Prioritize AI Oversight and Enable Innovation

How AI Risk Tiering and Advanced Data Sharing Accelerate Implementation

May 7, 2026

PRIVACY ANALYTICS

an IQVIA company

Speaker Introductions

Jennifer Geetter
Partner
McDermott Will & Schulte

Sorana Ionescu
Director, Smart Metering
IESO (Independent Electricity System Operator – Ontario)

Luk Arbuckle
Global AI Practice Leader, Chief Methodologist
IQVIA Applied AI Science

Brian Rasquinha
Associate Director, Solution Architecture
Privacy Analytics
(Moderator)

PRIVACY ANALYTICS
an IQVIA company

About the IESO

Operate Ontario's province-wide electricity system 24/7

Oversee the electricity market, driving competition to maintain affordability

Plan for Ontario's future energy needs

Support innovation and emerging technologies

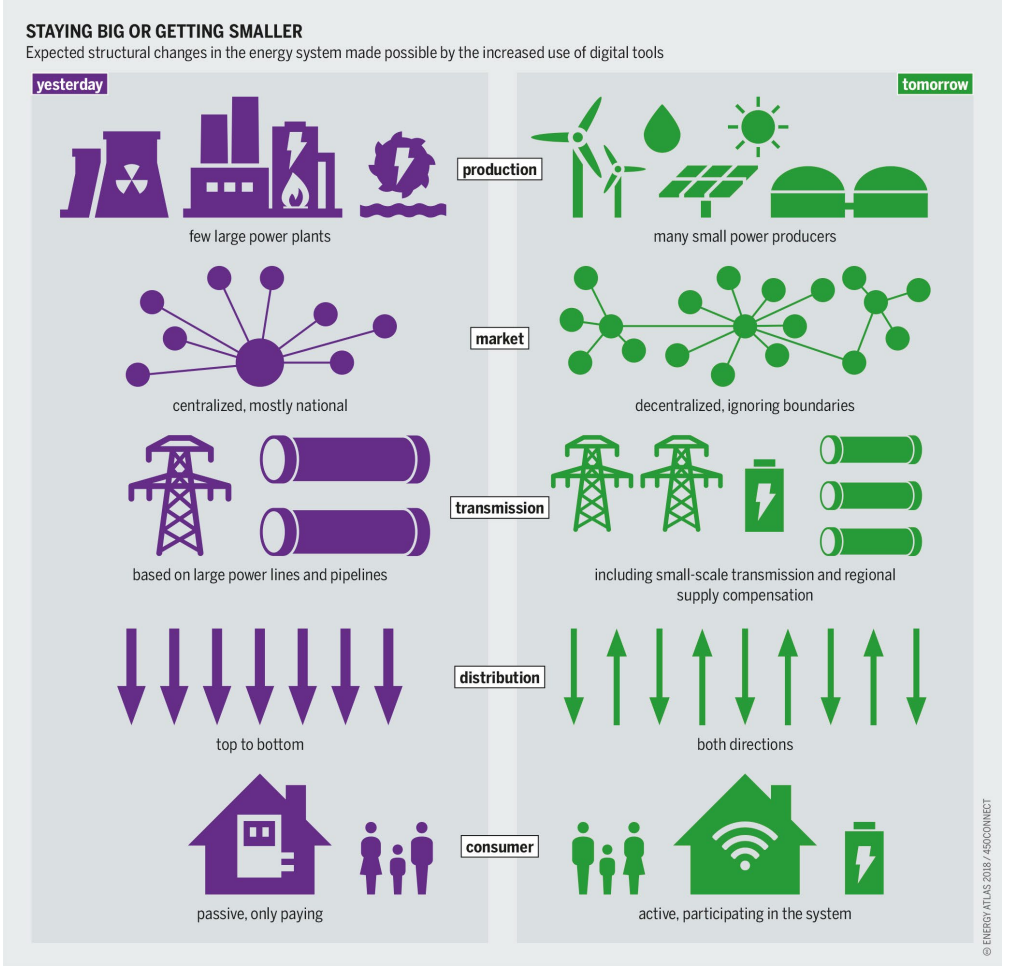
Work closely with communities to explore sustainable options

