

# Redefining Internal Audit in the Age of AI - Powered by SheLeadsTech



6 September 2025

# Panelists

Pacchanya Chutimawong

Vice President - ISACA Bangkok and SVP -  
Internal Audit, Frasers Property (Thailand) PCL

CISA, CISM, CRISC, CGEIT, CDPSE, CIA,  
CRMA, CPA, CFE



Natchaon Sunthonlap

Sheleadstech Director - ISACA Bangkok and  
Associate Director, KPMG Phoomchai  
Business Advisory Ltd

CISA, ISO27001 LA



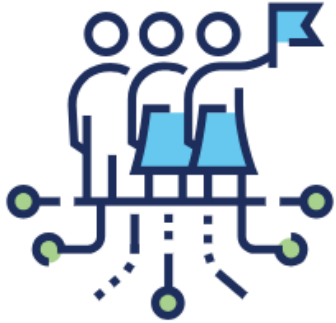
Sittichai Choosupanasorn

Chapter Membership Director - ISACA  
Bangkok

CISA, CRISC, CGEIT, AAIA, CIA, CRMA,  
CCSA, CFSA, CGAP, CPA



# SheLeadsTech program pillars



## **ENGAGE: Raising awareness**

We will engage with employees, allies and global professionals to increase diverse representation within our industry.



## **EMPOWER: Building alliances**

Through strategic partnerships and volunteer support, we empower our network and support our chapters in confronting the unique challenges in their countries and regions.



## **ELEVATE: Preparing to lead**

Our training and skills development programs will offer opportunities to elevate more female leaders in the digital space.

# Join us for the 2025 LeadHERship Series

Anyone is welcome to register and learn live or on demand. Members earn 1 FREE CPE.

Featured LeadHERship Series Webinar | 1 FREE CPE for Members

## Elevate Your Career

**Lauren Hasson**

**9 September 2025**

Explore ways to stand out, get ahead, and build value as a working woman through an award-winning five-step framework. Discover how you can better develop and demonstrate your value in the workplace.

**REGISTER NOW**





# Agenda

1. Exclusive summary from GNDI: Governing in the Age of Disruption – Artificial Intelligence (2024–2025)
2. Auditing the Future: HOW AI IS REDEFINING THE AUDIT LANDSCAPE AND HOW YOU CAN BE PREPARED
3. the ISACA Advanced in AI Audit™ (AAIA™)
4. Key insights and answers from IA Clinic session



