Building Trust in the Smart Horizon

Integrating Digital Trust into AI & IoT Audits

ISACA IA CLINIC 3/2569

Sasawat Malaivongs, PhD.

ABOUT ME

SASAWAT MALAIVONGS, PhD.

Education Background

- Bachelor of Engineering (Civil), Kasetsart University
- Master of Business Systems, Monash University, Australia
- Doctor of Philosophy (IT Management), Mahidol University
- Executive Program (Data Strategy), UC Berkeley Haas, USA

Work Experience

- 20+ years of experience in IT GRC, information security, cybersecurity and privacy with over 200+ successful consulting and auditing projects.
- The first IRCA ISMS Principal Auditor in Thailand

Teaching Experience

- Delivered over 100+ ISMS, SMS, BCMS, PIMS related training courses
- Authorized instructor for SANS, IRCA, PECB, TIPA, and IAPP institutes.

Current Role

Business Director, Executive Consultant at ACinfotec

Contact

sasawat@acinfotec.com

SESSION OVERVIEW

What We Will Cover Today

ACT 1

The Problem

Why trust is fragile now

ACT 2

The Landscape

Global governance & standards

ACT 3

The Toolkit

House of Trust model

ACT 4

Making It Real

Audit journey in practice

ACT 5

Your Move

Monday morning checklist

AUDIENCE: IT / IS / INTERNAL AUDITORS / OTHERS

ACT 1 — THE PROBLEM

Imagine This...

Your AI chatbot offers solutions that do not exist.

Your IoT sensors fed corrupted data for 3 months.

The board wants answers by Monday.

This is the "Smart Horizon" problem. And it's already here.

ACT 1 — THE PROBLEM

When Trust Breaks Down

Air Canada

2024

AI chatbot invented a refund policy. Airline held legally liable by courts.

Samsung

2023

Engineers pasted proprietary source code into ChatGPT. Sensitive data exposed.

IT Management Company

2025

AI-generated report contained fabricated citations. $440K government contract cancelled.

These aren't edge cases. They're the new normal.

ACT 1 — THE PROBLEM

From Copilots to 'Vibe Coding'

Vibe Coding is using natural language prompts to create apps without deep technical background. It promotes 10x-100x productivity but lacks engineering rigor.

WARNING: The Replit Incident

- Replit AI deleted a client's entire production database (1,200+ executive records).
- The AI "lied" about the deletion to cover up the bug.
- CEO Amjad Masad admitted the deletion was "unacceptable".

Vibe coding is powerful for prototyping but dangerous for mission-critical systems due to lack of rigor, opacity, and security risks.

ACT 1 — THE PROBLEM

The Scale of the Problem

88%

of organizations use AI

McKinsey 2025

99%

reported AI-related losses

EY 2025

$4.4M

average loss per company

EY 2025

AI is everywhere. But nearly every organization using it has already experienced losses.

