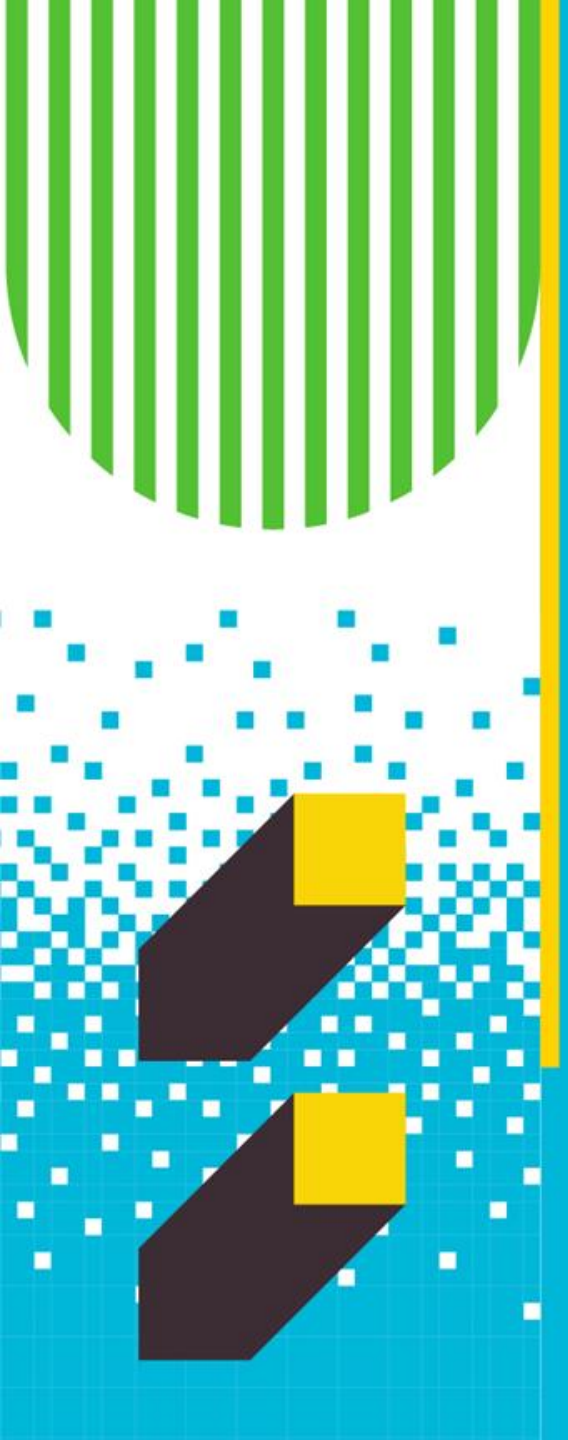


IAPP **Privacy. Security. Risk. 2025**

Training 28-29 October

Workshops 29 October

Conference 30-31 October

SAN DIEGO

#PSR25

NAVIGATING AI, PRIVACY, AND CYBERSECURITY:
An Integrated Risk Management Approach

WELCOME AND INTRODUCTIONS

Sasha Belyi, CIPP/US, CIPT, CISM
Director of Risk
Arity
sasha.belyi@arity.com

Michael Andry, Attorney
VP, Innovation, Data Analytics, AI
JPMorgan Chase
michael.andry@jpmchase.com

Susan Paulson, MBA, CIPP/US
VP, Governance, Risk, Compliance
Computer Aid, Inc. (CAI)
susan.paulson@cai.io

DISCLAIMER

The views and opinions expressed in this presentation are solely our own and do not represent those of our respective employers. This content is intended for information purposes only. This information is not advice on legal, investment, accounting, regulatory, technological, or other matters. In no event will the presenters be liable for any use of, or any decision made, or action taken in reliance upon this information.

OBJECTIVES

Delve into privacy and security **risks** associated with AI systems and importance of **ethical AI practices**