# สรุปสาระสำคัญจากรายงาน GNDI: Governing in the Age of Disruption – Artificial Intelligence (2024–2025)

Pacchanya Chutimawong

CISA, CISM, CRISC, CGEIT, CDPSE, CIA, CRMA, CPA, CFE

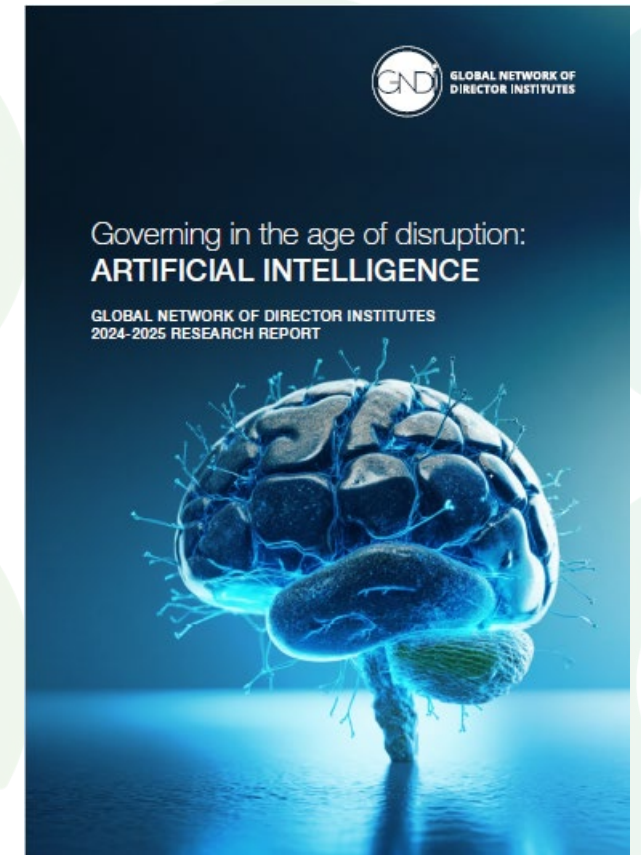
Vice President - ISACA Bangkok

SVP - Internal Audit, Frasers Property (Thailand) PCL

6 September 2025

# 1. ภาพรวมและวัตถุประสงค์

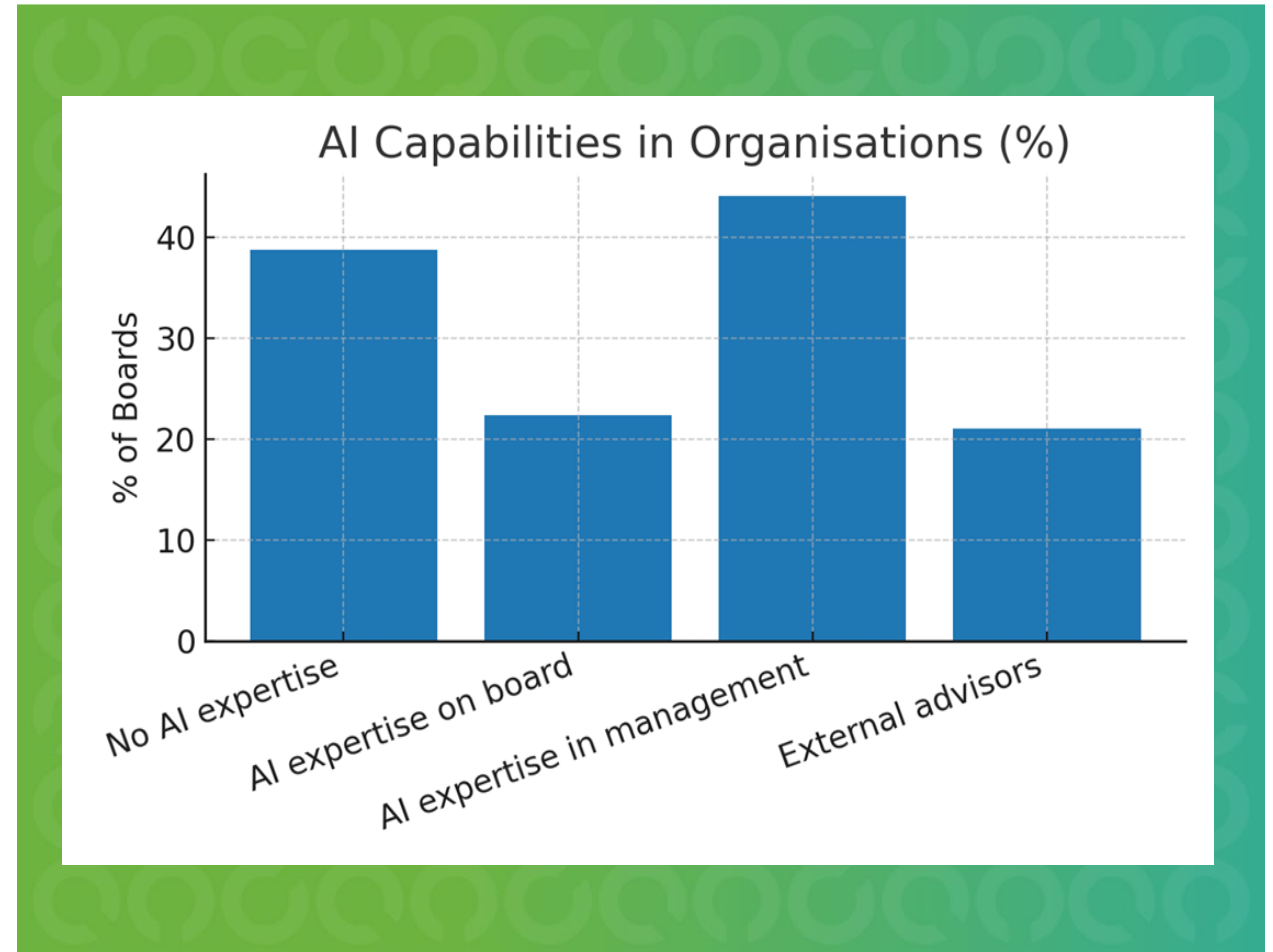
- รายงาน GNDI: Governing in the Age of Disruption – Artificial Intelligence (2024–2025) เป็นรายงานวิจัยระดับโลกจาก Global Network of Director Institutes (GNDI) ซึ่งมีสมาชิก 26 สถาบัน กว่า 150,000 กรรมการทั่วโลก
- สำรจวมุมมองของกรรมการต้อบทบาทการกำกัับดูแล AI ใน 3 มิติหลัก
  1. Capability – ความรู้ ความสามารถ และทรัพยากรในการกำกัับดูแล AI
  2. Risk & Opportunity Oversight – การมองเห็นและบริหารความเสี่ยง/โอกาสของ AI
  3. Policy – การมีนโยบายและกรอบธรรมาภิบาล AI



## 2. ผลสำคัญจากการสำรวจ: Our organization has AI capabilities to guide decision making?

### (1) ความสามารถ (Capability)

- 38.8% ขององค์กรไม่มีความเชี่ยวชาญด้าน AI เลย
- มีเพียง 22.4% ที่มีกรรมการซึ่งมีทักษะด้าน AI
- การใช้ที่ปรึกษาภายนอกเพื่อการตัดสินใจด้าน AI มีเพียง 21.1%
- การพัฒนาทักษะกรรมการ (board upskilling) ยังไม่ทั่วถึง

