

THE AI PRECIPICE

An Executive Guide to Balancing AI Innovation and Safety

Board Director and Executive Discovery Toolkit

Toolkit #2

AI Governance Controls
Maturity Assessment



INSTRUCTIONS

Toolkit Value

- To equip senior leaders from diverse industries and backgrounds, for-profit or not-for-profit, to advance their strategy, governance, and compliance /risk monitoring systems with an AI maturity assessment toolkit.
- Over 85% of organizations continue to struggle to sustain AI in their organizations, and this book offers precision guidance to achieve the value from AI and successfully balance AI innovation and safety.
- This AI Maturity toolkit provides an opportunity to reflect on where your organization is in relation to your AI investments, take stock, identify strengths and gaps, and build a gap closure plan.

Starting Gate

Read: ***The AI Precipice: An Executive Guide to Balancing AI Innovation and Safety.***

Toolkit Audience

- Senior Executives (Board Directors, CEOs, and Leadership Teams)
- Diverse Industries are explored in this book (i.e., Education, FSI, Government, Healthcare, High Tech, Manufacturing, Pharma, Telecom, etc).
- Small businesses to Large Enterprises, as AI is crucial for all businesses to advance with strong AI foundations for competitive advantage and business survival.
- Content is particularly relevant to private or public organizations, but still has relevance to the not-for-profit sector, especially for government organizations, covered in this book

Toolkit Overview

- This toolkit provides a useful self-evaluation toolkit for organizations to assess the maturity of their AI Model Risk Controls or in a working session with your colleagues.

- The maturity scale ranges from 1 to 5:
 - 1 = Not in place
 - 2 = In place for specific groups
 - 3 = In place and standardized enterprise-wide
 - 4 = KPIs are in place to measure AI performance
 - 5 = Highly automated and benchmarked
- Benchmarking means that you have, at a minimum, an annual exercise to benchmark the completeness and sufficiency of your control against external criteria (regulation or voluntary standard), or it is evaluated by an independent third party.

Get in Touch

aiprecipice.com

Cathy Cobey

cathy.r.cobey@ca.ey.com

[LinkedIn](#)

Cindy Gordon

cindy@saleschoice.com

[LinkedIn](#)

Table 1.0 – AI Governance Controls – Maturity Evaluation Toolkit

Control Type	Definition	Maturity Scale
Enterprise-wide AI Governance Controls		
Policies	An AI policy is a set of guidelines an organization uses to govern the development, deployment, and usage of AI systems. It aims to ensure responsible, ethical, and compliant AI practices, align with legal and regulatory requirements, and organizational values. These policies include areas like data privacy, security, transparency, accountability, data bias, and fairness.	1 2 3 4 5
AI strategy	An AI strategy is a plan that outlines how an organization will leverage AI to achieve business goals and enhance efficiency. It includes identifying key use cases, investing in infrastructure, and developing skills for successful implementation.	1 2 3 4 5
Accountability	Accountability refers to the attribute of being responsible for the actions and decisions of AI, as well as the impact AI systems have on individuals and society. Having clarity on the AI model originators and operators is crucial.	1 2 3 4 5
Training and education	Evidence of investments in workforce digital literacy and building AI skills is important to ensure resiliency during change, supporting an organization's cultural evolution.	1 2 3 4 5
AI Investment Committee	An AI Investment Committee focuses on evaluating both the technical and financial viability of AI projects, assessing whether they align with organizational goals. It also considers ethical and responsible implications, ensuring that investments are made in a manner that upholds integrity and societal values.	1 2 3 4 5
AI program KPI	KPIs measure the overall success and impact of AI initiatives across the organization. These metrics encompass various dimensions, including project completion rates, ROI, user adoption, and alignment with strategic goals, providing a comprehensive view of the program's effectiveness and value.	1 2 3 4 5
AI System Governance Controls		
Risk assessment	An AI risk assessment identifies, analyzes, and mitigates potential risks associated with the development, deployment, and use of AI systems. It involves evaluating various aspects of an AI system,	1 2 3 4 5

	including data, algorithms, decision-making, and potential impacts on individuals, communities, and society. The goal is to ensure that AI systems are used responsibly, minimizing harm and maximizing benefits.	
Incremental testing	Incremental testing is an approach used to test individual software components or modules of an AI system separately and then integrate them gradually. It involves testing each part of the system incrementally as new functionalities or components are added.	1 2 3 4 5
Inventory management	AI inventory management is the practice of documenting all the AI models, system cards, and having controls on data source history, model methods, model testing processes, and recording outcomes, resources in the model building, testing, and sustaining process. This area is key for audit controls, regulatory compliance, and mitigating unforeseen risks.	1 2 3 4 5
Risk mitigation plan	An AI risk mitigation plan is a proactive strategy for identifying, analyzing, and addressing potential risks associated with the development, deployment, and use of AI systems. It involves developing and implementing measures to reduce the likelihood or impact of these risks, ensuring responsible and ethical AI practices.	1 2 3 4 5
Independent testing	Independent AI model testing refers to a third party operating independently of the AI model development process, with the aim of uncovering any issues, latent defects, ensuring optimal performance, adherence to applicable regulatory requirements, etc. For high-risk AI applications, independent testing is highly encouraged to reduce risks.	1 2 3 4 5
AI performance metrics	AI performance metrics are a set of specific indicators designed to evaluate the effectiveness and impact of AI systems within an organization. This program focuses on tracking KPIs related to accuracy, efficiency, and user satisfaction, ensuring that AI initiatives align with business objectives and deliver measurable value.	1 2 3 4 5
Continuous monitoring	AI continuous monitoring involves continuously evaluating AI models to ensure they function as intended, identifying potential issues like data drift, performance degradation, hallucination, and making adjustments to maintain accuracy and	1 2 3 4 5

	trust.	
Adversarial attack management	AI adversarial attack management encompasses strategies and techniques to identify, mitigate, and defend against attacks on ML models that are designed to deceive or manipulate the model into making incorrect predictions or decisions. These attacks, known as adversarial attacks, exploit vulnerabilities in the ML model's learning mechanisms by introducing carefully crafted, often subtle, manipulations to the input data.	1 2 3 4 5
Intelligent monitoring	Intelligent monitoring uses AI to oversee IT systems, enhancing traditional monitoring by providing predictive insights, automating tasks, and improving incident response	1 2 3 4 5
Kill switch	A kill switch enables organisations to pause, contain, or disable compromised AI systems before they cause serious damage. Far from a simplistic shutdown mechanism, an AI kill switch is about enforcing control through machine identity security and having the audit tracking mechanisms to identify intrusion sources.	1 2 3 4 5