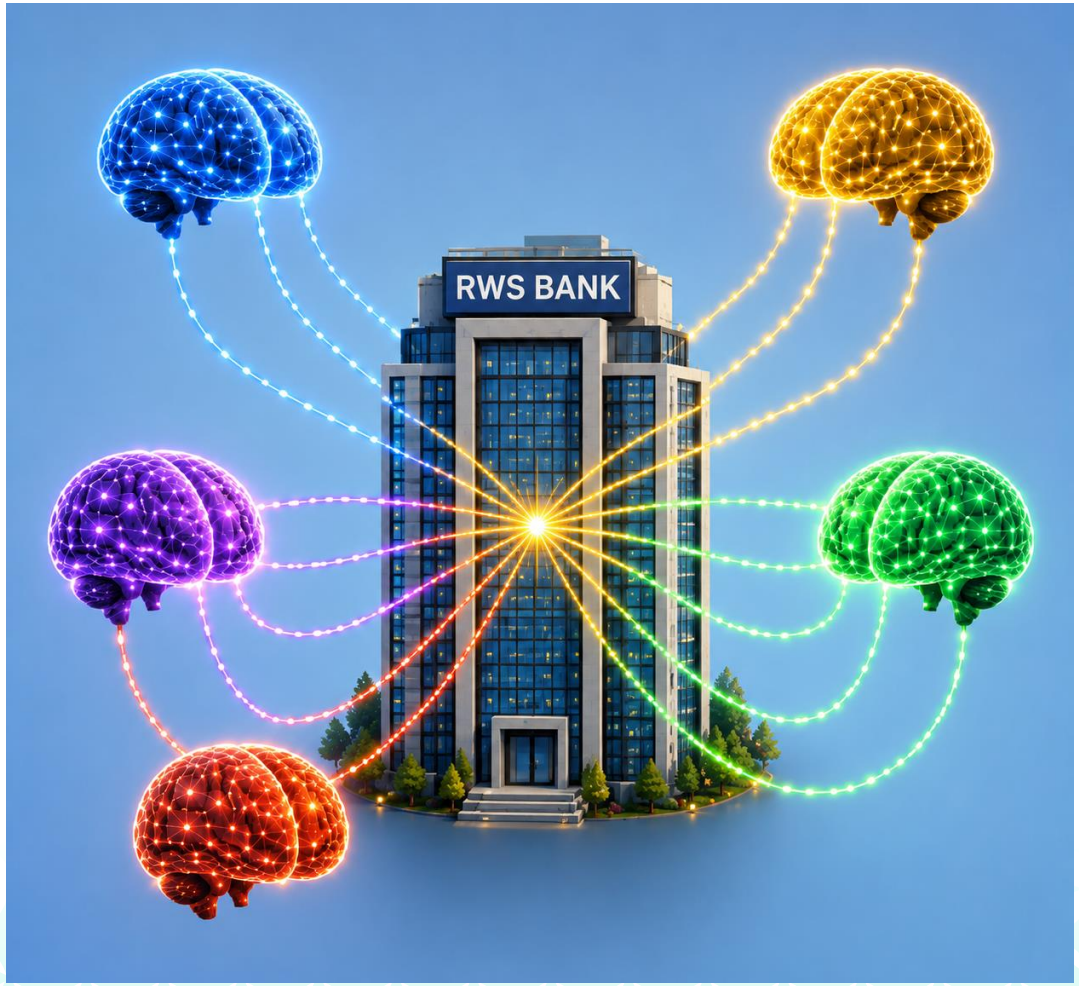
- AI model vendors are increasingly becoming more powerful and influential as they get closer to super intelligence capabilities
- As AI gets integrated into the fabric of every organization and economy in the world, the vendors will have significant economic power
- They can exercise this power by enforcing new restrictions on use of AI for specific use cases that may not align with ideologies of the vendors
- Anthropic exercised its power recently with US Department of War by restricting usage of its AI model for certain use cases

Mitigation Approaches

- Ensure explicit coverage of this risk in vendor contracts and preferred mitigation measures
- Utilize multiple AI vendors to reduce dependence on a single vendor
- Utilize open-source AI models or in-house AI models for subset of use cases to avoid this risk

9. AI risk exposures emerging from third parties

- Key risk exposures include:
  - Your AI strategy misaligned with AI strategy of key third parties (e.g., use of different AI models)
  - Third parties utilize AI for delivering their products/services without approval
  - Current contracts do not adequately cover AI risk exposures
  - Existing concentration risk amplified with small number of credible AI model vendors
  - Outages of AI models due to shortage of data center and electricity
  - Unexpected rise in cost of utilizing AI models (e.g., API costs, subscription fees)