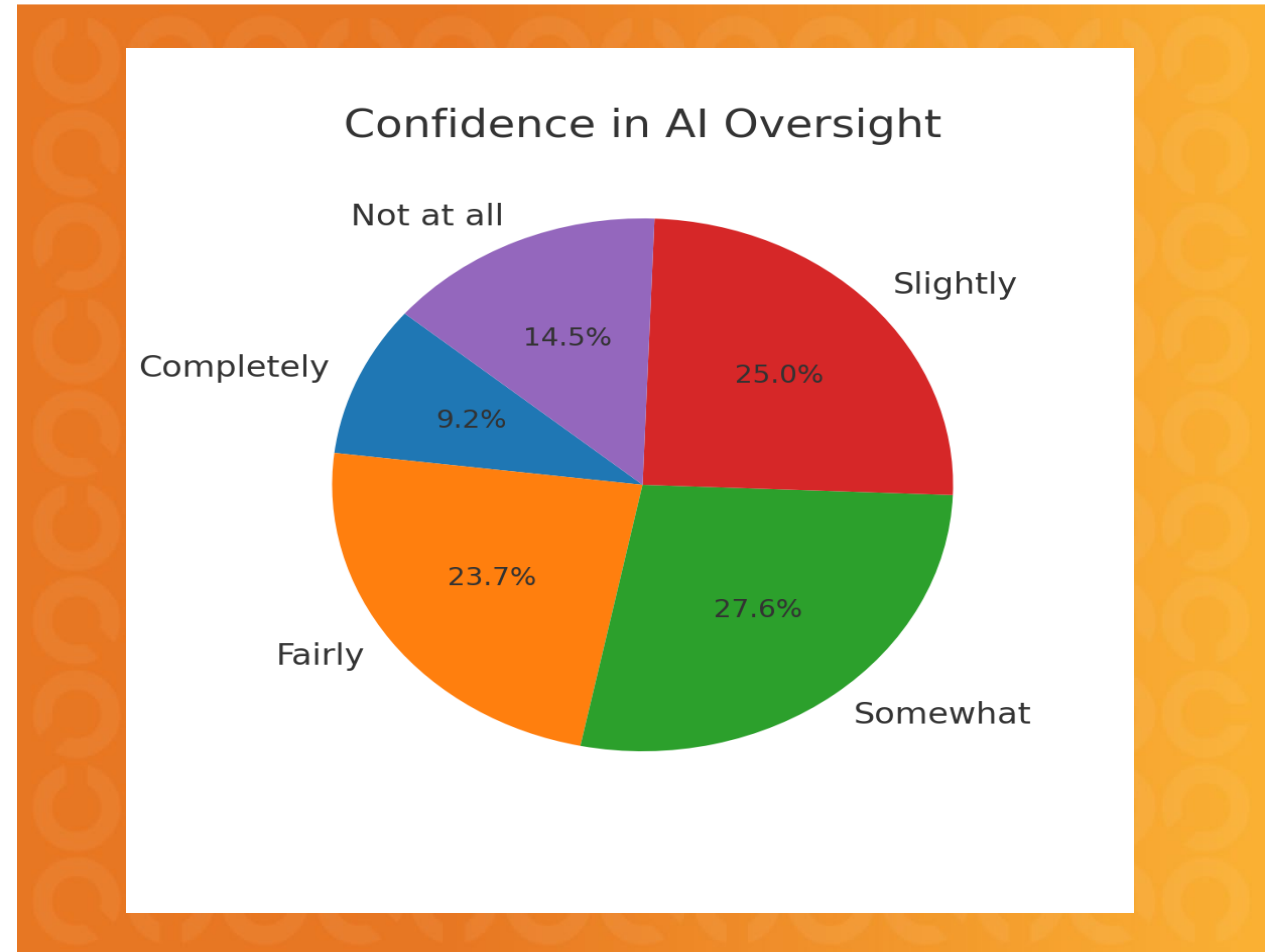




## 2. ผลสำคัญจากการสำรวจ: How confident are you that your board understands the implications of AI on strategy?

### (2) ความเสี่ยงและโอกาส (Risks & Opportunities)

- ความมั่นใจของบอร์ดต่อความเข้าใจผลกระทบเชิงกลยุทธ์ของ AI ค่อนข้างต่ำ
- มั่นใจมาก (Completely confident) แค่ 9.2%
- ความเสี่ยงหลัก: misinformation, bias, cybersecurity, “shadow AI”, ความซับซ้อนด้านกฎระเบียบ
- AI ยังมีโอกาสเชิงกลยุทธ์ เช่น เพิ่มประสิทธิภาพ, สร้างนวัตกรรม, ขยายโมเดลธุรกิจ



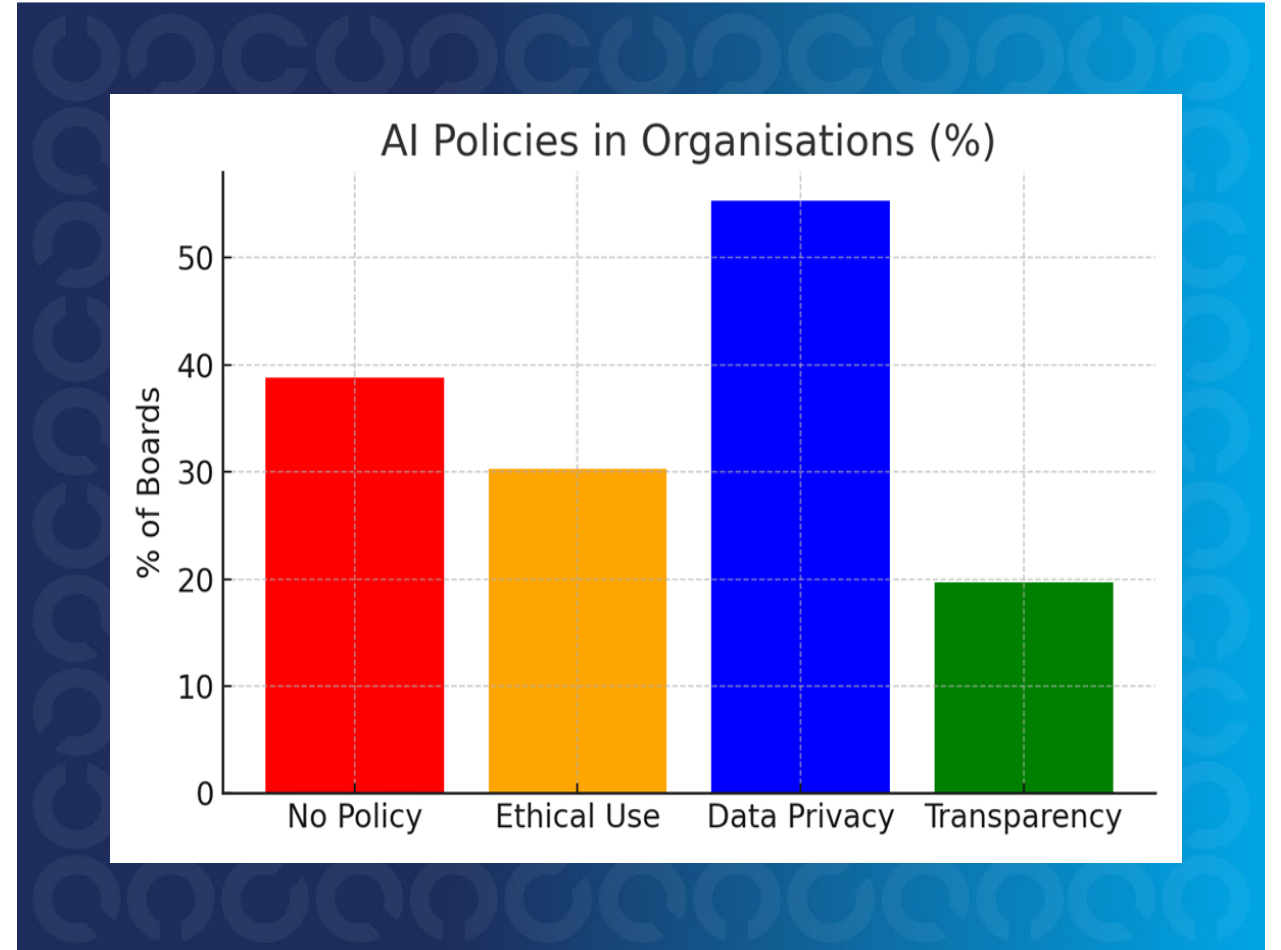
# The Evolution of Emerging Risks Over time