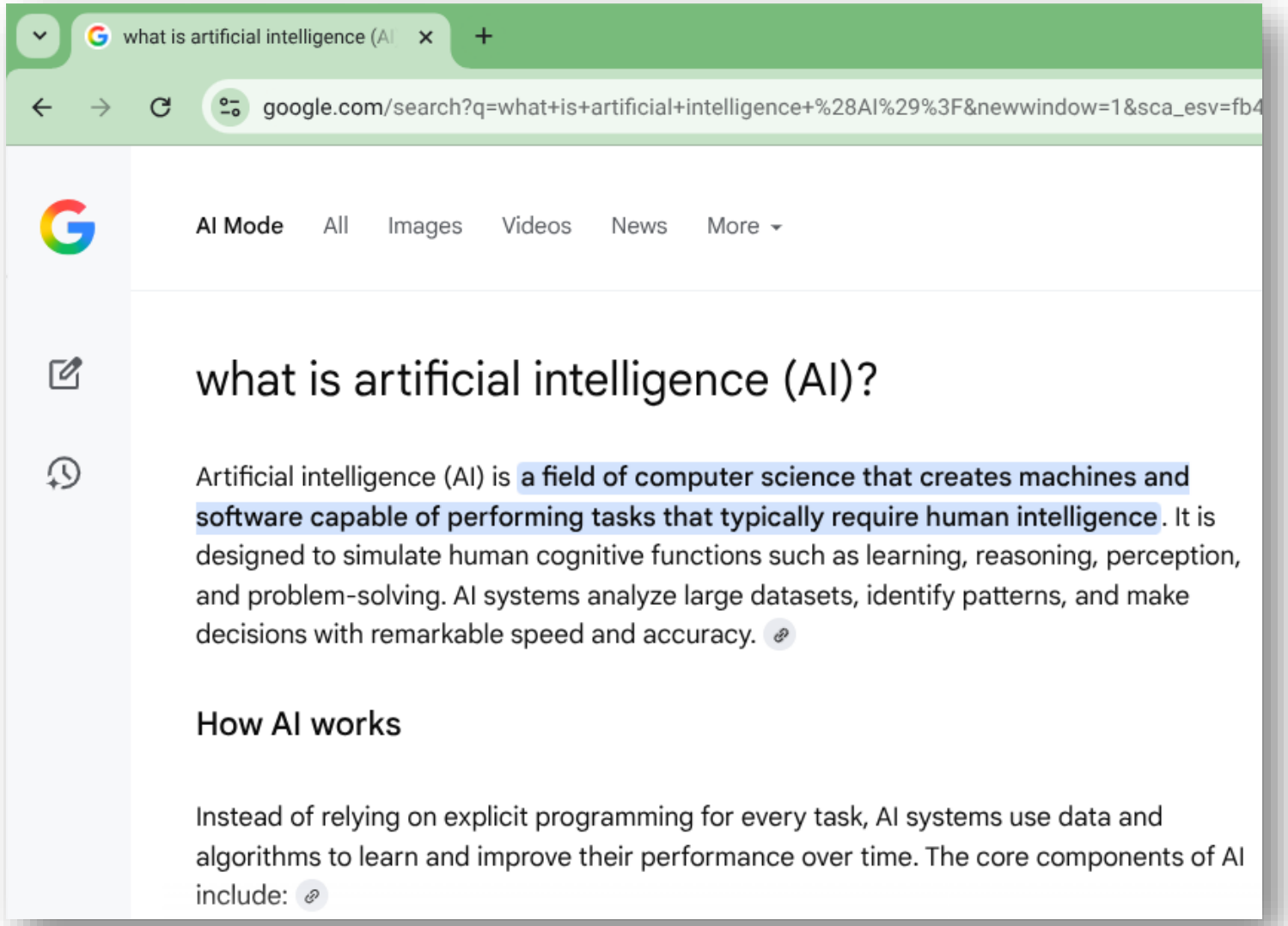
Discuss how to think about **emerging** AI technologies in the context of **risk management** programs

This session will:

Cover **strategies** for integrated risk management, focusing on aligning company practices with **consumer expectations** and **regulatory compliance**

Provide **practical insights** and actionable takeaways

WHAT IS ARTIFICIAL INTELLIGENCE?



IAPP COMMON PRINCIPLES OF RESPONSIBLE AI

Principle	Description
Fairness	Striving to eliminate bias and discrimination in AI systems and ensuring equitable outcomes for all users.
Safety	Creating guidelines and standards for development and use of AI systems.
Reliability	Ensuring that AI systems perform consistently and accurately over time.
Privacy	Protecting user data and ensuring that AI systems comply with privacy regulations and standards.
Security	Implementing robust security measures to protect AI systems from malicious attacks and unauthorized access.
Transparency	Ensuring that AI systems are clear and understandable, with their decision-making processes open to scrutiny.
Explainability	Ensuring that users can understand and interpret decisions made by AI ("black box").
Accountability	Assigning responsibility for the actions and outcomes of AI systems, making sure there is a mechanism to address any harm or issues that arise.
Human Centricity	Ensuring that humans retain ultimate control over AI systems, particularly in critical decision-making areas ("human in the loop").
Sustainability	Considering the environmental impact of AI systems and striving for sustainable use of resources.

