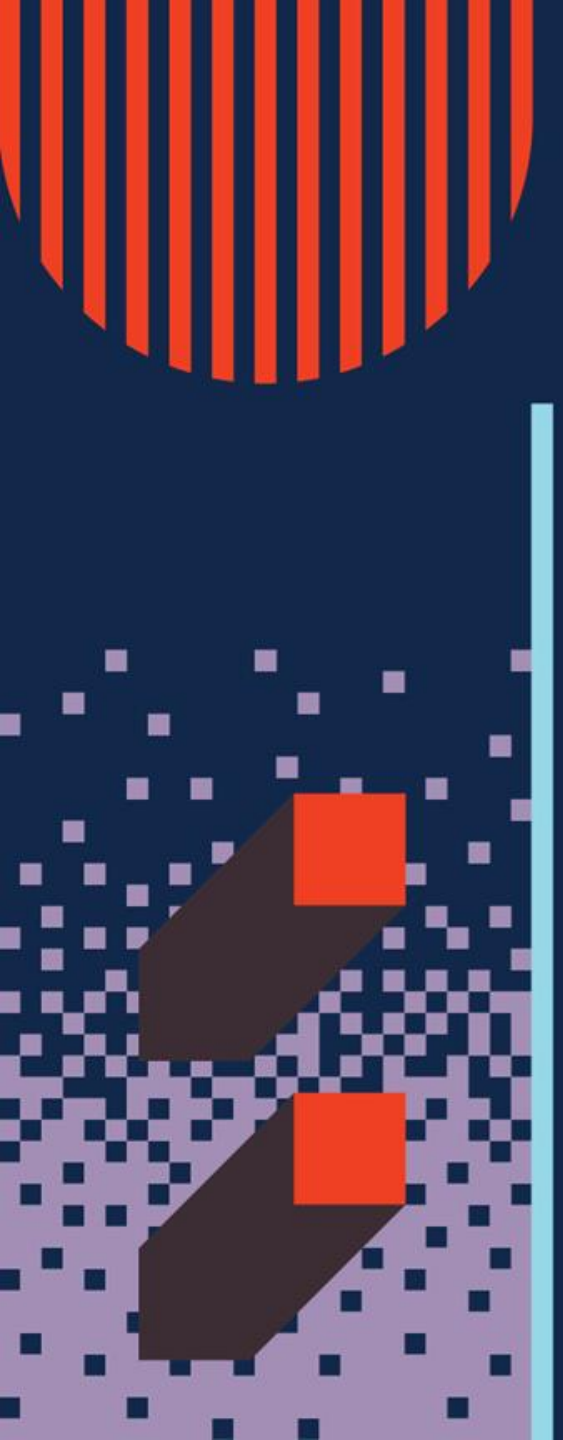


IAPP **AI Governance Global North America 2025**

Training 16-17 September

Workshops 17 September

Conference 18-19 September

BOSTON

MAD DASH TO AI:

How to Slow Your Vendors' Roll

WELCOME AND INTRODUCTIONS

Emily Choi-Greene
CEO & Co-Founder
Clearly AI

Robin Andruss
Director, Data & AI Privacy
PayPal

Jim Gregoire
Senior Director, Privacy and AI Governance
Rivian

Today we'll cover

Reality

- AI is commonplace in enterprises and in vendor tooling
- Governance is behind adoption
- Vendors are rolling out AI at lightning speed… often without adequate controls
- Shadow IT makes the problem worse