Category	1980	2000	2005	2010	2015	2020	2025	2030 - Prediction
<b>Geopolitical &amp; Security</b>	Cold War tensions, nuclear risks, regional conflicts	Post-Cold War optimism; early terrorism alerts	Terrorism, Iraq/Afghanistan wars, nuclear proliferation	Arab Spring, sovereign instability, piracy	Crimea annexation, ISIS, refugee crises	US-China rivalry, hybrid warfare, trade tensions	Russia-Ukraine war, Taiwan tensions, economic weaponization	Cyber warfare, AI-driven disinformation, space militarization
<b>Economic &amp; Financial</b>	Oil shocks, stagflation, debt crises	Dot-com bubble burst; globalization risks	Oil volatility; early housing bubble warnings	Post-GFC recovery; sovereign debt crises	Market volatility; shadow banking	Pandemic-driven recession; inflation uncertainty	High debt; deglobalization pressures; energy shocks	Structural AI/automation disruptions; financial instability
<b>Technology &amp; Cyber</b>	Early IT risks; analog system failures	Y2K; early internet; basic hacking	Network outages; offshoring risks	Cloud adoption; mobile; big data emergence	Cyber breaches; IoT vulnerabilities	Ransomware; state-sponsored attacks	AI-driven cyberattacks; misinformation; deepfakes	Quantum disruption; autonomous AI failures
<b>Environmental &amp; Climate</b>	Acid rain; ozone depletion; local pollution	Low priority; localized disaster focus	Tsunami; Hurricane Katrina; climate alerts	COP15; growing climate awareness	Paris Agreement; ESG integration	Extreme weather; climate disasters; net-zero push	Extreme weather; biodiversity loss; litigation risks	Climate tipping points; water scarcity; mass migrations
<b>Health &amp; Biological</b>	HIV/AIDS crisis; localized outbreaks	SARS (2003); pandemic planning	Avian flu (H5N1) fears	H1N1 pandemic; surveillance growth	Ebola; Zika outbreaks	COVID-19 pandemic; healthcare strain	Biosecurity; pathogen mutations; vaccine tech risks	Synthetic biology misuse; engineered pathogens

## 2. ผลสำคัญจากการสำรวจ: We have policies in place to ensure ethical AI use and data privacy compliance?

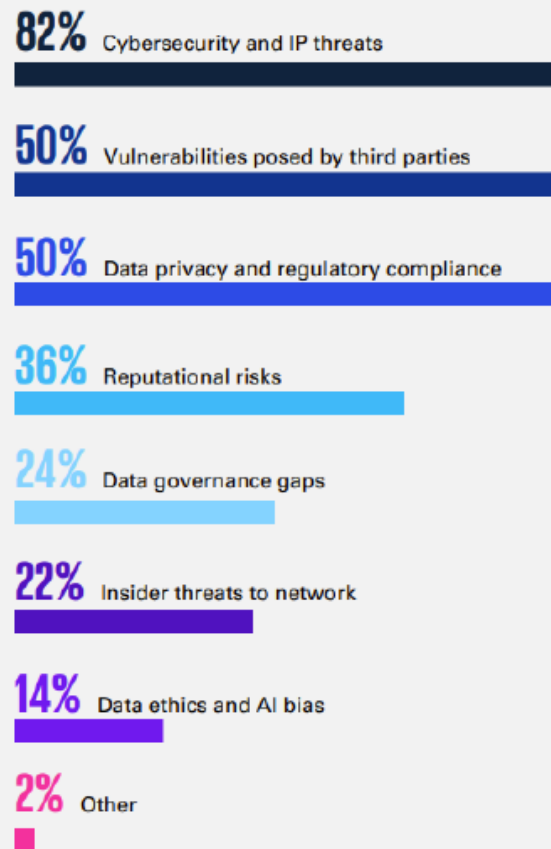
### (3) นโยบาย (AI Policies)

- 38.8% ไม่มีนโยบาย AI เลย
- 55.3% มีนโยบายคุ้มครองข้อมูลส่วนบุคคล
- 30.3% มีนโยบายใช้ AI อย่างมีจริยธรรม
- 9.7% มีนโยบายด้านความโปร่งใส



# Cyber, Data and AI Risks – Top Concerns by the Board

## Oversight risks



## Challenges

- Fragmented digital risk ownership across committees
- Limited GenAI-specific oversight capabilities
- Inadequate cyber preparedness amid rising threats
- Gap between board's understanding and real-time tech evolution.



## Opportunities

- Build tech-fluent boards with expertise in data ethics and AI
- Integrate cyber and privacy oversight into ERM frameworks
- Use tabletop exercises to stress-test digital resilience
- Elevate third-party and ecosystem-level digital scrutiny.