Source: AIGP Body of Knowledge and Exam Blueprint

RISKS AUGMENTED BY AI

- Privacy and Confidentiality
- Data Security and Retention
- Misinformation/ Hallucination
- Bias and Fairness
- IP Concerns
- Ethics and Legal Liability
- Psychological/ Workplace Impacts
- Over-reliance and Skill Atrophy
- Model Drift and Availability

See details in the Appendix

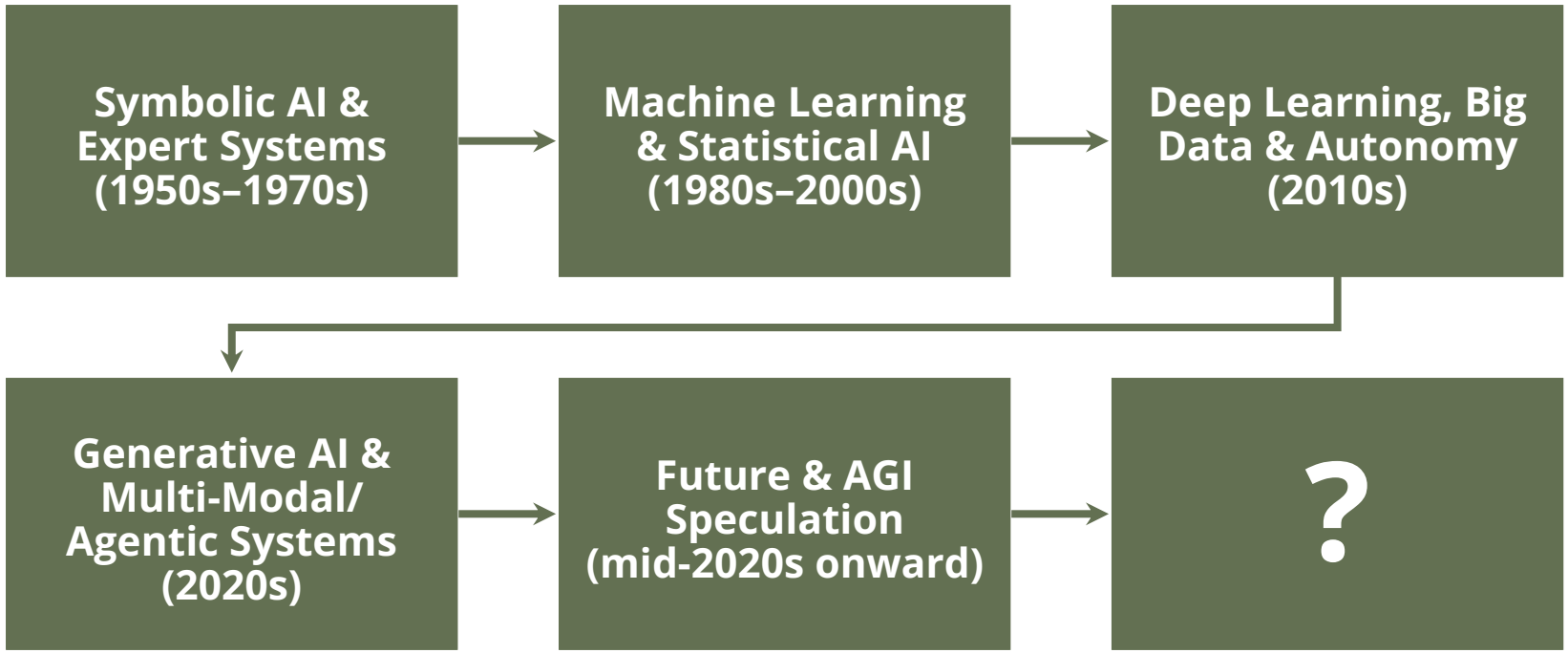
AI risk vs. traditional privacy and cyber security risks