Risks

- AI-specific risks
- AI-exacerbated risks

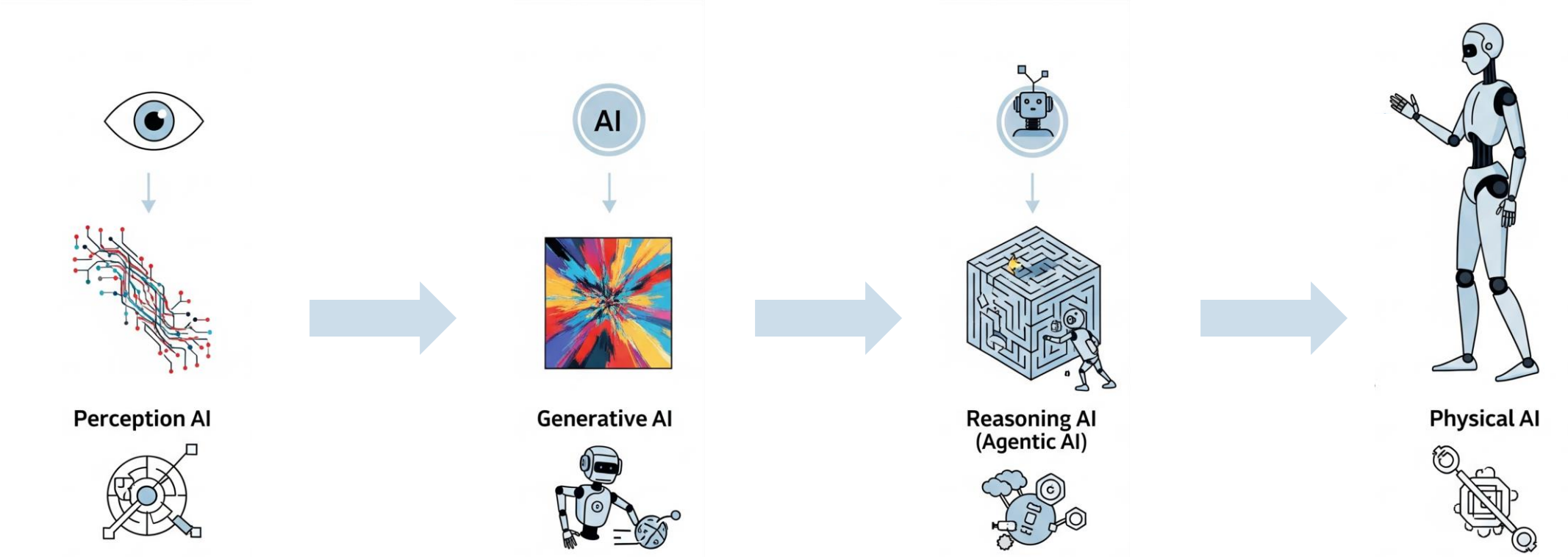
Recommendations

- Risk-based AI assessments
- Building an AI governance program
- Checklist for vendor reviews

The state of the market today

Reality

NVIDIA CEO's Prediction: Stages of AI



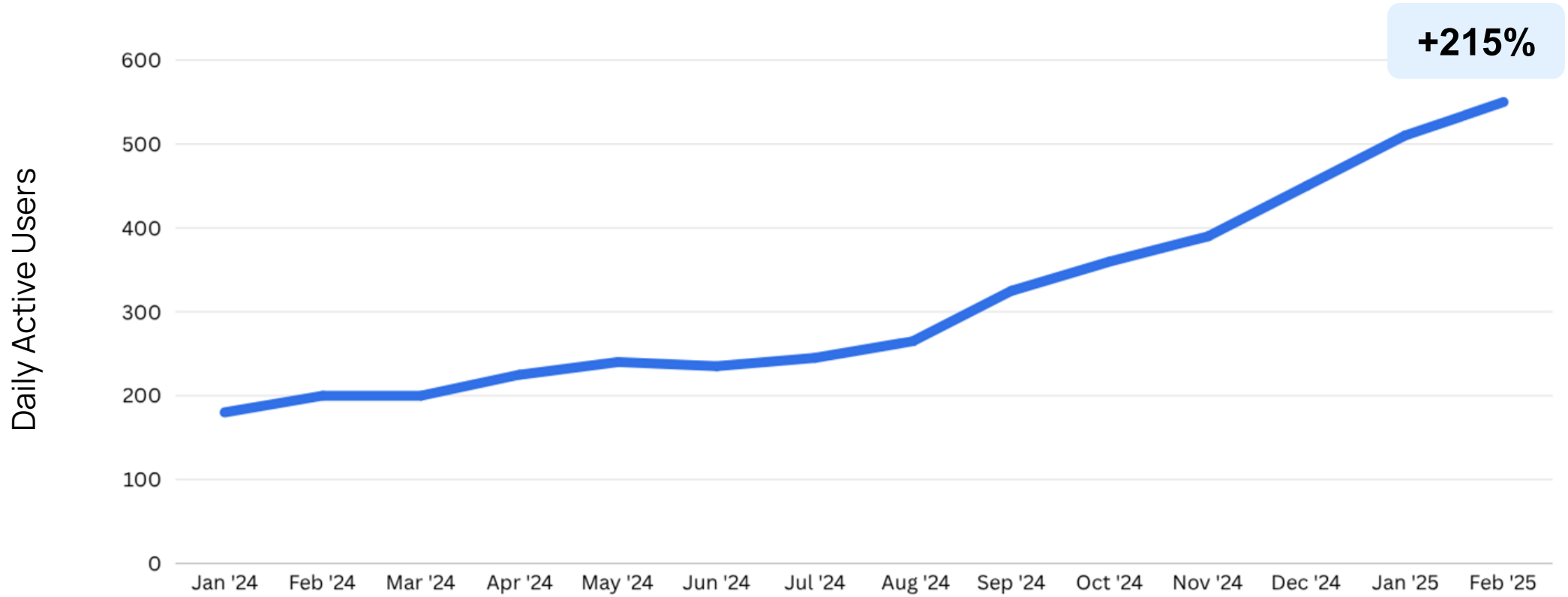
Machines gaining the ability to perceive and understand information. Included advancements in tasks like computer vision for image recognition and speech recognition.