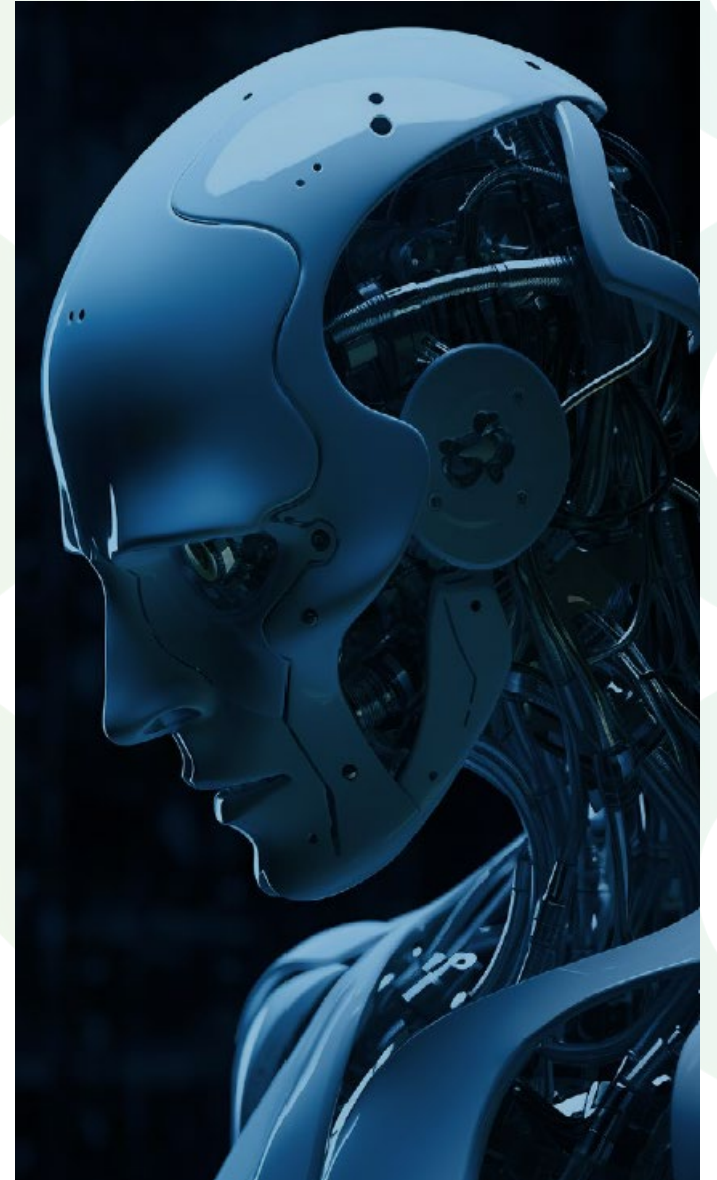


Technology and digital risks have emerged as the top area of concern for boards, especially in terms of potential oversight and preparedness gaps.



### 3. ประเด็นปัญหาเชิงระบบ (Systemic Issues)

- 1) Lack of prioritisation – มอง AI เป็นเรื่อง IT มากกว่ากลยุทธ์
- 2) Capability gaps – ขาดความรู้เชิงลึกและการฝึกอบรม
- 3) Governance fragmentation – การกำกับกระจาย กระจาย ไม่มีเจ้าภาพชัดเจน
- 4) Policy underdevelopment – ไม่มีกรอบนโยบายที่ชัดเจน
- 5) Trust & ethics challenges – ความเชื่อมั่นสาธารณะต่ำ
- 6) Reactive oversight – จัดการหลังปัญหาเกิด ไม่ได้ป้องกันล่วงหน้า
- 7) Regional divides – ความพร้อมและกฎเกณฑ์ต่างกันมากในแต่ละภูมิภาค



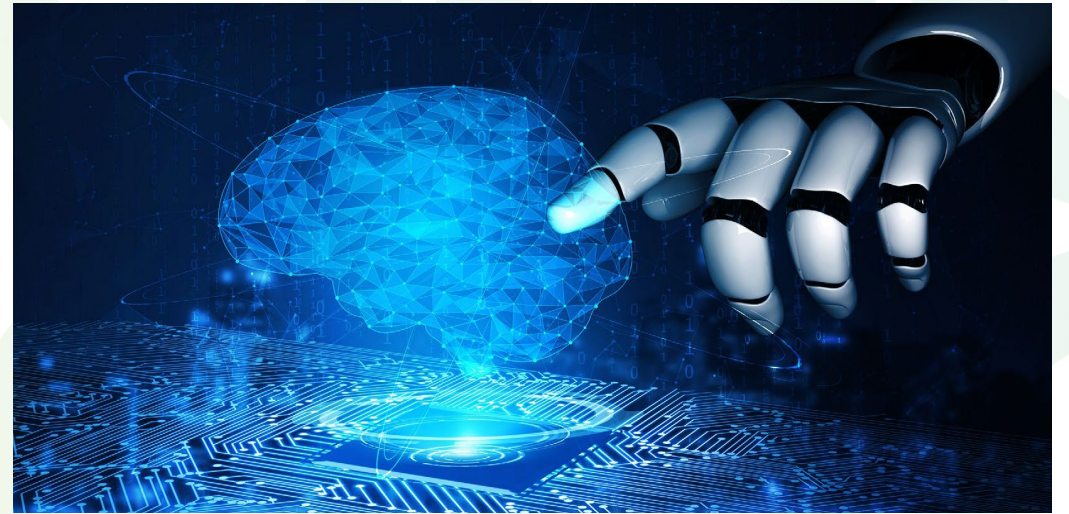
## 4. คำถามสำคัญสำหรับห้องประชุมบอร์ด

รายงานแนบมาให้คณะกรรมการตั้งคำถามต่อไปนี้เพื่อการกำกับดูแลที่มีประสิทธิภาพ:

- ✓ **ความสามารถและการกำกับดูแล:** เรามีทักษะที่จำเป็นในการกำกับดูแลความเสี่ยงและโอกาสจาก AI หรือไม่ และเรากำลังแก้ไขช่องว่างเหล่านี้หรือไม่
- ✓ **นโยบายและจริยธรรม:** เรามีนโยบายที่ได้รับการอนุมัติจากคณะกรรมการเพื่อควบคุมการใช้ AI อย่างมีจริยธรรมและความเป็นส่วนตัวของข้อมูลหรือไม่
- ✓ **การบริหารความเสี่ยง:** เราได้รวมความเสี่ยงที่เกี่ยวข้องกับ AI เช่น ข้อมูลผิดพลาด, อคติ, หรือภัยคุกคามทางไซเบอร์ เข้าไปในกรอบการบริหารความเสี่ยงของเราแล้วหรือยัง
- ✓ **ความไว้วางใจของผู้มีส่วนได้ส่วนเสีย:** เรากำลังสื่อสารแนวทางในการกำกับดูแล AI ของเรากับพนักงานและผู้มีส่วนได้ส่วนเสียอย่างไร
- ✓ **โอกาสจาก AI:** AI สามารถปลดล็อกโอกาสเชิงกลยุทธ์อะไรให้กับองค์กรของเราได้บ้าง
- ✓ **ความพร้อมสำหรับอนาคต:** เราติดตามการเปลี่ยนแปลงของกฎระเบียบและแนวปฏิบัติที่ดีที่สุดเกี่ยวกับ AI อย่างไร และเราลงทุนในการศึกษาต่อเนื่องของกรรมการหรือไม่