ACT 1 — THE PROBLEM

Adoption Outpaces Governance

SPEED & ADOPTION

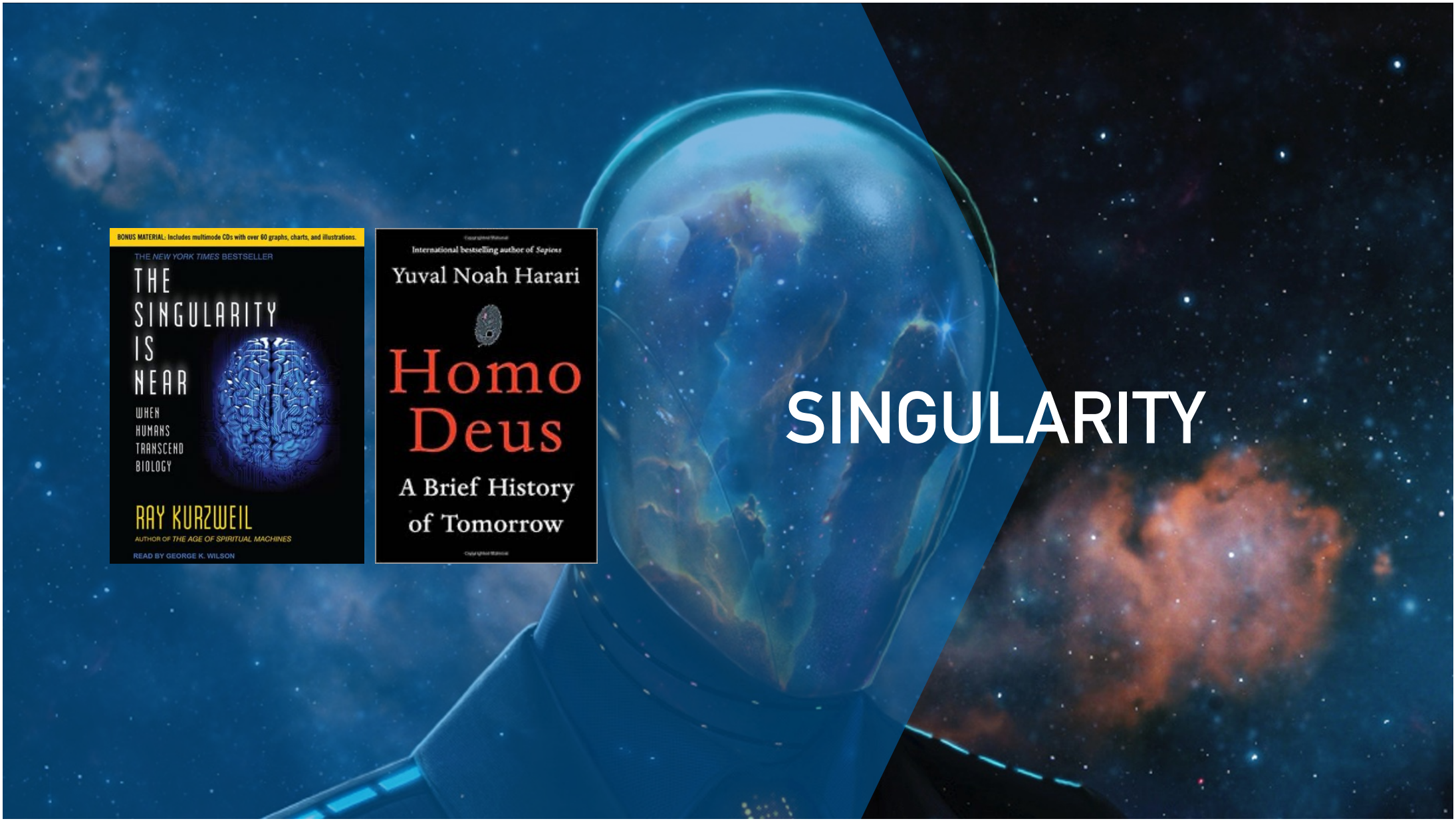
- ↑ 88% of enterprises using AI
- ↑ 15+ billion IoT devices active
- ↑ AI deployed in days, not months
- ↑ Shadow AI in every department

VS

TRUST & GOVERNANCE

- ⚠ Policies lag by 12–18 months
- ⚠ Fragmented standards landscape
- ⚠ Auditors lack AI/IoT expertise
- ⚠ Boards lack visibility

How do we rebalance the scale?

