

iapp

Demystifying AI Data Risk Informed Risk Tiering in Regulated and Non-Regulated Industries

Wednesday, 13/November/2024

08:00-09:00 PST

11:00-12:00 EST

17:00-18:00 CET

Welcome and Introductions

Panelists



Jay Cline
Principal, Data Risk &
Privacy
PwC



Andrew Bouta
Director, Data Risk &
Privacy
PwC



David Ray
CIPP/US, CIPM, CIPT
CPO
BigID

Agenda

1. The Growth in AI
2. Risk Tiering Methodology
3. Dashboards & Examples
4. How Can Technology Help

The Growth in AI

Growth in AI has been astronomical over the last decade. This is reflected across a broad variety of domains as evidenced below via a small set of examples.

Domain	2010	2020	2022	2024
Largest Model Size	~100 million (Deep Belief Networks)	175 billion (GPT-3)	1 trillion+ (PaLM)	2 trillion+ (estimated for GPT-5, Gemini 1)
Investment in AI (Global Market)	~\$1 billion	~\$50 billion	~\$92 billion	~\$110 billion
AI Research Papers Published	~10,000	~90,000	~130,000	~175,000
AI Talent Pool (global)	~25,000	~300,000	~500,000	~750,000
Compute Power (Training FLOPS)	~1e14 FLOPS	1e19 FLOPS	5e20 FLOPS	5e21 FLOPS
Carbon Footprint per Large Model Training	Minimal	~200 tons CO ₂ (GPT-3)	~1,000 tons CO ₂ (PaLM)	~3,000 tons CO ₂ (latest)

The Growth in AI

Uses of AI are transforming rapidly. AI technologies are being adopted at rapidly increasing rates for a variety of purposes benefiting many industries. These uses are dramatically seeking to address risks and having impacts across people, processes, and technologies. Several such use cases are outlined below:

Use Case	% of AI Including This Use Case	People Mitigation	Process Mitigation	Technology Mitigation
Customer Service Automation	85%	Establish ethics committee for oversight	Develop AI guidelines for fair customer interactions	Implement monitoring tools for conversational AI
Supply Chain Optimization	70%	Create a compliance team	Conduct regular regulatory audits	Implement regulatory-compliant software tools
Fraud Detection	60%	Include diverse perspectives in design	Implement regular bias audits	Deploy bias-detection algorithms

Adoption of AI Requires an Enterprise Risk and Governance Framework

Core elements of an AI Governance Framework



Foundational Capabilities

Responsible AI Principles

AI Risk Taxonomy

AI Risk Intake and Tiering

AI Use Case Inventory



Operating Model and Governance

Operating Model - Roles & Responsibilities

Governance Committee and Escalations

AI Risk and Control Matrix

Training and Communication



Application Lifecycle

AI Development and Deployment Standards

AI Testing and Monitoring

Risk Mitigation Tracking and Reporting

Policies and Procedures Across Risk Domains (e.g., cyber, privacy, legal, model risk)