## 5. ข้อเสนอแนะสำหรับบอร์ด

- ✓ ยกกระดับ AI literacy ของกรรมการ
- ✓ ผังการบริหารความเสี่ยง AI เข้ากับ Enterprise Risk Management
- ✓ จัดทำ AI governance framework ครอบคลุม จริยธรรม ความโปร่งใส ความรับผิดชอบ
- ✓ สื่อสารชัดเจนเพื่อสร้าง stakeholder trust
- ✓ มอง AI เป็น strategic enabler ไม่ใช่แค่เครื่องมือเทคโนโลยี
- ✓ เตรียมพร้อมรับมือ regulatory changes และลงทุนใน continuous education



## 6. ข้อสรุปหลัก: Key Stats – Key Actions

Key Stats	Key Actions
38.8% boards have no AI expertise	Upskill directors, recruit AI advisors
Only 9.2% boards fully confident in AI oversight	Integrate AI into ERM & strategy reviews
38.8% no AI policies	Develop board-approved AI ethics & privacy policies
Stakeholder trust fragile	Enhance transparency & communication
Regional divides in readiness	Monitor global best practices & adapt locally



## 7. บทส่งท้าย

- ❑ AI กำลังเป็นทั้ง โอกาสและความเสี่ยงระดับกลยุทธ์ ที่บอร์ดต้องกำกับดูแลอย่างจริงจัง ไม่ใช่เรื่องเฉพาะฝ่ายเทคโนโลยีอีกต่อไป
- ❑ บอร์ดที่ประสบความสำเร็จจะบูรณาการการกำกับดูแล AI เข้ากับกลยุทธ์ วัฒนธรรมองค์กร การจัดสรรทุน และการสร้างคุณค่าในระยะยาว
- ❑ AI เพิ่มความเร็วและขยายขอบเขตความเสี่ยงความเสี่ยงดั้งเดิม เช่น cyber fraud, misinformation หรือระบบล่ม ยิ่งทวีความรุนแรงเมื่อ AI เข้ามาเกี่ยวข้อง เพราะทำให้การโจมตี หรือการสร้างข้อมูลปลอมง่ายขึ้นและแนบเนียนขึ้น
- ❑ องค์กรต้องปรับกลยุทธ์ด้าน governance ไม่ใช่แค่ IT แต่บอร์ดและ Audit Committee ต้องเข้ามากำกับ ตรวจสอบ และตั้งคำถามกับ management อย่างต่อเนื่อง

**“Complacency around the risks of ...  
technologies should be avoided given the  
fast-paced nature of change in the field of  
AI and its increasing ubiquity.”**

WEF, Global Risks Report, 2025



# Auditing the Future: HOW AI IS REDEFINING THE AUDIT LANDSCAPE AND HOW YOU CAN BE PREPARED

# Introduction to AI Auditing

- **AI's Role in Internal Audit**

AI is now a vital tool in internal audit, changing decision-making and processes.

- **Proactive Risk Assessment**

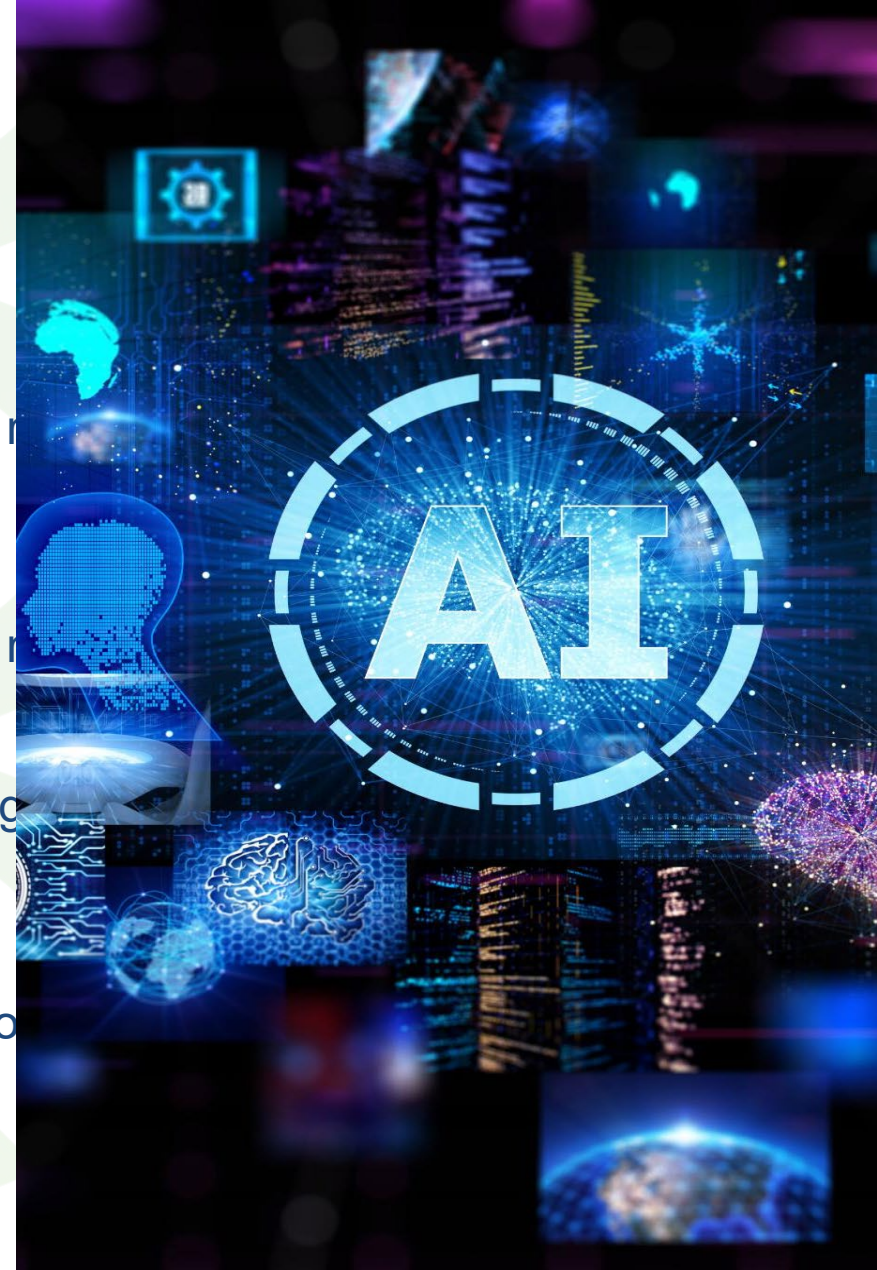
Machine learning enables auditors to shift from reactive to proactive risk assessment.