RISK MITIGATION

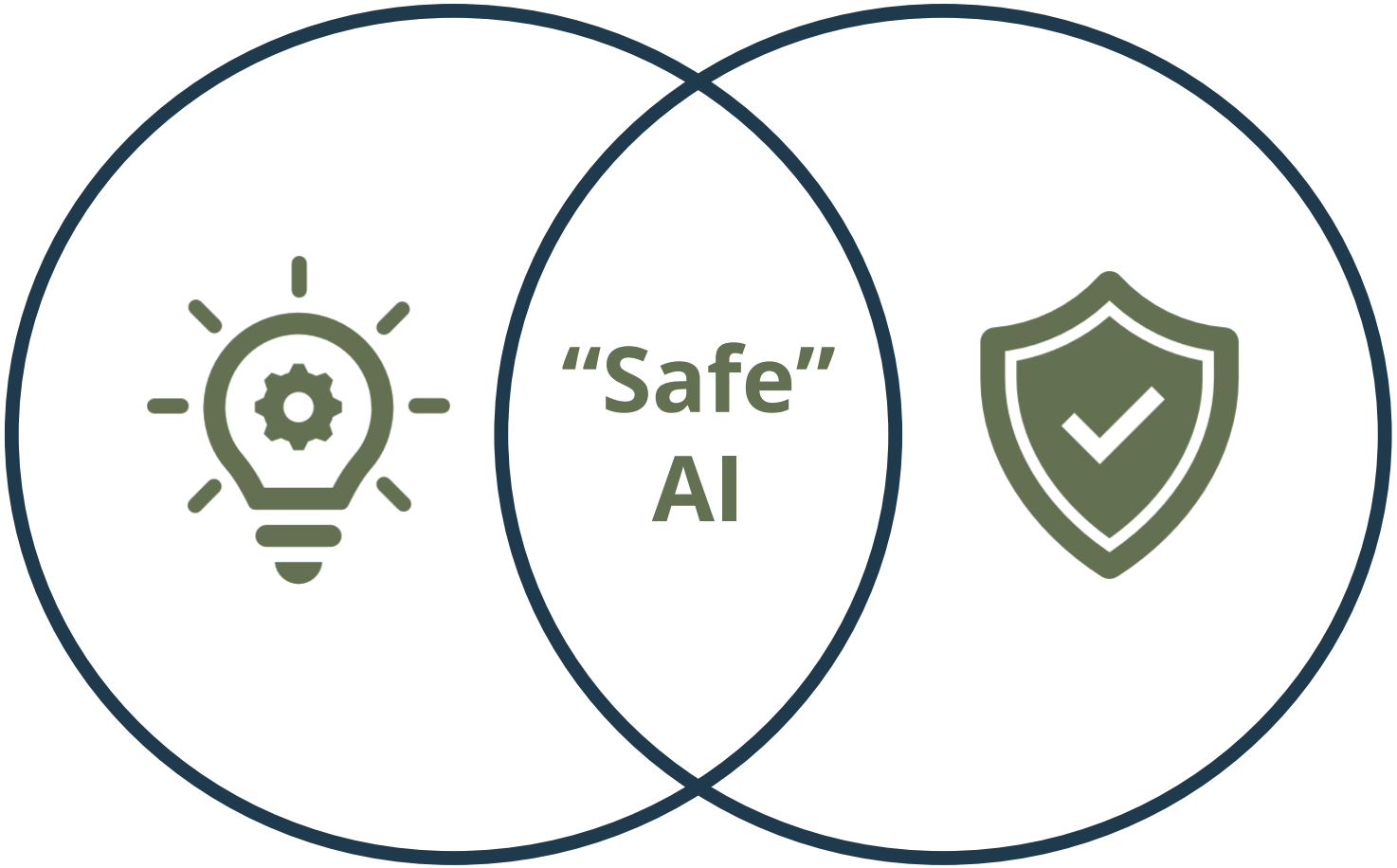
Risks	Mitigation
Privacy, Confidentiality, Security	Deploy a private instance that **keeps data in-network** with encryption in-transit and at rest. Mask, redact, **anonymize PI/PHI** before a prompt is sent, DLP style. Set **retention period** and dispose of data.
Data Quality & Accuracy	Establish **human in the loop** review for output that may be used for critical decisions or publication. Require **citation generation** and source checking. **Track hallucinations** through prompt/response QA.
Bias & Fairness	Implement **fairness testing** with sample personas to detect biased responses. Plan for and execute regular **monitoring and validation**.
Ethics, Legal Liability, and IP Concerns	Add contractual clauses that **address indemnification**. Educate users to prompt for and use credits.
Operational	Align controls to **existing frameworks** (NIST, COSO OECD, ISO, US AI RMF, etc.) Follow version and **change control processes** like with any other technology. Create **back up information** sources like FAQs and knowledge bases to use if AI is down. **Monitor** and audit usage, accuracy, access, etc.
Governance, Policy, Training	Create acceptable use and **ethical use policies**. Offer users **meaningful onboarding** process include how to best prompt the tools.

AI risk vs. traditional privacy and cyber security risks

EVOLUTION OF AI

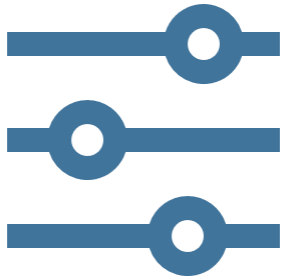


INNOVATION VS. RISK



A delicate balance of innovation with robust risk management

PRIVACY CONSIDERATIONS



It is important to prioritize **consumer privacy & choice** in AI risk management to maintain consumer **trust** with AI