Mitigation Approaches

- Renegotiate legacy technology contracts to address AI-specific liability exclusions, ensuring meaningful financial recovery for foreseeable AI-related losses
- Demand explicit AI-specific indemnities within vendor agreements, particularly regarding intellectual property infringement and data privacy breaches
- Require independent, third-party attestations (such as SOC audits) from vendors to verify the security and integrity of opaque or "black box" AI models
- Implement contractual requirements that legally compel third-party vendors to notify the institution before introducing new AI capabilities or substantially modifying existing models
- Incorporate clear data use rights and protection commitments into vendor agreements to ringfence client data and prevent unauthorized downstream usage for vendor model training
- Ensure procurement teams include interdisciplinary experts with AI-specific legal, technical, and risk-management skills to adequately assess complex vendor agreements
- Implement override rights and "circuit-breakers" within third-party contracts to ensure the institution can rapidly suspend or deactivate services during severe AI malfunctions without legal penalty

10. Systemic Risks

- Key systemic risk exposures include:
  - Mass unemployment (protests, civil unrest)
  - Rethinking of economic model, role of labor, capitalism, and role of organizations
  - Societal level changes (UBI, short working hours)
  - Volatility during the AI transition
  - Power outages due to electricity shortage and rising power costs (mainly due to AI data centers)
  - Severe shortage of resources such as data center capacity, servers, GPUs, memory chips
  - Threat of a rogue nation getting access to super intelligence capabilities

Mitigation Approaches

- Adopt systems thinking approach towards strategic and operational resilience
- Prepare library of plausible scenarios and utilize for testing resilience
- Participate in industry collaboration initiatives on AI risks
- Seek guidance from regulators on systemic risks
- Proactively monitor emerging AI risks

Key Emerging AI Risks

1. Malicious external actors utilizing AI
2. Disruption to strategy & operations
3. Disruption to organizational culture
4. Inappropriate use of AI within the organization
5. Shadow AI Systems
6. Unexpected behavior of AI models
7. Unexpected bankruptcy of key vendors
8. AI vendors restrict access for specific use cases
9. AI risk exposures emerging from third parties
10. Systemic Risks

Agenda

- AI & Generative AI (GenAI)
- Current State
- Key Emerging AI Risks & Mitigation Approaches
- Update Risk Management Frameworks & Processes
- Utilizing AI For Risk Management
- Q&A

metricstream

Update Risk Management Frameworks & Processes

Adopt recognized AI risk framework

- Adopt primary external AI risk framework instead of inventing this internally
- Recommended frameworks:
  - The NIST AI Risk Management Framework (released in January 2023 and updated in July 2024 for Generative AI)
  - US Treasury's Financial Services AI Risk Management Framework (published in February 2026). Translates above framework into 230 control objectives across four maturity levels
  - ISO/IEC 42001:2023 – Information technology - Artificial Intelligence - Management system (published in December 2023)
  - ISO/IEC 23894:2023 – AI Guidance on Risk Management (published in February 2023)