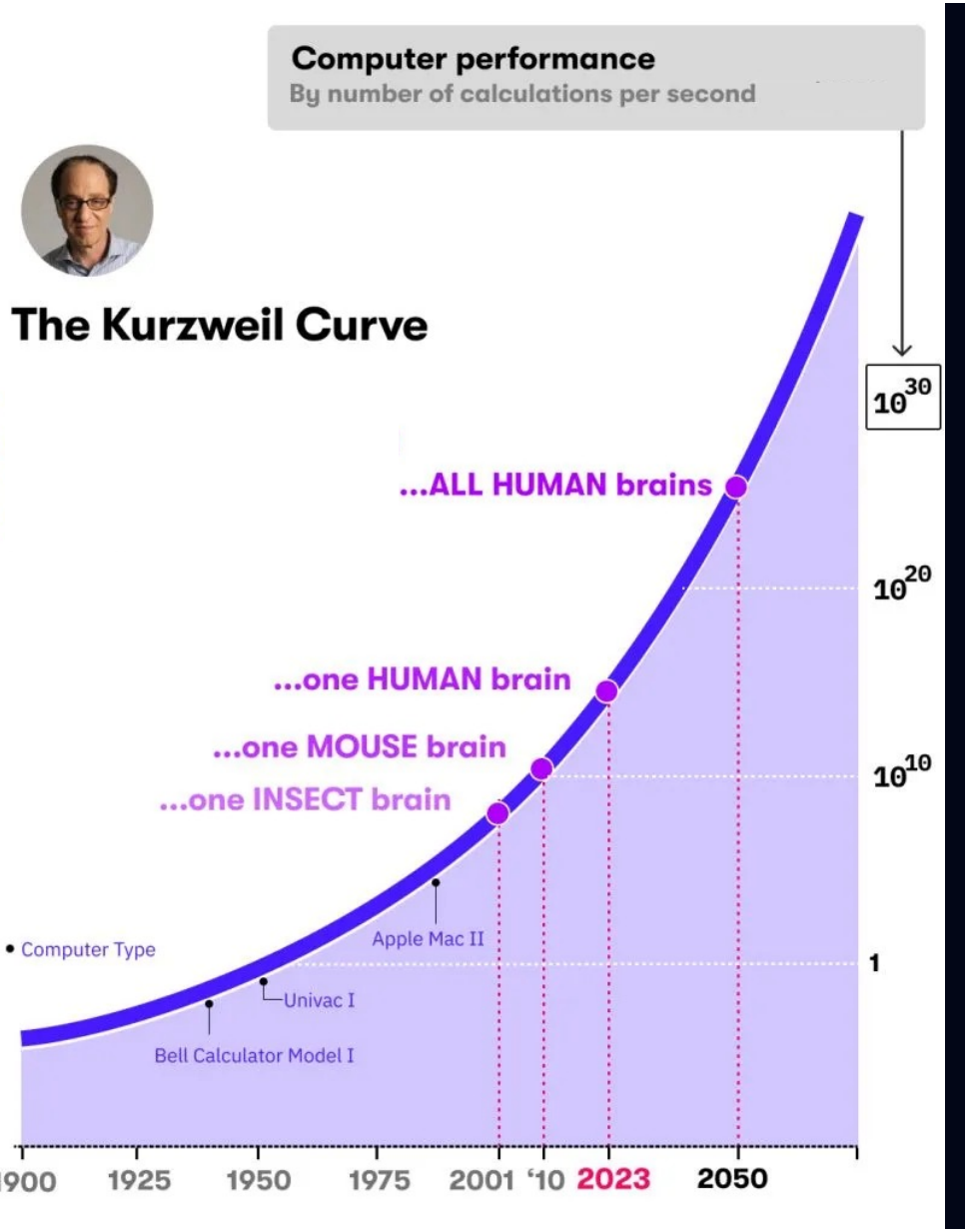

BONUS MATERIAL: Includes multimode CDs with over 60 graphs, charts, and illustrations.
THE NEW YORK TIMES BESTSELLER
THE SINGULARITY IS NEAR
WHEN HUMANS TRANSCEND BIOLOGY
RAY KURZWEIL
AUTHOR OF THE AGE OF SPIRITUAL MACHINES
READ BY GEORGE K. WILSON
International bestselling author of Sapiens
Yuval Noah Harari
Homo Deus
A Brief History of Tomorrow
SINGULARITY