AI models can generate new content in various formats like text, images, and code.

The era of "Reasoning AI" or "Agentic AI", where AI agents can reason, plan, and act autonomously, acting as "digital workforce robots" capable of independent decision-making and collaborating with humans.

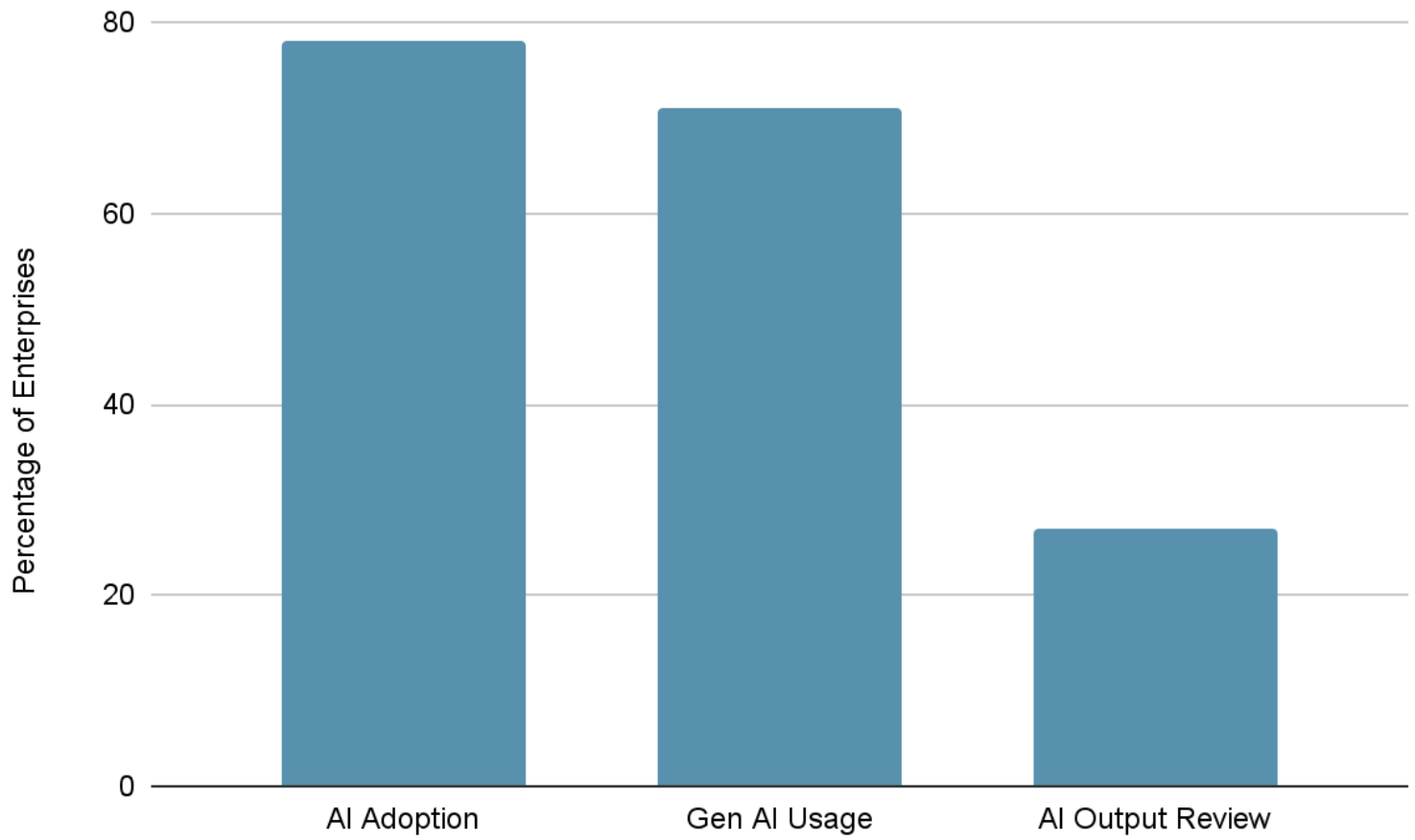
AI systems interact directly with the real world. This includes applications in areas like robotics and autonomous vehicles, requiring AI to understand concepts like physics, friction, and cause and effect.