Enable province-wide energy conservation

Ontario's designated Smart Metering Entity

Current Challenges and Future Trends

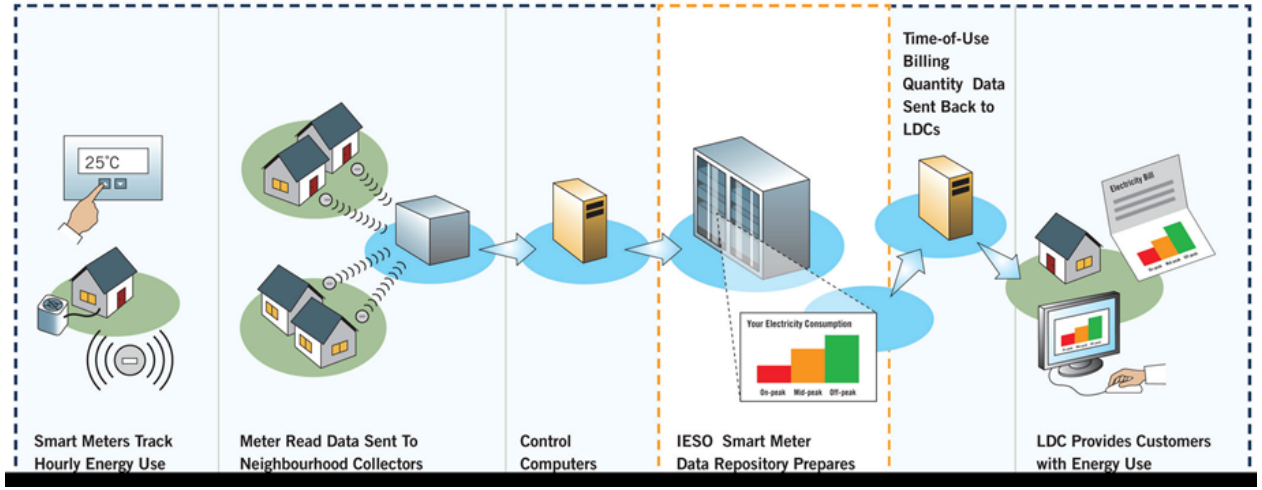
- From Centralized Control to Distributed Orchestration
- AI becomes foundational to Reliability and Planning
- DERs evolve from Passive Load to Coordinated Reliability Resources
- Cybersecurity evolves into a cross-layer System Risk
- Markets adapt to Distributed, Machine-speed Participation
- System efficiency depends on integrated DX–TX digital optimization



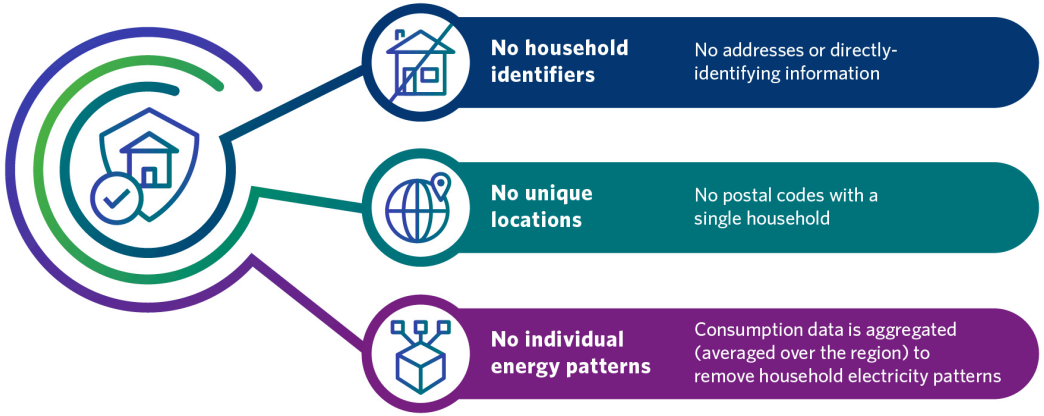
ieso
Connecting Today. Powering Tomorrow.

Ontario's Smart Metering System

- One of the largest data systems globally, supporting Ontario's 50+ utilities billing of 5.5million customers and creating broad data & analytics value from its massive datastore.



- Privacy, Security and Ethical Use of Data are Built-in, so that Ontarians' information is Anonymized, Aggregated, Scrutinized for Ethics and Legally Protected.