- **Enhanced Document Analysis**

Natural Language Processing helps auditors quickly and accurately gather insights from large documents.

- **Skill Development Necessity**

Training in AI skills is essential for auditors to effectively use technology while maintaining professional standards.





# 5 Ways Auditors Can Use AI Effectively

## Risk Analysis with Predictive Analytics

AI helps auditors analyze large datasets to predict risks like fraud or system failures in advance.

## Automated Evidence Collection

AI automates gathering data from logs, emails, and policies, reducing manual errors and saving time.

## Intelligent Control Testing

AI analyzes entire datasets instead of samples, accurately detecting anomalies and deviations from standards.

## Continuous Assurance & Real-time Alerts

AI provides continuous audit monitoring and real-time alerts for immediate corrective actions.

## Automation with Chatbots and Avatars

AI-powered chatbots assist auditees and help reduce auditors' workload by providing instant information.



# AI IN AUDITING: NOW AND IN THE FUTURE

The role of the auditor traditionally has been to provide assurance without bias and help reduce negative impacts to the organization. As we think of current auditor skills at a high-level, vs. the future auditor, there are some clear changes we can anticipate across four key areas – Skills, Efficiency, Risk Analysis and Monitoring.

The table below highlights some points that can be further assessed and thought through.

	PRESENT AUDITOR	FUTURE AUDITOR
SKILLS	Requires strong analytical skills and regulatory mindset	Use of AI tools and which areas can be automated vs. manual or hybrid
EFFICIENCY	The manual, human element is high	Data-driven, large matrixed environment of knowledge
RISK ANALYSIS	Sampling approach, judgmental	Pattern use, predictability and complex external and internal risk factors
MONITORING	Passive, reactive measurements	Proactive measures, embedded controls by design, digital auditor twin

# Risk Management Approach for Third-Party AI

## Defining AI Strategy and Requirements

Identify business challenges for AI and assess acceptable risk levels to set a clear strategy.

## Provider Selection and Risk Assessment

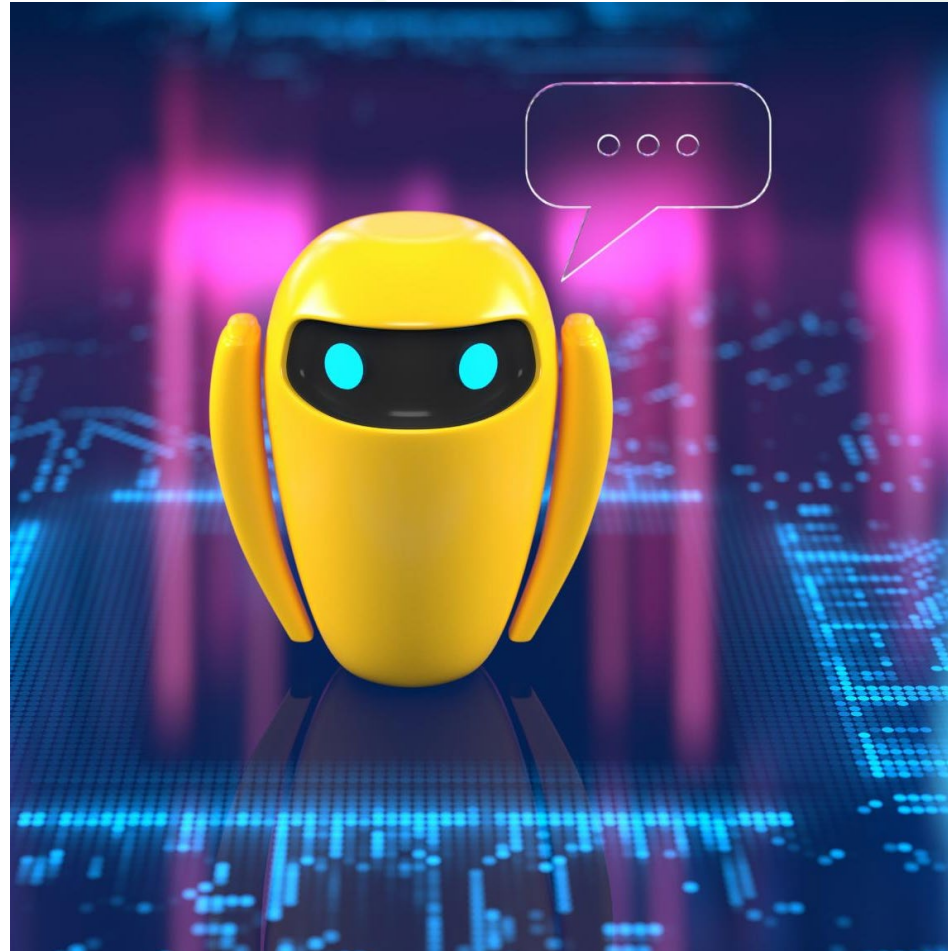
Analyze the market to prioritize third-party providers based on their importance and associated risks.