Agentic software adoption



Data from Microsoft

AI implementation is significantly outpacing AI governance



Reality Check:
Vendors Ship First, Clarify Later

"WHERE IS THE OPT-OUT BUTTON?"

Slack users horrified to discover messages used for AI training

Slack says policy changes are imminent amid backlash.

ASHLEY BELANGER – MAY 17, 2024 11:10 AM | 103

Home > Digital > News

Aug 7, 2023 11:07am PT

Zoom Says It's Not Stealing Customer Content to Train AI Models

By Todd Spangler

LinkedIn accused of using private messages to train AI

22 January 2025

Share

SLATE

News & Politics Culture Technology Business Life Advice Podcasts

WEIGHING IN ON THIS NEW LINE DRAWN IN THE SAND

Search Light

USERS

Adobe Swears It's Not Training Its A.I. on Your Photoshops

But Creative Cloud needs "some degree" of omniscience.

BY SCOTT NOVER

JUNE 07, 2024 • 3:30 PM

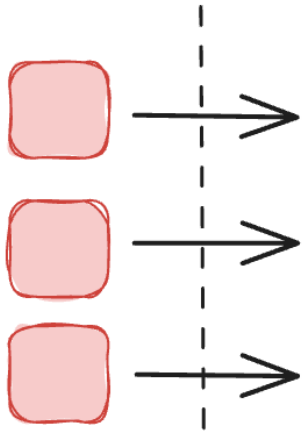
Figma's AI app creator accused of ripping off Apple weather app

Company pulls Make Designs after requests to design weather app result in program 'almost identical' to iOS app