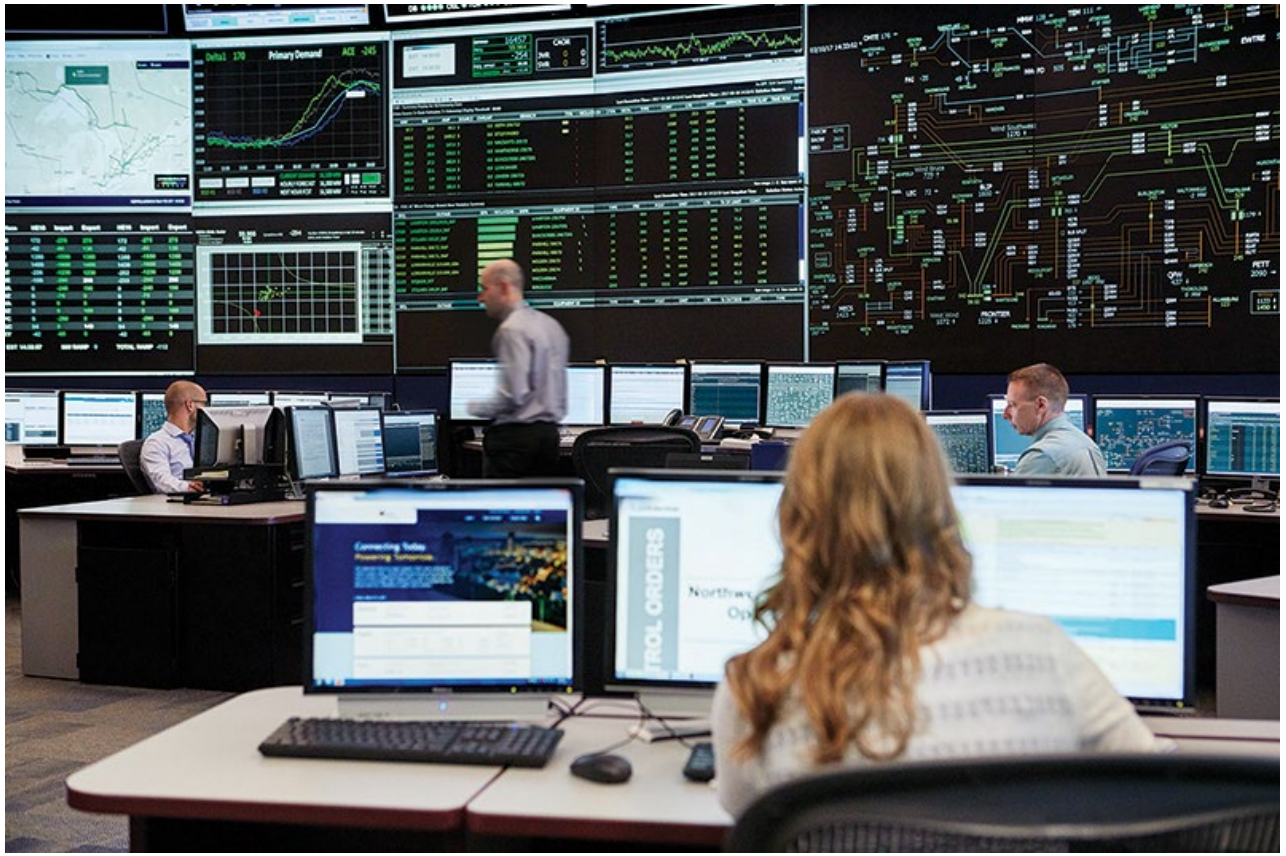


https://www.ieso.ca/en/Sector-Participants/Smart-Metering-Entity/Consumption-Data

"AI is the New Electricity"

"Just as electricity transformed almost everything 100 years ago, today I actually have a hard time thinking of an industry that I don't think AI will transform in the next several years…."

Andrew Ng, Stanford Graduate School of Business address, 2017



Why is this so hard? Systemic & Specific Challenges

Systemic

Deck Chairs Problem

- Differences in kind versus degree
- Failure is not a choice

Risk Tolerance

- “Over trust” in computers
- Lack of alignment with “baseline” human error rate
- AI problem or underlying problem?