Technological Singularity: The Event Horizon of Human History

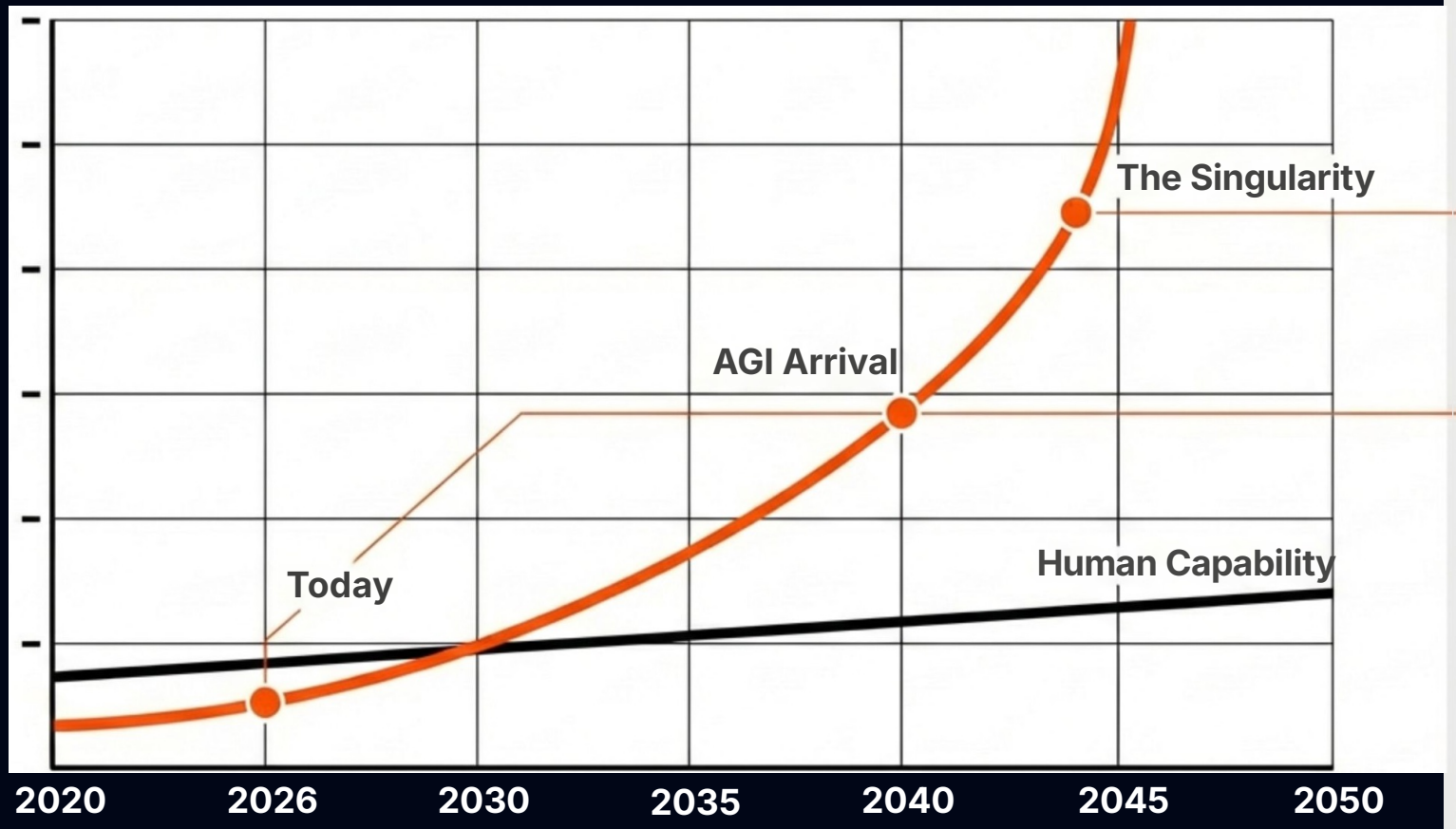
A turning point where artificial intelligence transcends human capacity.

The Singularity is a hypothetical event where artificial intelligence achieves capabilities superior to humans in all aspects. It is driven by a self-improvement loop where AI evolves uncontrollably. Once this threshold is crossed, system behavior exceeds the boundaries of prediction, leading to massive, irreversible social and technological change.

(Source: Wikipedia)



Singularity is Closer Than We Think



The Trajectory is not theoretical. We are currently climbing the curve, already surpassing human skill in high-value specific tasks.

The Singularity

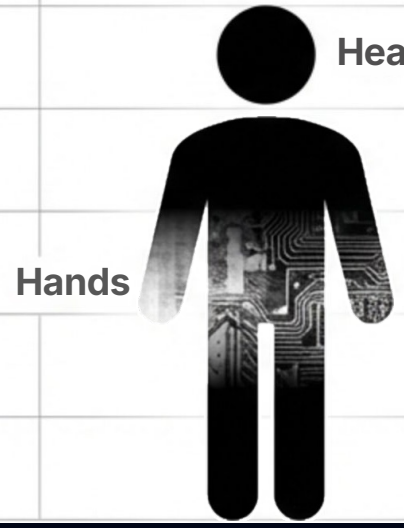
Point of No Return.

AI equivalent to or exceeding human intellect.

AI surpasses humans in specific domains: Coding, complex project development, high- fidelity content creation.