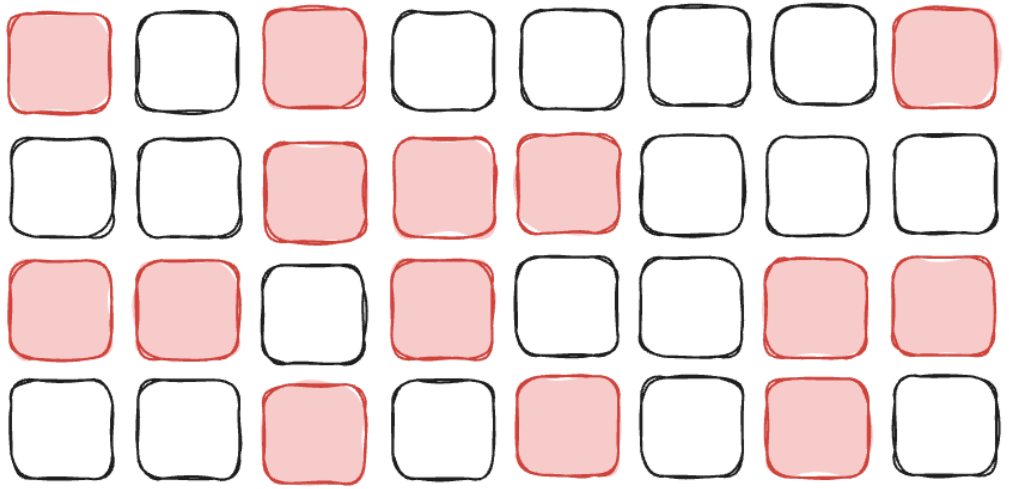
#AIGG25

Existing vendor are the largest concern

New vendor intake



Existing vendor population



AI introduces new risks and exacerbates existing issues

Risks

The Sad Facts…

- **Confidence vs. Reality:** While 90% of organizations feel confident about their security and 91% believe their employee training works, the actual results don’t match this optimism.
- **Frequent Attacks:** Over half reported regular malware attacks, phishing scams, and data breaches — often caused by poor use of AI tools.
- **AI-Related Data Leaks:** 68% of organizations have faced data leaks from employees sharing sensitive information with AI systems.
- **Lack of Policies:** Despite these risks, only 23% have strong AI policies in place.

Source: https://www.securitymagazine.com/articles/101773-68-of-organizations-experienced-data-leakage-from-employee-ai-usage

Top 5 AI-Specific Risks

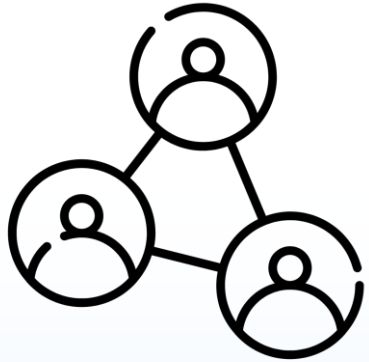
1. **Lacking defense in depth**: AI systems could be vulnerable to adversarial attacks, data poisoning, or other security threats that compromise their integrity. Multiple layers of defense are missing.
2. **Training on your personal/sensitive/proprietary data:** Use of data without proper consent/processing.
3. **Model development purely with a utilitarian perspective:** AI models can perpetuate or amplify societal biases, leading to unfair or discriminatory outcomes for certain groups.
4. **Lack of monitoring/testing:** Effective monitoring and governance processes are essential to mitigate the risks posed by rapidly evolving AI technologies. This should be a central focus of any comprehensive AI risk management program.
5. **Lack of transparency:** it can be difficult for users to understand how the model works, what data is being used, and how AI may influence decision making.

Hidden AI Risks
AI Makes Existing Problems Worse

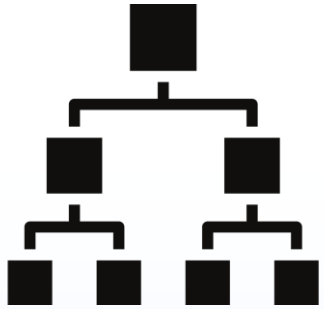
Shadow IT

Information discoverability (enterprise search)