## Contract Management and Monitoring

Set risk-related contract terms, audit rights, and continuously monitor AI model performance.

## Safe Termination Procedures

Securely revoke system access and data, and consider switching providers for risk mitigation.



# How do we get started with AI auditing?



## Overall strategy for AI

- 1 Internal auditors should begin by researching and gathering relevant information regarding **the potential use of AI** under review from multiple internal and external sources.
- 2 Collaborate with management in reviewing an inventory to **capture which AI is being utilized** (or planned for future use).
- 3 Start the process of understanding what **AI governance is in place**.



## How is AI being used?

- 1 Internal auditors should have a discussion with the AI/data science/IT/Risk team. That discussion should include asking them to explain which **AI/algorithms have been deployed, including their function, sources of data used, use, limitations, risks and ethical implications**.
- 2 Internal auditors should also begin to understand what **existing controls are in place to help manage the risks posed by AI**.
- 3 Gaining a preliminary **understanding of the design of the controls** used to manage AI-related risk is an important step that can be performed in concert with these initial discussions.



## Data and cybersecurity

- 1 Internal auditors should determine **what organizational data is being used** within any given AI application and **how that data is managed**.
- 2 Understand **user access and who can edit or make changes to data**. Manipulating data sets from an input standpoint can impact the downstream output of AI.
- 3 Internal auditors need to determine where AI-reliant data is stored (internally, externally, or both) and **consider what cybersecurity controls are in place**.
- 4 Internal auditors must always **consider the risks related to third (and fourth) party transactions**.



# AI auditing

THE IIA'S  
Artificial  
Intelligence  
Auditing  
Framework

The IIA's AI Auditing Framework

Governance

Management

Internal Audit

Desirable Attributes for Artificial Intelligence

- Effective
- Valid
- Reliable
- Safe/Secure
- Unbiased
- Transparent
- Ethical
- Explainable

- Private
- Compliant with laws
- Fair
- Confidential
- Responsible
- Accurate
- Efficient
- Accountable

ISACA.

Artificial Intelligence Audit Toolkit

E	C	D	E	F	G	H	I	J	
High Risk Control?	Control Number	Control Family	Control Category	Control Name	AI-Specific Description of the Control	Rationale Explanation Description	Rationale Explanation Evidence/Debit/Debit/Debit	Rationale Explanation Assessment Types	
General	ADR-DM-01	Adversarial Defense & Robustness	Defensive Model Strengthening	Anomaly Detection Techniques	Develop and implement anomaly detection techniques to detect unusual or unexpected patterns, behaviors, or data points in the AI system. Document and analyze the anomaly detection results.	Anomaly Detection Techniques are implemented in an AI system to identify unusual or unexpected patterns, behaviors, or data points. The rationale for this control is to ensure that the AI system can make informed decisions by detecting and flagging anomalies, which may be indicative of errors or malicious activity. This explanation should be delivered in a non-technical and accessible way for various stakeholders.	Rationale Explanation Report: A document that provides a high-level overview of the need for anomaly detection techniques in the AI system and their role in ensuring data integrity and decision-making. Visual Representation: Diagrams or infographics that illustrate how anomaly detection works in the context of the AI system, making it easier for non-technical stakeholders to understand.	Examine: Review the Rationale Explanation Report to assess if it effectively communicates the importance of anomaly detection in the AI system. Interview: Discuss with responsible individuals to ensure they can explain the rationale clearly to non-technical stakeholders.	Doc Alig and Test score resp. Intra score test

Artificial Intelligence Risk Management Framework (AI RMF 1.0)








NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

ISO/IEC 42001:2023  
Artificial Intelligence Management System

ONE IN TECH  
SheLeadsTech

ISACA.

# Rising global regulatory guidelines for AI

Core governance principle	 Fairness	 Explainability	 Integrity of data	 Security & resiliency	 Accountability	 Privacy	 Risk approach
Global regulatory guidance							
National AI Initiative Act	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AI in Government	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
The National AI Research Resource Task Force				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
NIST AI Risk Framework	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FHFA AB 2020-02	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NAIC Principles on AI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Federal Trade Commission	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
EU Artificial Intelligence Act	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
EU Digital Services Act	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OECD Principles	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Social Principles of Human Centric AI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
AIST ML Quality Management Guideline	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
Brazilian AI Strategy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	
Brazilian AI Bill		<input checked="" type="checkbox"/>					
AI National Policy (Chile)		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
AI National Plan (Argentina)	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
AI Governance Guideline, ETDA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Generative AI Governance Guidance, AIGC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
AI Guidelines for Financial Sector, SEC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



# Preparing Auditors with AAIA

## AI Skill Gaps in Auditing

AI advancements create skill gaps in auditing, especially in governance and complex AI systems like Deep Learning.

## AAIA Certification Overview

AAIA certification helps auditors enhance skills in AI governance, operations, and auditing techniques.

## Governance Frameworks and Tools

Knowledge of frameworks like COBIT, NIST AI RMF, and ISO 42001 is critical for effective AI audit and risk assessment.

## AI Judgment and Human Review

AAIA emphasizes Generative AI judgment practice and human review to ensure accurate AI control assessments.



# AI Governance: Primer to Deep การกำกับดูแลปัญญาประดิษฐ์: จากพื้นฐานสู่เชิงลึก



AI Governance: Primer to Deep  
การกำกับดูแลปัญญาประดิษฐ์: จากพื้นฐานสู่เชิงลึก

October 14 - 15, 2025

Mandarin Samyan

สอบถามรายละเอียดได้ที่  
คุณประทีป วงศ์สินคงม่น  
โทร: 089-777-0900  
Email: training@isaca-bangkok.org

ISACA  
Bangkok Chapter

ลงทะเบียนกับที่

12  
CPE

\*วันแรกฟรี! ในวันขอบคุณ