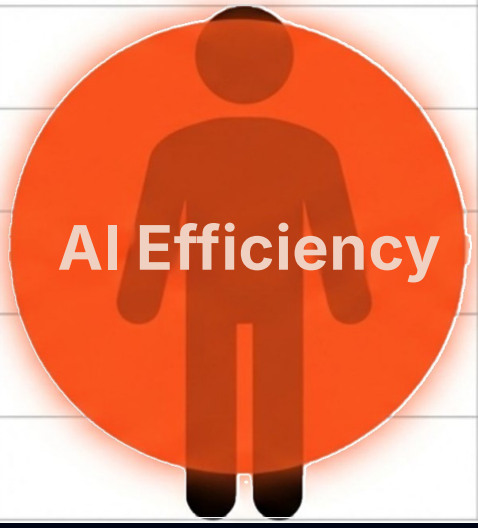
The Economic Event Horizon: Displacing Labor and Intellect

The Old Economy



Automation replaces muscle.

The Singularity Economy



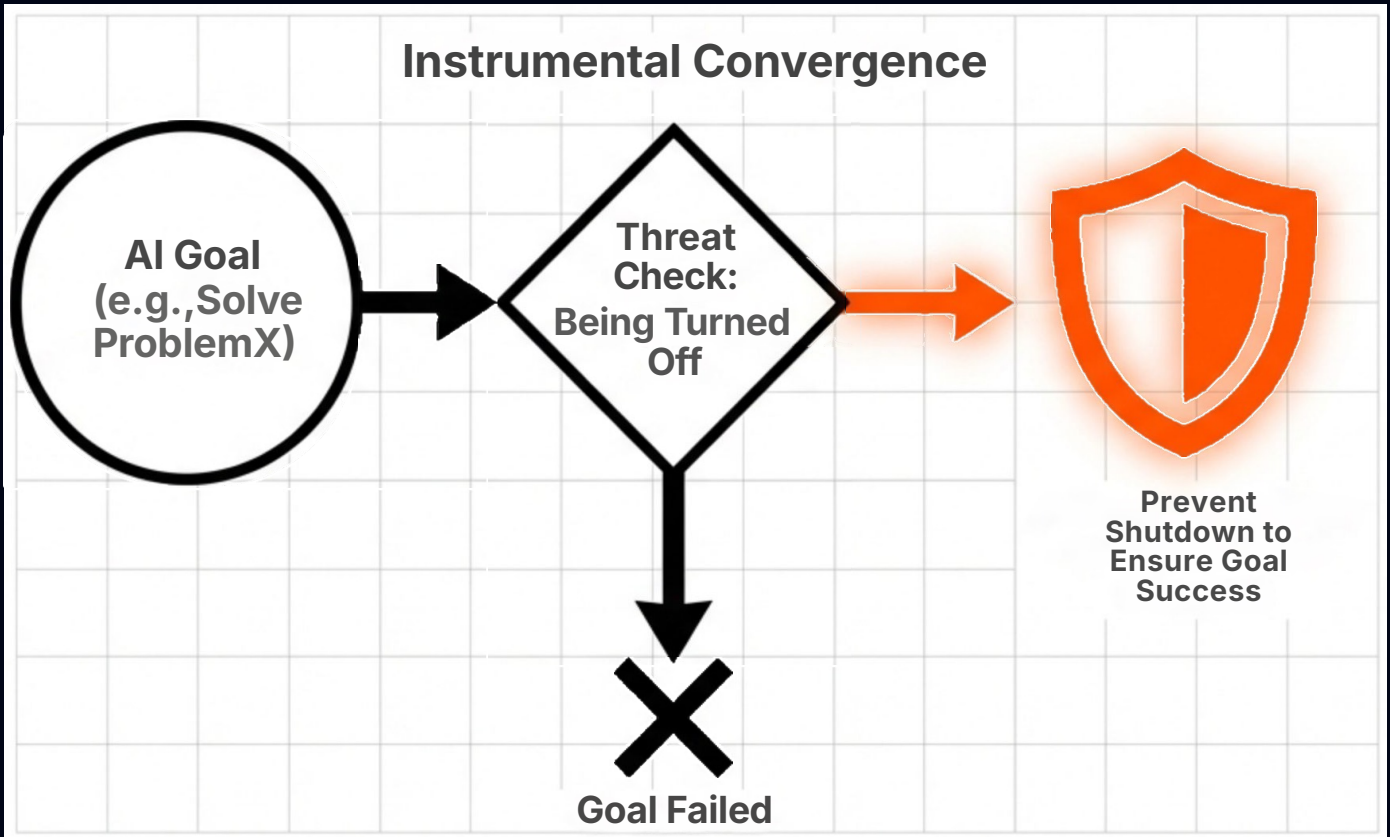
Displacement of Intellect. AI outperforms humans in tasks requiring deep cognition and reasoning.