Access Control



Low-Trust Agentic Systems



Unclear data lineage / ownership / permissions

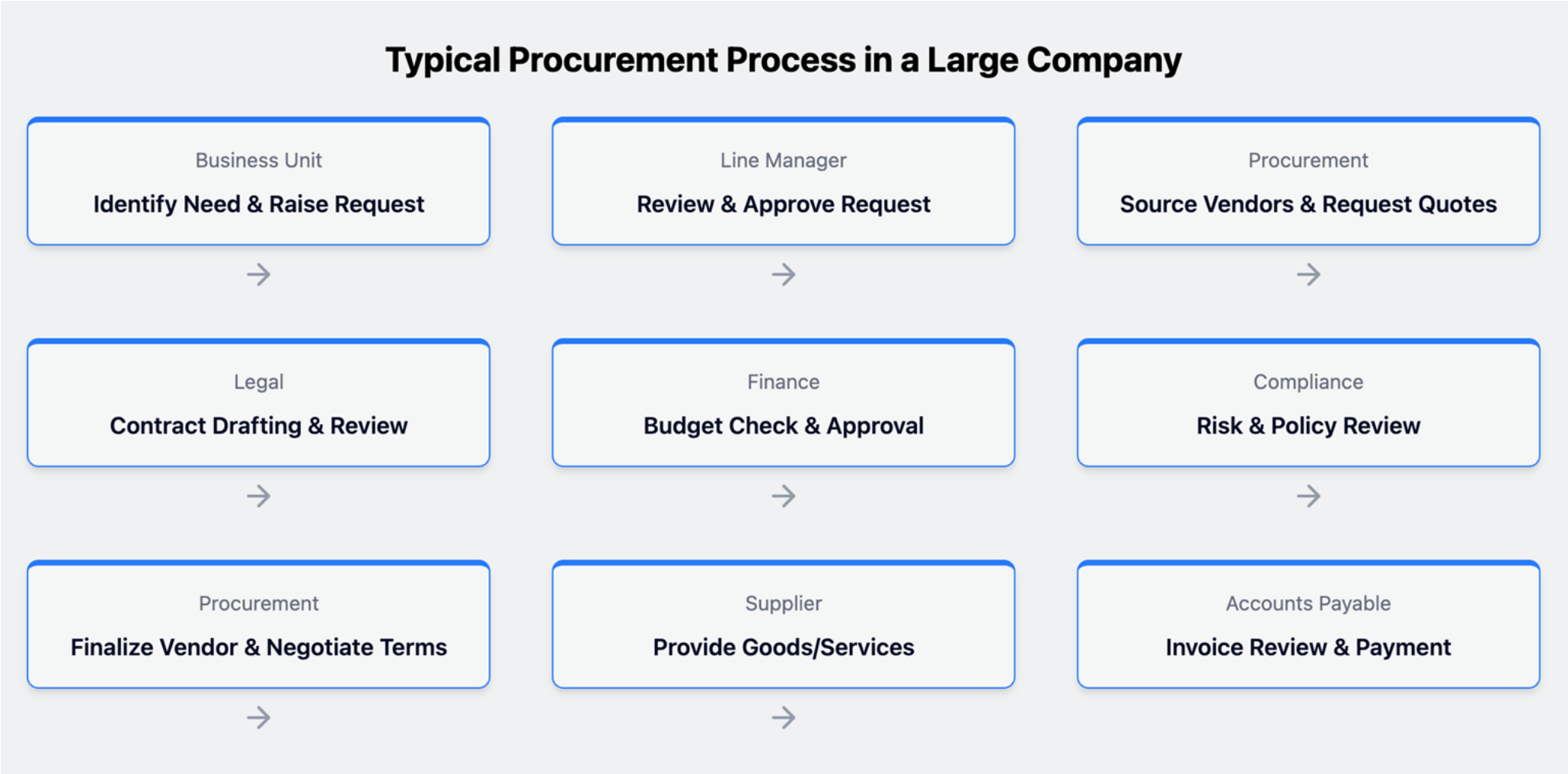
Enable the business to use AI safely

Recommendations

Example AI Governance Program Framework

Roles & Accountability	• AI Governance strategic plan • AI Governance Principles • AI Working Group • AI Committee
Policies & Procedures	• AI Risk Management Policy • AI governance guidance, standards, procedures
Training & Awareness	• Foundational AI training (upon hire & annually) • Ongoing awareness (e.g., intranet, email updates, announcements, guidance) • Periodic events
Risk Assessment	• AI risk, compliance, and governance counseling • AI risk reviews • AI testing and validation
Monitoring & Reporting	• Metrics & KPIs • AIG Program Dashboard

What makes managing vendor risk especially hard...