AI GOVERNANCE FRAMEWORKS

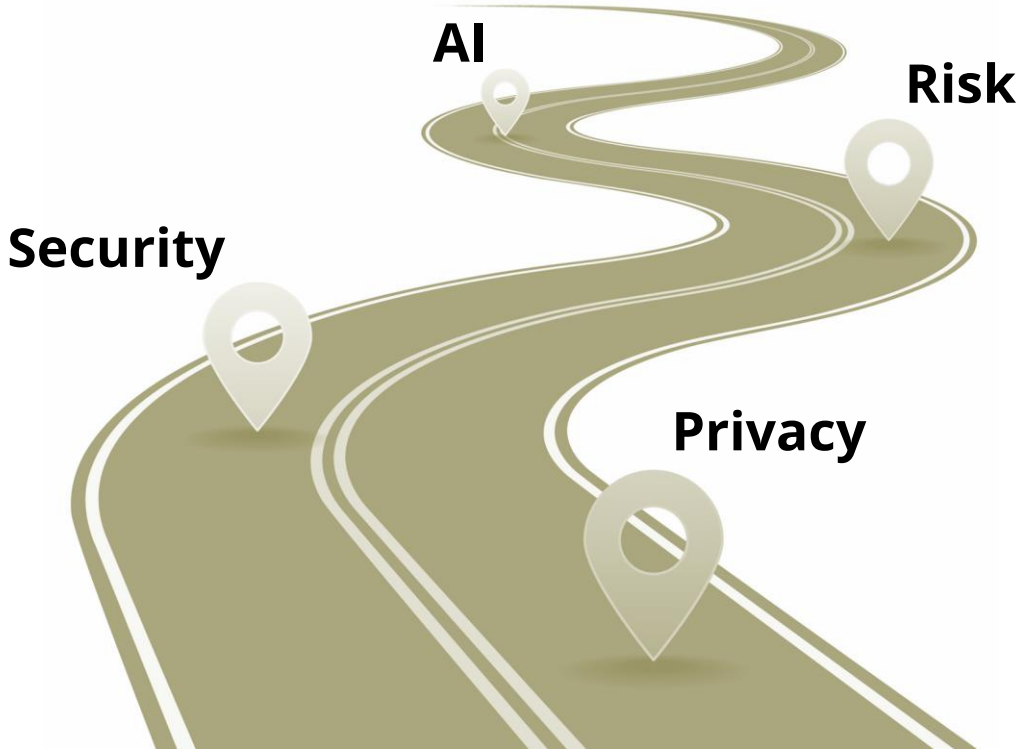
- ✓ NIST AI RMF
- ✓ NIST CSF 2.0
- ✓ COSO
- ✓ SOC 2 (AICPA)
- ✓ OECD Principles on AI
- ✓ EU AI Act
- ✓ ISO/IEC 42001

Best practices for integrating AI risk management into existing privacy and cybersecurity frameworks

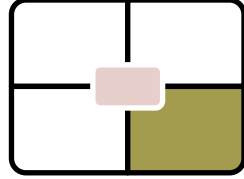
DRIVING BUSINESS VALUE

Integrating AI risk management with privacy & cybersecurity to deliver business value

LOOKING AHEAD



What steps should organizations take now to prepare for the evolving landscape of AI, privacy, and cybersecurity?



Questions?

How Did Things Go?
(We Really Want To Know)