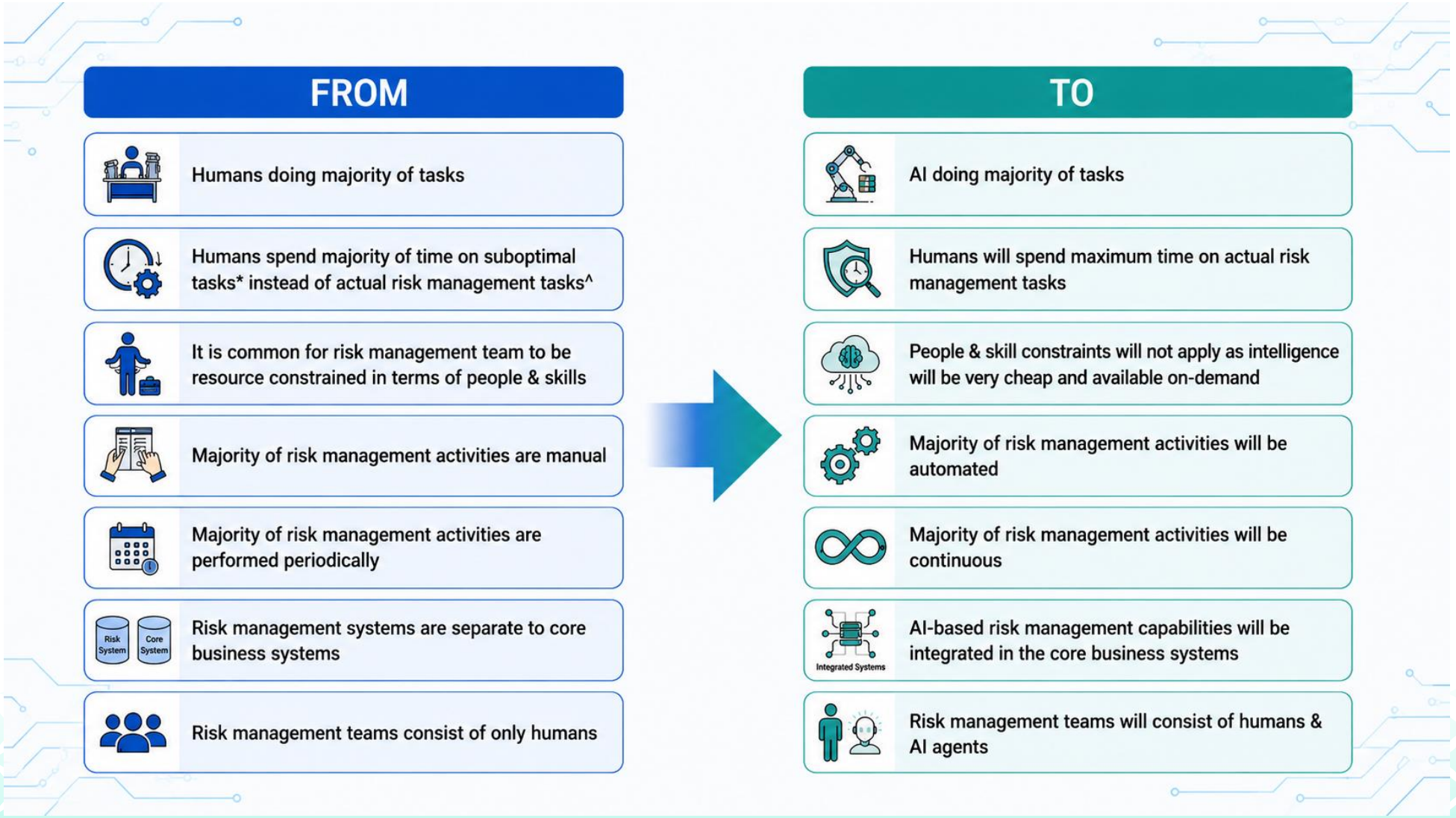
Update Risk Taxonomy

- Risk taxonomy should be updated to reflect AI topics.
- Do not create a new AI Risk Taxonomy. This will cause confusion and result in duplication of risk management effort.
- Consider
  - AI will be a causal factor for existing risks (e.g. cyber criminals utilising AI tools increases the sophistication of cyber attacks they can launch against financial services firms, AI deepfakes are used by fraudsters to commit external fraud).
  - New AI risks that should be added to the taxonomy (e.g. AI Washing, AI chatbot provides incorrect advice to customers resulting in mis-selling claims).

Create & Update Policies

- Create new AI specific policies
  - AI Governance and Responsible AI Policy
  - GenAI Acceptable Use Policy
- Update existing policies for AI topics
  - Enterprise Risk Management Policy
  - Operational Risk Policy
  - Model Risk Management Policy
  - Data Governance Policy
  - Data Privacy Policy
  - Information Security Policy
  - Cyber Risk Policy
  - Technology Risk Policy
  - Third-Party Risk Management Policy
  - Outsourcing Policy
  - Procurement Policy
  - Conduct Risk Policy
  - Complaints Policy
  - Operational Resilience Policy

GenAI Will Transform Risk Management



*compliance, documentation, follow-up, manage spreadsheets

^helping firm make risk-informed decisions & enable achievement of business objectives

Agenda

- AI & Generative AI (GenAI)
- Current State
- Key Emerging AI Risks & Mitigation Approaches
- Update Risk Management Frameworks & Processes
- Utilizing AI For Risk Management
- Q&A

metricstream

Utilizing AI For Risk Management

GenAI Benefits

1. Enhanced Productivity (Personal, Team, Organization)
2. Improved Risk Management Quality
3. Do More

Brainstorm Topics

- Help me identify risks for a new product
- Help me identify effective preventative controls for mitigating my risk
- Help me with list of sections I should include in a new Generative AI Usage policy

Enhance Data Quality

- Identify data quality gaps in current control library and address these
- Identify data quality gaps in risk library and address these
- Identify data quality gaps in RCSAs and address these

Analyse Content

- Analyse internal loss event data and identify insights
- Analyse control assessment results and identify weak controls
- Analyse emerging risk content and identify key actions to respond to these

Risk Management Use Cases

Check Content Completeness

- I have identified 7 risks for my process. Tell me if I have missed any key risks
- I have identified 12 controls for my risk. Give me feedback on these controls and any additional ones I should consider.
- I have drafted this Business Impact Analysis document. Review and provide feedback on whether I am missing any key topics.