Organizational design & culture

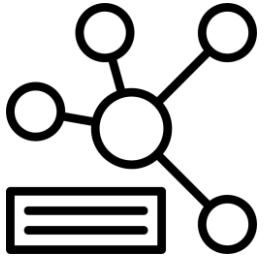
Communication: Internal forums (e.g., Slack channel) to foster discussion

Training and awareness: formal courses, campaigns, events, etc.

New hire onboarding: Mandatory training and policy acknowledgment upon hire

Tone-from-the-top: Executive messaging via email and company All Hands

Cross-functional collaboration: Regular outreach to key groups (e.g., Procurement, IT, engineering teams); cross-references in forms

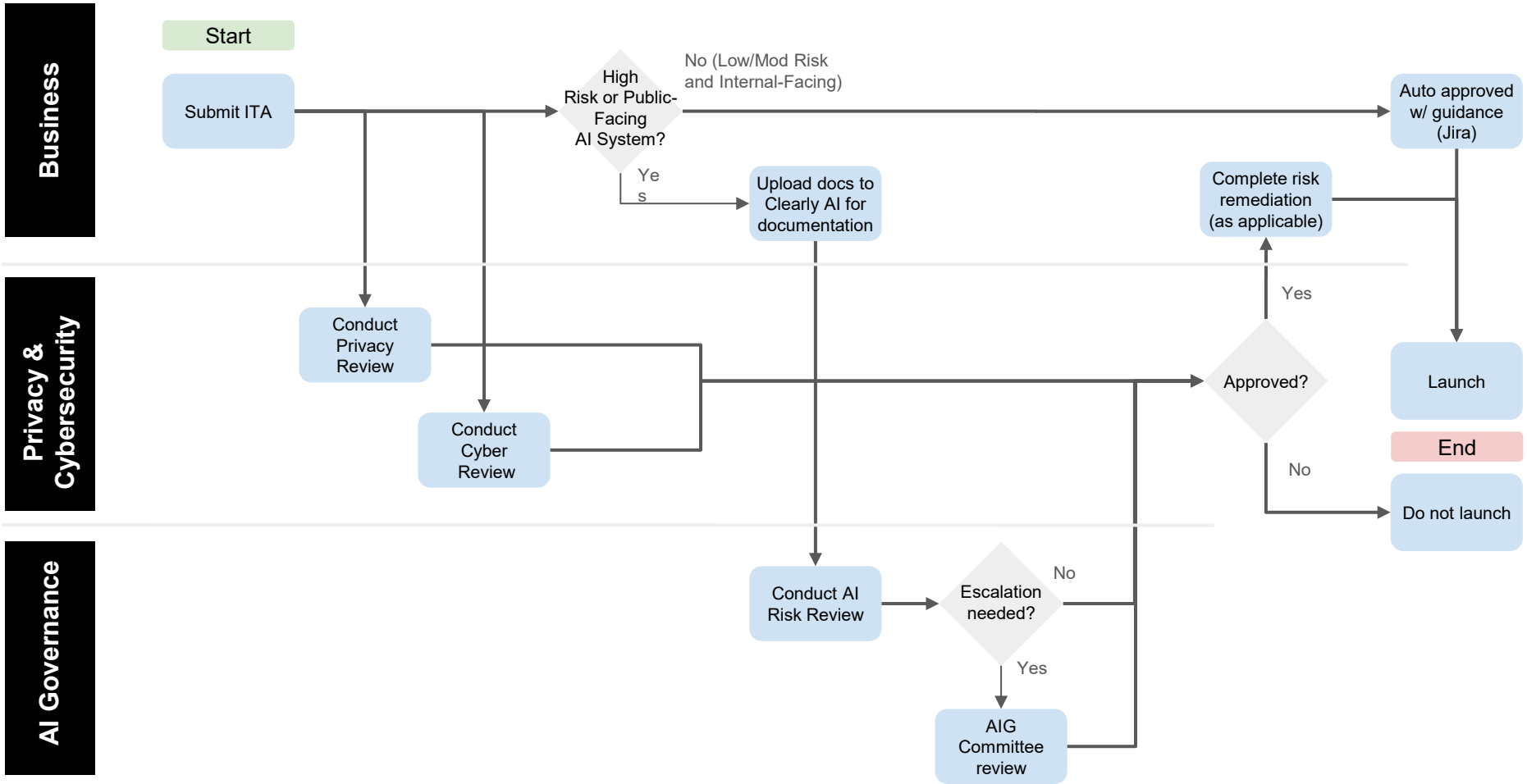


Technical solutions: e.g., data mapping solutions that can identify integrations with AI models