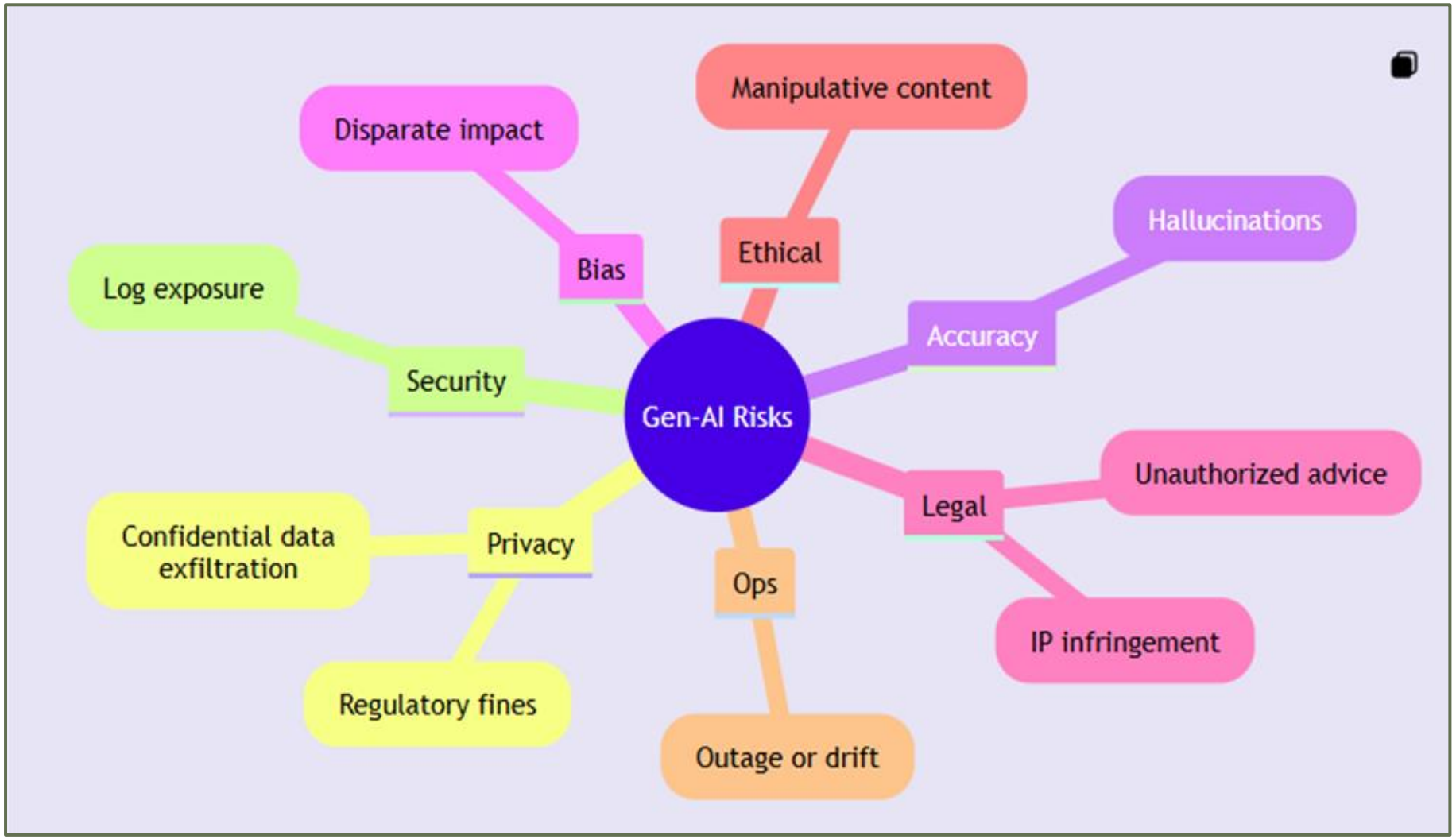
Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Privacy. Security. Risk. 2025**
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!

APPENDIX

AI SAYS THESE ARE ITS RISKS!



TRADITIONAL VS. AI-RELATED (BY RISK)

Risk Category	Traditional	AI-Related
Strategic	Market competition, strategic misalignment	AI-driven market prediction errors
Operational	Human error, supply chain interruptions, data quality, undocumented processes, inconsistent sales offerings	AI system errors, algorithmic bias in operational decisions, PI leakage, training data leakage, AI model hosting, use of AI in responding to RFPs, human error in implementation
Financial	Errors or fraud in reporting, exchange rate fluctuations, credit risk	Misjudgment in financial forecasting or decision making
Compliance	Compliance with laws and regs, contractual liabilities, unfavorable T&C in contracts	Compliance with laws and regs, challenges with immature AI regulation
Reputational	Brand damage, negative publicity	AI ethics violations, AI-generated misinformation, PI leakage
Technological	System failures, cybersecurity threats, malicious use, outdated systems, data breaches	AI model vulnerabilities, rapid tech obsolescence, IP control, malicious use, use in cyber attacks, data breaches
Third-Party	Vendor reliability, supply chain risks	AI misinterpretations of third-party data
Political	Political volatility, policy changes	AI influence on political processes
Environmental	Natural disasters, resource depletion	AI impact on natural resources

TRADITIONAL VS. AI-RELATED (BY ASPECT)