Perform Deep Research

- Perform deep research on AI risks and mitigation strategies
- Perform deep research on operational resilience best practices
- Perform deep research on emerging third-party risks and mitigation strategies

Prepare Risk & Compliance Reports

- Identify key insights to include in reports
- Draft report content in consistent manner
- Create visual elements (bar charts, pie charts) for reports

AI Agents Enabling Automation

- Automate risk/control/KRI monitoring
- Automate monitoring and responding to emails from 1st line to 2nd line on risk related queries
- Automate monitoring of risk related business content (e.g. customer complaints, IT helpdesk request)

Draft Document/Presentations

- Draft a comprehensive control testing script for my control
- Prepare a presentation for risk committee members on a new regulation
- Draft content for a new policy

Create Risk & Compliance Training Content

- Create training video script on a topic
- Create training video on a topic
- Utilise AI Avatars and Voice Cloning from key stakeholders in training videos

Risk Management Use Cases

AI Agents Enabling Consistency

- AI agent to consistently respond on risk and compliance policies
- AI agent to provide guidance on risks and controls based on firm's risk framework
- AI agent to guide stakeholders on key risk and compliance topics

Draft Communication Content

- Draft email content to 1st line on changes to the risk management process
- Create images, posters, and infographics to raise awareness on a risk topic (risk culture)
- Draft response to regulators on key risk issues

Seek Best Practices & Guidance

- Evaluate my risk management process against ISO 31000 guidance and provide feedback on alignment
- Evaluate my information security controls against ISO 27000 and provide feedback on alignment
- Evaluate my risk appetite policy against Basel guidance and provide feedback on alignment

Operating Modes

- WorkIQ (enabled vs. disabled)
- Quick response vs. Think Deeper
- ChatGPT vs. Opus models
- Attach & Reference Content
- Temporary Chat
- Audio to Text Mode
- Voice Chat Mode
- Notebooks
- Desktop & Mobile App

AI Agents

- AI agents developed by users
- AI agents developed by Microsoft (Researcher, Analyst)
- Copilot CoWork (Skills, Professional Word, Excel, PowerPoint content)
- Personal vs. Team agents
- Configure basic context
- Configure advanced context
- Suggested prompts

Personalisation Features

- Memory
- Custom Instructions
- Chat History
- Manage Chats (rename, continue, delete)
- Prompt Library
- Brand Kits
- Pages
- Scheduled Prompts

Content Creation

- Text
- Tables
- Images
- Posters
- Banners
- Stories
- Infographic
- Draft Content
- Videos

Microsoft Copilot Functionalities For Risk Management

Copilot in Excel

- ChatGPT vs. Opus Models
- Local vs. Cloud Excel
- Select Sources (e.g. Web, Work)
- Edit Content, Plan, Chat Only Modes
- Create Content
- Analyse Content
- Prepare Dashboards & Reports
- Copilot Formula

Copilot in Word

- ChatGPT vs. Opus Models
- Local vs. Cloud Word
- Edit Content, Chat Only Modes
- Draft New Content
- Summarise Content
- Update Content
- Create Images

Copilot in PowerPoint

- ChatGPT vs. Opus Models
- Local vs. Cloud PowerPoint
- Edit Content, Chat Only Modes
- Create Presentations (on topics, from documents)
- Create Slide
- Update Slide
- Brand Kits
- Utilise Skills
- Create Images

Copilot in Microsoft Tools

- Outlook
- Teams
- Forms
- Edge browser
- SharePoint sites
- OneDrive folders & files

Use Case Demonstration

- OpRisk Advisor AI Agent
- Emerging Risk Analysis
- Dashboards & Reports in Excel
- Regulation & Policy Gap Analysis
- Generate Risk & Compliance Training Content

Agenda

- AI & Generative AI (GenAI)
- Current State
- Key Emerging AI Risks & Mitigation Approaches
- Update Risk Management Frameworks & Processes
- Utilizing AI For Risk Management
- Q&A

Q&A

Contact: manoj.kulwal@riskspotlight.com

GRC SUMMIT 2026
LONDON ✦ JUN 2-3

Thank You

Contact: manoj.kulwal@riskspotlight.com

Experience the **Power** of **AI** & **Resilience**

Hosted by **MetricStream**


metricstream