Public Trust

- “Consent”, “notice” and other models
- Technological complexity

Specific

1. AI FOMO
2. Procurement Uncertainties
3. Non-harmonized regulation
4. Technologically complex; reliance on developers
5. Lack of industry standards; qualifying body
6. Hallucinations (or sometimes called “bullsh*&#tting”)
7. Privacy considerations
8. Degradation
9. Unpacking bias
10. Ambiguity of the status of “training” in PHI permitted uses
11. Evolving IP landscape
12. Compliance-Technology Translation

PRIVACY ANALYTICS
an IQVIA company

Concerns and solutions

AI Threat

Why the concern

- **“AI”** is used to describe a wide range of tools, from regression to large language models; the **size** and **impact** of an AI system is highly variable.
- **Regulators** increasingly focused on AI applications.
- **Risks of data misuse** can be heightened given reduced AI explainability and transparency, and increased ease of use

Managing Threat

What can be done

- The **use case** for the AI system is a critical factor in determining risk, scaling the impacts of misuse.
- Attacks depend on the **access** and **type** of AI technology. Predictive AI vs generative AI is a useful classification.
- **Tiering** AI risk builds on best practice from financial services, a highly regulated field with extensive experience delivering on model risk management.

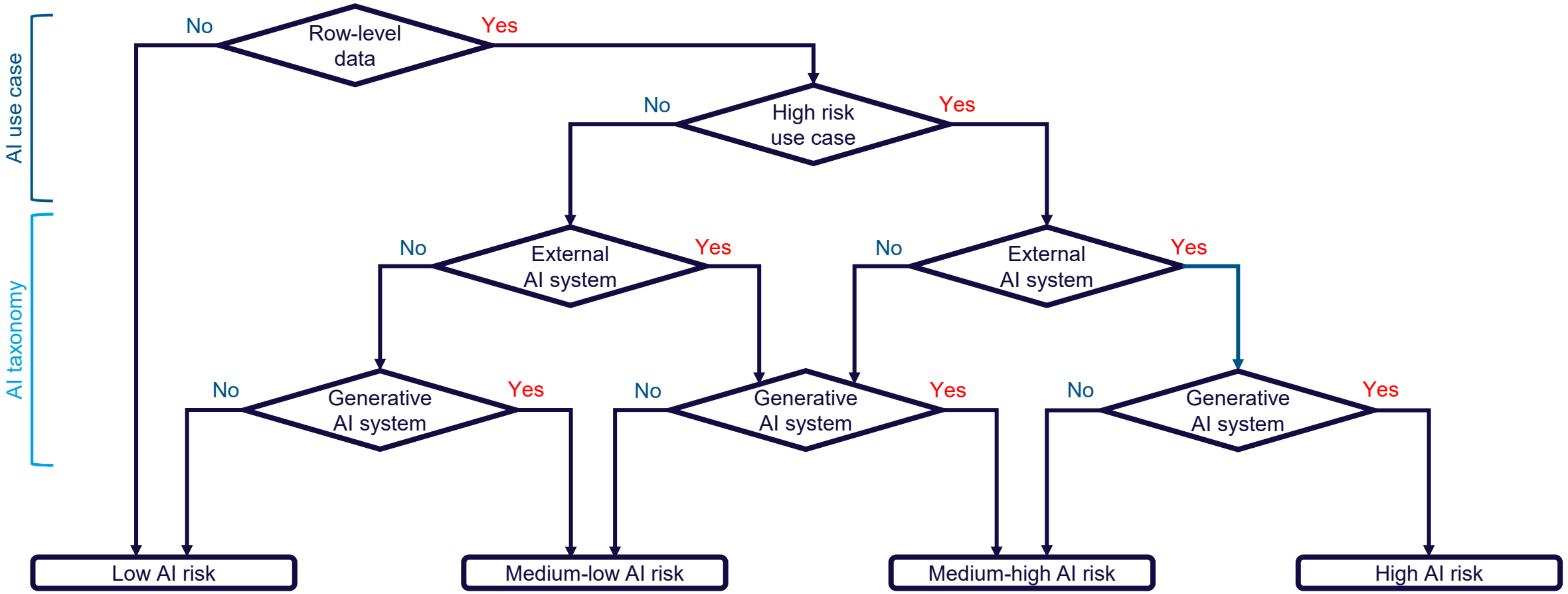
Data Sharing

Options to mitigate

- **Contractual obligations** to ensure purpose definitions, AI governance, formal certifications, attestations, or best practices.
- **Inform and train** data users on the risks of AI and their obligations in terms of best practices.
- **Verify adherence** for higher risk use cases/systems by requiring proof of certification, assessment, or documented practices.