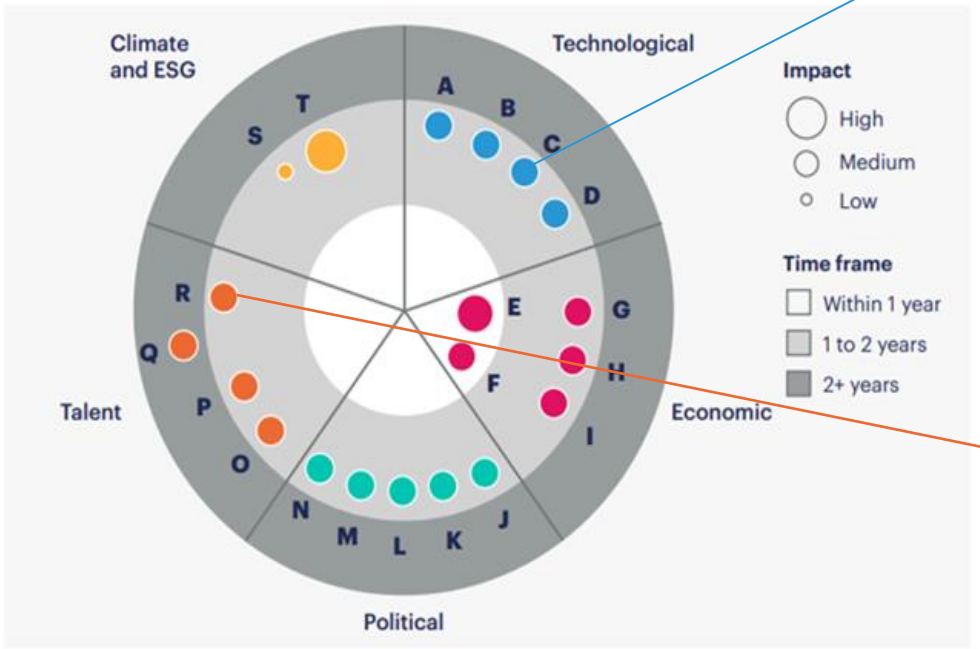
Aspect	Traditional	AI-Related
Nature of risks	Financial, operational, compliance, and strategic.	Bias, fairness, privacy, security, ethical considerations, and autonomy in AI systems.
Scope and focus	Enterprise-wide focus, integrating risk management with strategy and performance.	Emphasis on designing trustworthy AI systems and managing AI-specific risks.
Governance and culture	Establish governance roles and responsibilities for overall risk management.	Include AI-specific roles, promote awareness of AI technologies and associated risks.
Strategy and objectives	Align risk management with organizational strategy and objectives.	Integrate AI initiatives with organizational strategy, assess AI impact on risk appetite.
Performance	Monitor organizational performance through traditional metrics.	Use AI performance indicators, evaluate AI systems' impact on organizational performance.
Review and revision	Regularly review and revise risk management practices.	Continuously adapt AI risk management practices to evolving technologies and risk landscapes.
Information and reporting	Ensure transparent communication of risk management practices and outcomes.	Develop reporting mechanisms for AI risk-related incidents, share best practices.
Security and privacy	Focus on cybersecurity and privacy risks of information systems.	Ensure AI compliance with data privacy regulations, safeguard sensitive information.
Compliance	Adherence to regulations.	Voluntary use of AI RMF for trustworthiness considerations in AI systems.

GARTNER'S EMERGING RISK UNIVERSE MAP

Quarterly Emerging Risk Report

2Q25 emerging risk universe map

#	Risk category	Risk name
A	Technological	Agentic AI ☆
B	Technological	AI intellectual property control
C	Technological	Information-governance-driven AI risks
D	Technological	Misuse of data by state actors ☆
E	Technological	Escalating tariff and trade war
F	Technological	IT vendor criticality
G	Economic	Increased financial exposure
H	Economic	Low-growth economic environment ☆
I	Economic	U.S.-China decoupling ☆
J	Political	Anticorporate sentiment
K	Political	Deglobalization ☆
L	Political	New geopolitical partnerships
M	Political	Strained U.S.-Euro relations
N	Political	U.S. financial deregulation
O	Talent	Decline in employee productivity
P	Talent	IT workforce planning uncertainty ☆
Q	Talent	Retirement wave
R	Talent	Shadow AI ☆
S	Climate and ESG	Divergent ESG expectations ☆
T	Climate and ESG	Increased extreme weather frequency and severity



Note: Bubble placement within a ring does not indicate absolute time frame value.
Source: 1Q25 Gartner Emerging Risks Survey: n = 266
☆ = New to emerging risk universe in 1Q25

Source: Gartner's Quarterly Emerging Risk Report - 2Q 2025

Information-governance-driven AI Risk: "Risks related to weak information governance policies or practices that lead to unintended data feeding AI models, causing inaccurate results, legal or policy breaches, and privacy failures." Gartner says this risk is caused by the rapid pace of AI model adoption, lack of consistent global governance standards, and inadequate oversight of third-party data practices and may result in inaccurate and biased data outputs, IT deployment slowdown, and erosion of confidence in AI-enabled technologies.

Shadow AI: "The risk that employees use unauthorized AI tools and applications outside of their organization's approved framework, which can lead to data breaches, compliance issues, inconsistencies, or reputational damage." Gartner says this risk is caused by unrestricted access to advanced AI tools, increased productivity pressure, and inconsistent policy enforcement and may result in loss of IP, increased unmonitored vulnerabilities, and legal/compliance/reputational risks.