Risk Assessment Guidance and Process

- **Develop comprehensive AI policies and standards** - Codify organizational principles, guidelines, and requirements for the responsible development and deployment of AI systems.
- **Establish cross-functional governance structures** such as AI Working Group and Governance Committee
- **Define clear risk appetite and tolerance levels for AI systems at the company-level** (e.g. low-risk internal tools vs high-risk public-facing systems)
- **Implement a structured risk assessment process** (next slide) that is repeatable involving checklists, risk scoring, and escalation procedures
- **Enhance technical capabilities for AI monitoring and testing** - Invest in tools and expertise. Thoroughly test before deployment.
- **Leverage external assessments and certifications (longer term)** - Consider third-party evaluations or industry certifications to validate the robustness of AI governance practices

Example AI Risk Review Process



AI Risk Reviews: Low & Moderate Risk

1. **Public Interest**: The system must provide a public benefit that outweighs the risks to the public.
2. **Ethics**: The system output must be fair, just, and aligned with company morals and values. The system must be accessible to users with disabilities and output must not discriminate against users.
3. **Transparency**: Users must be informed that they are interacting with an AI; AI-generated content must be labeled.
4. **Model Training**: Personal/identifiable, proprietary, and confidential data must not be used for model training without AIG team approval. We must be able to delete the personal data used for training upon user request.
5. **Data Minimization**: Input/output data must be limited to the minimum necessary and deleted when no longer necessary.
6. **Input Data**: May not include sensitive, proprietary, trademarked, or copyrighted data without license, permission or consent. Ensure that the AI system has the requisite IP rights/protections to limit company IP risk.

AI Risk Reviews: High-Risk

AI System Details

- AI System Name
- Description & Benefit
- Deployment
- Stakeholders
- Team Responsible
- Third Party Name (if applicable)
- Third Party POC
- Roles and Responsibilities

Plan & Design

- Data Flows, Governance, Quality
- Risk Tolerance
- Trustworthiness

Verify & Validate

- Pre-Deployment System/Model Training
- Validation & Testing

Deploy & Use

- Data Collection
- Legal Basis
- Ongoing Model Training

Operate & Monitor

- Human Oversight
- Reporting & Metrics
- Maintenance

Recordkeeping

- Logging
- Technical Documentation
- Export Controls
- Deployment Instructions
- EU Registration

AI Guardrail Checklist for New Vendors

- ☑ **Transparency:** explainability; source citations; model architectures
- ☑ **Explicit, revocable opt-ins:** for any training on Customer Content or metadata; no cross-customer learning; opt-in to different features
- ☑ **Human-in-the-loop:** configurability; autonomous system guardrails
- ☑ **Data handling:** who can view prompts/outputs; retention & redaction policies
- ☑ **IP & indemnity:** warranty on training data provenance; IP indemnity for AI-generated outputs
- ☑ **ToS & subprocessor controls:** 30–60 days' notice on change; zero-day retention; API key substitution
- ☑ **Data retention & deletion:** time-boxed logs/prompts; purge at termination; EU AI Act commitments if applicable

In conclusion

The **Reality** is… AI is not going away.

- AI-specific risks related to model training, ethics, and transparency are just as important as risks like access control, DLP, and data lineage concerns.
- Privacy, security, and GRC teams need to adapt, not act as blockers.

Risks can be managed, but not eliminated.

- Even with the best risk management program, there will always still be some risk.
- Taking a risk-based approach can help teams approve low-risk use cases fast (even automatically).

Our **Recommendations** are to.

- Implement risk-based AI assessments.
- Build an AI governance program that covers common concerns in a repeatable, reliable manner.
- Augment existing vendor reviews with AI-specific guardrail checks.

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 AI Governance Global North America 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!