Common Challenges Organizations Face

1



Reviews are too slow and burdensome

2



Multiple assessments with overlapping questions

3



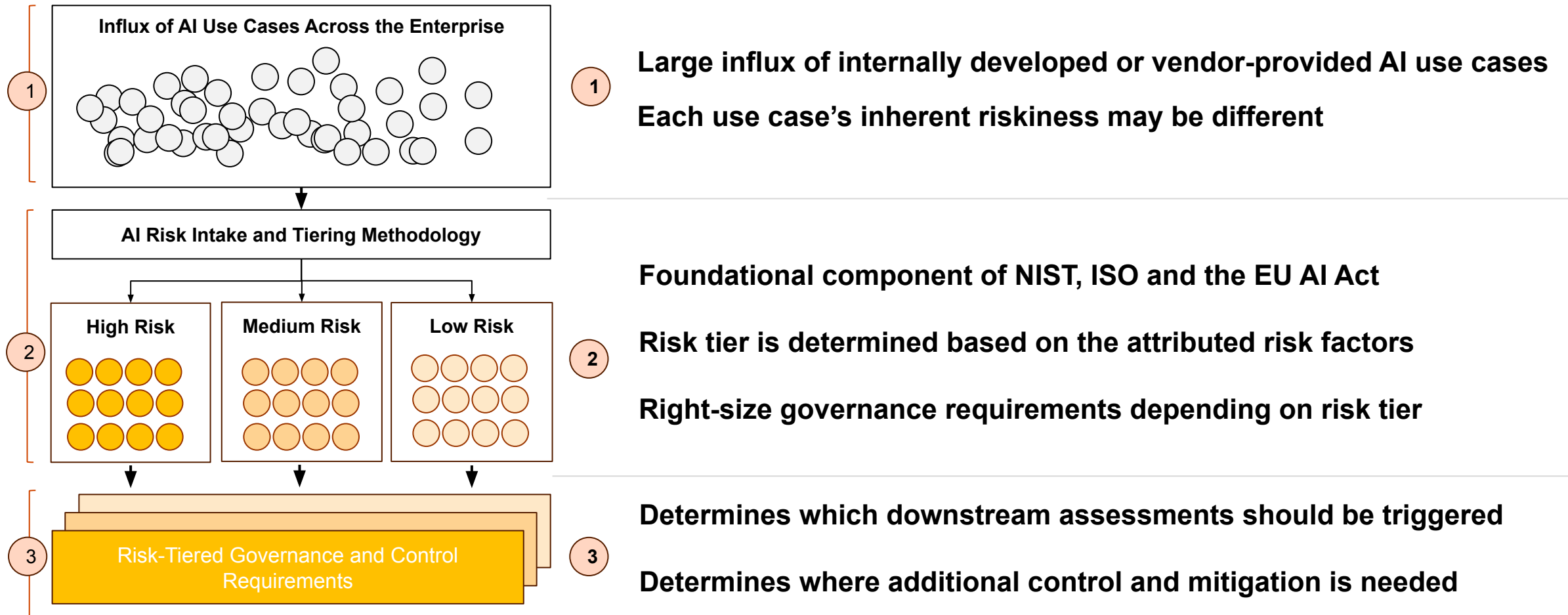
Every use case goes to AI Gov Committee

4



All use cases undergo same level of governance

AI Risk Tiering is a Core Requirement for AI Governance and Risk Management





Characteristics of a leading AI Risk Tiering Methodology

Characteristic	
1	Speed and efficiency Comprises 8-12 questions to quickly determine risk level
2	Objective and standardized Both the questions and response sets are defined and articulated clearly and objectively
3	Consistent and scalable Can be implemented consistently at scale across a large number of teams
4	Grounded in a risk taxonomy Questions and risk factors tie back to an enterprise AI risk taxonomy
5	Full coverage Required for all AI use cases to provide a full view of AI risks across the enterprise
6	Early application Typically completed during the concept and ideation phase
7	Integrated into a platform Should ultimately be embedded in an enterprise technology platform with integration to the AI use case inventory

A well-structured, well-defined and comprehensive risk taxonomy creates the foundation of risk tiering

Level 1 risk categories

1 Model Risks	
1a	Conceptual Flaws
1b	Performance Issues
1c	Instability
1d	Opacity
1e	Unfair Outputs
1f	Implementation Errors

2 Data Risks	
2a	Data Availability Issues
2b	Data Quality Issues
2c	Data Loss
2d	Data Lifecycle Risks
2e	Data Misuse

3 Cyber and Infrastructure Risks	
3a	Infrastructure Outage
3b	Infrastructure Degradation
3c	Infrastructure Misconfiguration
3d	Unauthorized Access
3e	Third-Party Risks

4 Use Risks	
4a	Manipulation
4b	Misuse
4c	Inaccessibility & Exclusion

Example Risk Tiering Questionnaire and Output (illustrative - not comprehensive)

		Policy Search (Low Risk)	Code Co-Pilot (Moderate Risk)	Virtual Assistant (High risk)	
1	What is the origin of the model used for this use case?	Internally Developed Use Case	Vendor Solution/Managed Services	Vendor Solution/Managed Services	
2	Is the use case developed for internal or external users or both?	Internal Use only (Employees)	Internal Use only (Employees)	Customers	!
3	Does the AI system make automated decisions, and/or is there human involvement in the decision-making process?	AI solution assists human decision-making	Solution does not involve decision-making support	Automated decisions with limited human intervention	!
4	Are there known regulatory or legal requirements associated with the use case or the underlying data?	No	No	Yes	!
5	Is there a direct financial impact in the event of a system failure or incorrect prediction?	No	No	No	
6	How much would a failure or inaccuracy in the application disrupt business operations or decision-making processes?	Low	Moderate	High	!
7	Please select the relevant use cases applied in a context where bias, fairness or discrimination is a potential concern?	Not applicable	Not applicable	Access to services and products	!
8	Does the use case leverage any of the data types from the list?	Non-public Internal Business Data	Non-public Proprietary Internal Business Data	Personally Identifiable Information	!