Symbolic AI & Expert Systems (1950s–1970s)

- Early rule-based AI systems (e.g., Dendral, MYCIN) relied on human-coded rules to emulate expert reasoning.
- Transparency risk was low—systems were simple and interpretable, with no major data protection laws.
- Privacy/Security concerns were minimal due to limited datasets and internal-only usage.
- Accountability was straightforward—decision logic was fully documented.
- *Citations: picloud.ai, thehistory.tech*

Machine Learning & Statistical AI (1980s–2000s)

- Shift to algorithms learning from data (e.g., decision trees, Bayesian networks).
- Privacy risks increased as datasets grew—U.S. Privacy Act of 1974 proved insufficient for large-scale automated data processing.
- Fairness risks emerged as biased training data could perpetuate inequities.
- Accountability decreased—harder to trace outputs to specific rules.
- *Citations: humanizeai.io, globalaivision.com, en.wikipedia.org/wiki/Privacy_Act_of_1974*

Deep Learning, Big Data & Autonomy (2010s)

- Rapid adoption of deep neural networks driven by GPUs, big data, and breakthroughs like AlexNet (2012) and AlphaGo (2016).
- Transparency and Explainability risks grew as models became 'black boxes'.
- Privacy regulations like GDPR (2018) and CCPA (2020) expanded consumer data rights, but compliance was challenging for opaque AI systems.
- Security vulnerabilities (adversarial attacks) became more complex.
- *Citations: datainsidetech.com, rand.org*

Generative AI & Multi-Modal/ Agentic Systems (2020s)

- Emergence of large language models (LLMs) and multi-modal systems capable of text, image, and code generation.
- Transparency and Security addressed by the EU AI Act (2024) requiring risk assessments and disclosures.
- Privacy risks now include deepfake misuse, IP infringement—laws like Tennessee ELVIS Act and California AB 2013 target these concerns.
- Fairness and Accountability addressed through algorithmic impact assessments, audits, and traceability mandates.
- *Citations: en.wikipedia.org/wiki/Artificial_Intelligence_Act, safecomputing.umich.edu, investopedia.com*

Future & AGI Speculation (mid-2020s onward)

- Research moves toward Agentic and potentially 'Conscious' AI (AI 4.0).
- Safety, Human-Centricity, and Accountability will be critical for autonomous decision-making systems.
- Governance gaps expected—current legal frameworks may not anticipate self-directed AI behavior.
- *Citations: arxiv.org/abs/2502.11312*

LEGAL RISKS AND RELATED PRINCIPLES (1)

Risk	Related AI Principle	Relevant Regulations / Frameworks	Pending or Active Legal Matters
AI "washing" / False Claims	Transparency / Accountability	FTC Act (Section 5), emerging AI disclosure standards	Multiple securities fraud class actions in 2024 over misleading AI capability claims (Heller, Reuters)
Unauthorized use of personal or copyrighted data for training	Privacy / Accountability / Fairness	EU AI Act, proposed AI Accountability & Personal Data Protection Act (U.S.)	Numerous copyright lawsuits (Getty vs. Stable Diffusion; Times vs. OpenAI; Disney vs. Midjourney), plus a June 2023 OpenAI scraping lawsuit (Wikipedia, New York Post)
Input data misuse by AI vendors (e.g., confidential/PII reuse)	Privacy / Security	GDPR, CCPA, general data processing agreements	No major lawsuits yet, but rising concern in vendor agreements (AMBART LAW PLLC, JD Supra)
Algorithmic bias and discriminatory outcomes	Fairness / Human-Centricity	EU AI Act (bias audits), GDPR's fairness obligations	Growing regulatory focus; DISCUSSION but not yet high-profile lawsuits (Wikipedia, Investopedia)
Lack of governance around autonomous AI agents	Safety / Accountability	EU AI Act (high-risk obligations), state AI regulations	Early litigation not yet; risk frameworks under development (Reuters)

LEGAL RISKS AND RELATED PRINCIPLES (2)

Risk	Related AI Principle	Relevant Regulations / Frameworks	Pending or Active Legal Matters
Privacy violations via biometric or surveillance AI (e.g., facial recognition)	Privacy / Security	GDPR, state biometric privacy laws	Clearview AI fined and banned in EU for privacy breaches (Wikipedia)
Federal investigations into data practices	Privacy / Transparency	FTC laws against unfair practices	FTC investigation of OpenAI for data security and false output concerns (Wikipedia)
Regulatory fragmentation & compliance burden	Accountability / Reliability	Patchwork of state laws, slow federal action	Tech industry pushing for federal AI law amid regulatory uncertainty (The Wall Street Journal)
Legal ambiguity about AI-generated content ownership	Accountability / Explainability	U.S. Copyright Act (human authorship doctrine), evolving case law	Lawsuits questioning copyright status of AI outputs; ongoing judicial scrutiny (Wikipedia)
Operator liability for AI-generated harms	Accountability / Safety	Emerging state liability frameworks	The "AI Accountability and Personal Data Protection Act" introduced to address liability (New York Post)