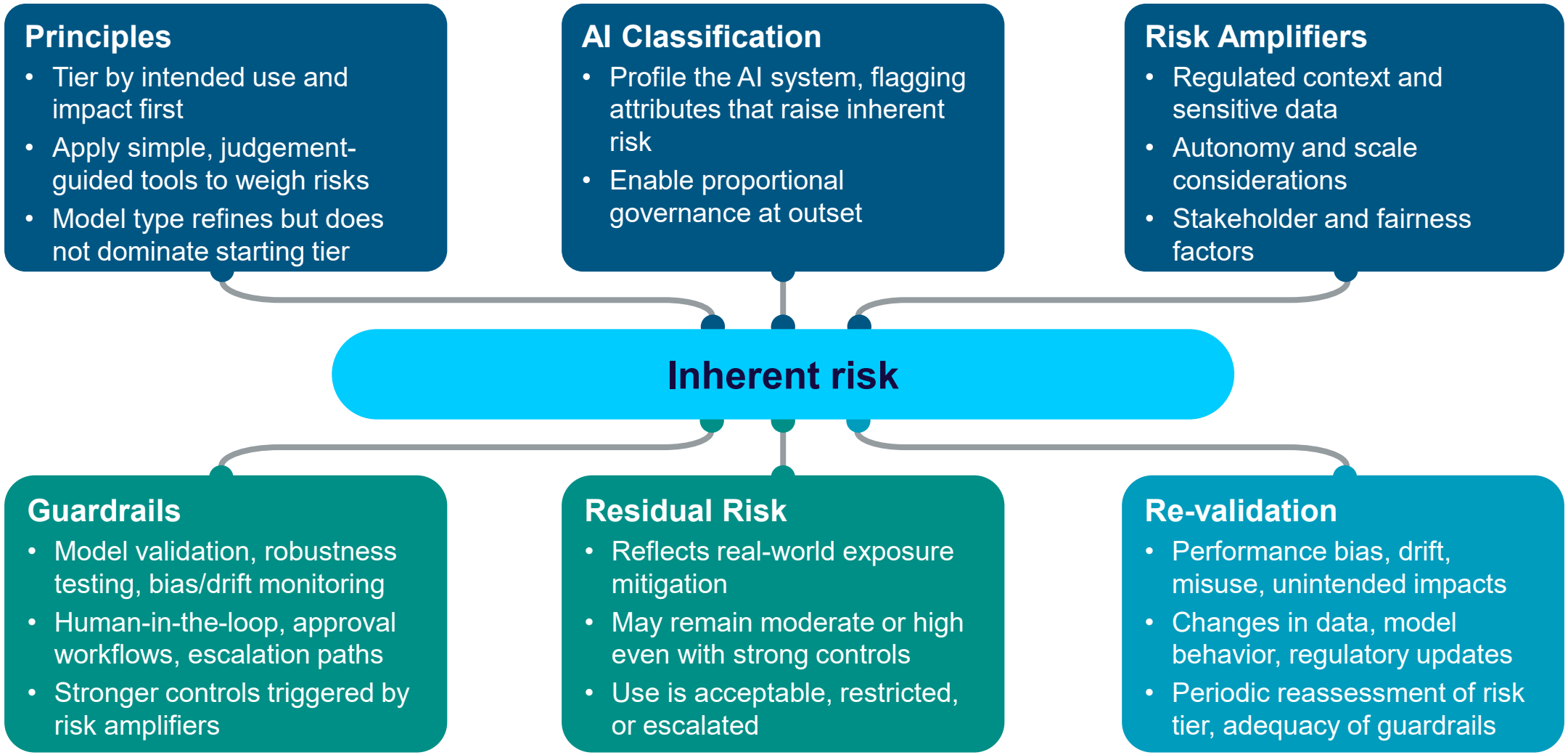
PRIVACY ANALYTICS
an IQVIA company

AI risk tiering example: preliminary rating before mitigation



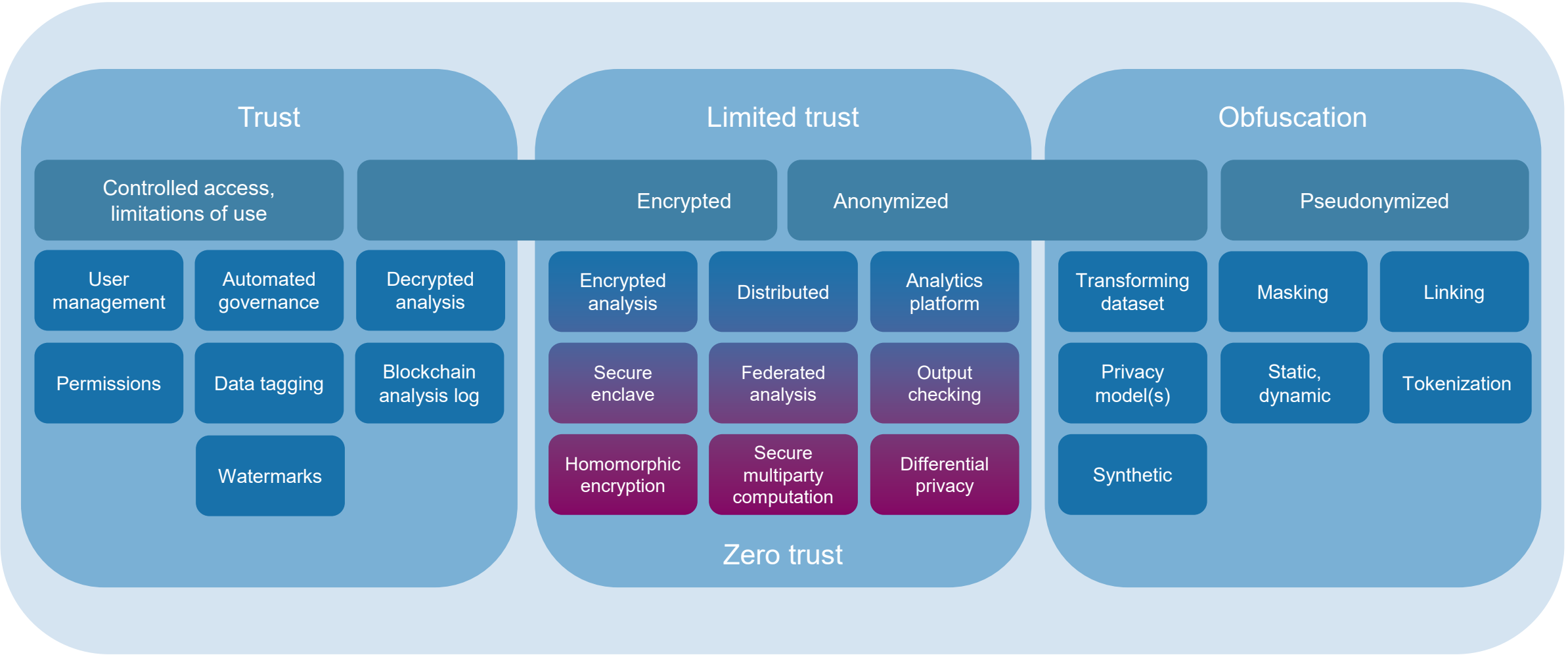
PRIVACY ANALYTICS
an IQVIA company

Inherent risk and guiding principles



PRIVACY ANALYTICS
an IQVIA company

Spectrum of Privacy Enhancing Technologies



Advancing Privacy Enhancing Technologies https://privacy-analytics.com/resources/articles/advancing-privacy-enhancing-technologies/

PRIVACY ANALYTICS
an IQVIA company

There is no risk-free AI, but the right AI is worth reasonable risks

- All technologies, tools, and products carry risks
- Important to assess your risk tolerance – for the business and for the Office of the General Counsel
- Consider establishing a risk-based approach that incorporates the **risk standard of the non-AI alternative**
- Look for opportunities where the benefits to the OGC outweigh the risks (this is a good general principle)
- Don't feel AI FOMO – it doesn't have to be AI to be better
- Look for opportunities to
  - Maximize efficiency
  - Minimize time spent on unrewarding tasks
  - Accelerate growth or control costs
  - Facilitate business intelligence
- Don't make compliance hard – find ways to hardwire **guardrails** *and* create **a post-implementation safety check** system

Focus on what AI is good at – like any tool, AI is good at certain things, and not appropriate for other things

PRIVACY ANALYTICS
an IQVIA company

Thank You!

Jennifer Geetter
Partner
McDermott Will & Schulte

Sorana Ionescu
Director, Smart Metering
IESO (Independent Electricity System Operator – Ontario)

Luk Arbuckle
Global AI Practice Leader, Chief Methodologist
IQVIA Applied AI Science

Brian Rasquinha
Associate Director, Solution Architecture
Privacy Analytics
(Moderator)

PRIVACY ANALYTICS
an IQVIA company