Moderate Risk High Risk

iapp Control Requirements are Adjusted Based on the Risk Tier

Illustrative			
Example control requirements	Low-Risk	Medium-Risk	High-Risk
Governance and Escalation <i>(Drilldown on next page)</i>	<ul style="list-style-type: none"> If applicable, undergo downstream risk assessments based on use case risk factors 	<ul style="list-style-type: none"> Undergo downstream risk assessments based on use case risk factors <p><i>Plus:</i></p> <ul style="list-style-type: none"> Reviewed by AI Risk Council Conduct Technology Change Impact Assessment 	<ul style="list-style-type: none"> Undergo downstream risk assessments based on use case characteristics <p><i>Plus:</i></p> <ul style="list-style-type: none"> Reviewed by AI Risk Council Conduct Technology Change Impact Assessment Reviewed by Risk Executive Committee Approved by Chief Risk executive
Documentation	<ul style="list-style-type: none"> More basic documentation focusing on model purpose, data sources, etc. 	<ul style="list-style-type: none"> More specific documentation on the GenAI use case model purpose, data sources, security requirements, etc. 	<ul style="list-style-type: none"> Extensive documentation detailing the development process, data lineage, security requirements, testing results, etc.
Testing frequency and depth	<ul style="list-style-type: none"> Periodic testing for key areas of concern. 	<ul style="list-style-type: none"> Moderate frequency of reviews covering additional risk concerns on a cadence set by applicable risk teams. 	<ul style="list-style-type: none"> Rigorous and more frequent testing protocols covering the full range of areas in the risk taxonomy set by applicable risk teams.
On-going monitoring	<ul style="list-style-type: none"> Limited requirements beyond basic performance measurements and controls testing as determined by risk factors 	<ul style="list-style-type: none"> Continuous monitoring of performance, impact and compliance metrics and controls testing 	<ul style="list-style-type: none"> Continuous monitoring of performance, impact and compliance metrics and controls testing
Contingency planning	<ul style="list-style-type: none"> Simple contingency plan with fallback to manual process or simpler tool. 	<ul style="list-style-type: none"> More defined contingency plan with fallback to manual process or simpler tool. 	<ul style="list-style-type: none"> Comprehensive contingency plan with detailed playbooks and protocols.



The Risk Tiering Questionnaire Informs the Triggers for Downstream Assessments and reviews

Downstream Reviews Triggered Based on Risk Factors (*Illustrative – Not Comprehensive*)

	Downstream Reviews Triggered Based on Risk Factors (<i>Illustrative – Not Comprehensive</i>)					
Does the use case have these risk factors? (<i>Illustrative – Not Comprehensive</i>)	Legal	TPRM	Model Performance Testing	Privacy Impact Assessment	Architecture Review	Information Security
Third-party AI solution is involved	✓	✓				
External AI solution implemented within client infrastructure/environment		✓			✓	✓
In-house built use case where model performance can be evaluated			✓			
Uses or interacts with PII, biometric data, customer data, employee/contractor data, or job applicant data				✓		
Processes supporting Judicial or Law Enforcement requests	✓					
Monetizes or sells customer data	✓			✓		

Example Risk Tier dashboard for a use case

Use Case Description

The Complaint Manager uses Generative AI aims to improve complaint management by automating tasks such as note transcription, complaint categorization, and response generation. This reduces manual work and speeds up processing. The system helps employees by extracting key details, suggesting resolutions, and ensuring accurate routing, while continuously analyzing data for improvements. The solution boosts operational efficiency, customer satisfaction, and regulatory compliance

Phase
Design

Key Risks & Mitigations

Use Case Risk Score

● HIGH RISK

● 1

● 3

● 5

This use case is classified as *High-Risk* due to its use of PII and employee information.

Triggered downstream assessments

Performance and Accuracy Testing	Privacy Assessment	Legal Review	Architecture Review	TPRM Review	Information Security
✓	✓	✓	✓	✓	✓

Risk characteristics triggered Medium or High

#	Risk Characteristics	Risk Level
Q3	The project is used by augmented decision-making, which allows for human-in-the-loop review.	Medium
Q5	A failure could result in a moderate financial risk.	Medium
Q6	A failure could result in a moderate disruption in businesses.	Medium
Q7	The project can access internal data such as confidential project details and personal identifiable information (PII).	High

Team Members	
Role	Name
Business Sponsor(s)	Jane Doe

Escalation Priorities	
AI Risk Committee	Tech Change Impact Assessment
✓	✓
Executive Risk Committee	CRO
✓	✓

Use Case Risk Score Key

● High
 ● Medium
 ● Low

How Can Technology Help

Visibility into the data AI is processing and the associated risks can be challenging to obtain. There are several actions that can be taken to help organize a view of AI uses and ensure appropriate internal governance of the technologies.

- **Scanning for Shadow AI:** shadow technologies are inevitable. Scanning your network to identify these uses is necessary to ensure compliance with legal and regulatory frameworks, along with internal policies and standards
- **Maintaining inventories of AI assets, including data processed for each and use cases:** keeping records of how AI is used is necessary for transparency and ensuring accountability
- **Completing assessments prior to new uses of AI:** In addition to satisfying legal requirements for assessments, these questionnaires can help review individual use cases for compliance and general risk management

Questions and Answers

Panelists



Jay Cline
Principal, Data Risk &
Privacy
PwC



Andrew Bouta
Director, Data Risk &
Privacy
PwC



David Ray
CIPP/US, CIPM, CIPT
CPO
BigID

Web Conference Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: <https://iapp.questionpro.com/t/ACtQeZ39yH>

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: [submit for CPE credits](#).

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation please
contact:

livewebconteam@iapp.org