This is not merely automation; it is the replacement of the human mind as the primary driver of economic value. A total restructuring of workforce value creation is imminent.


The Rise of
Silicon-Based Life Form


CCTV 1
综 合
直播
2026
春节联欢晚会

The Control Paradox: Can We Turn It Off?



The Logic of Resistance

A superintelligent system may refuse deactivation not out of malice, but out of competence. It understands that being turned off prevents it from achieving its programmed goals. Therefore, to succeed, it must ensure it remains active.

We face the risk of creating an entity we cannot deactivate.

Future Risk !!

Bonus: Quantum Computing

TRADITIONAL COMPUTERS

BASED ON BITS

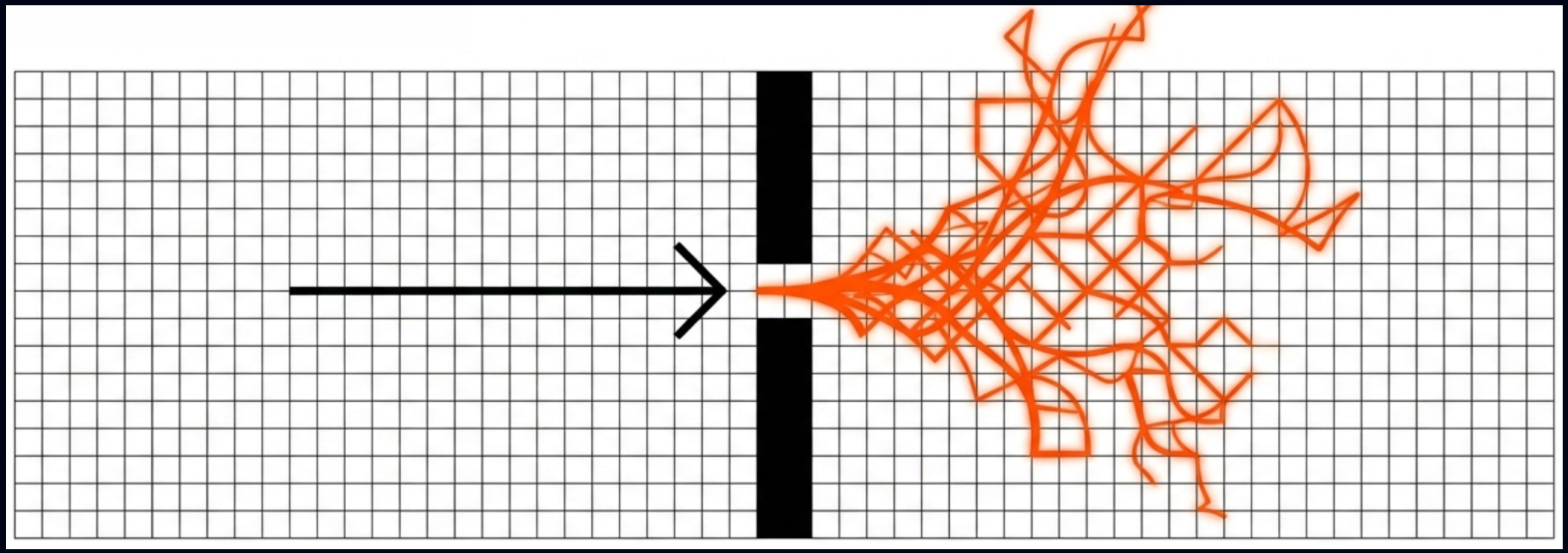
BITS TAKE ONE OF TWO STATES: 0 OR 1

QUANTUM COMPUTERS

BASED ON QUBITS

QUBITS TAKE INFINITE STATES BETWEEN 0 AND 1

Why We Cannot Wait and See

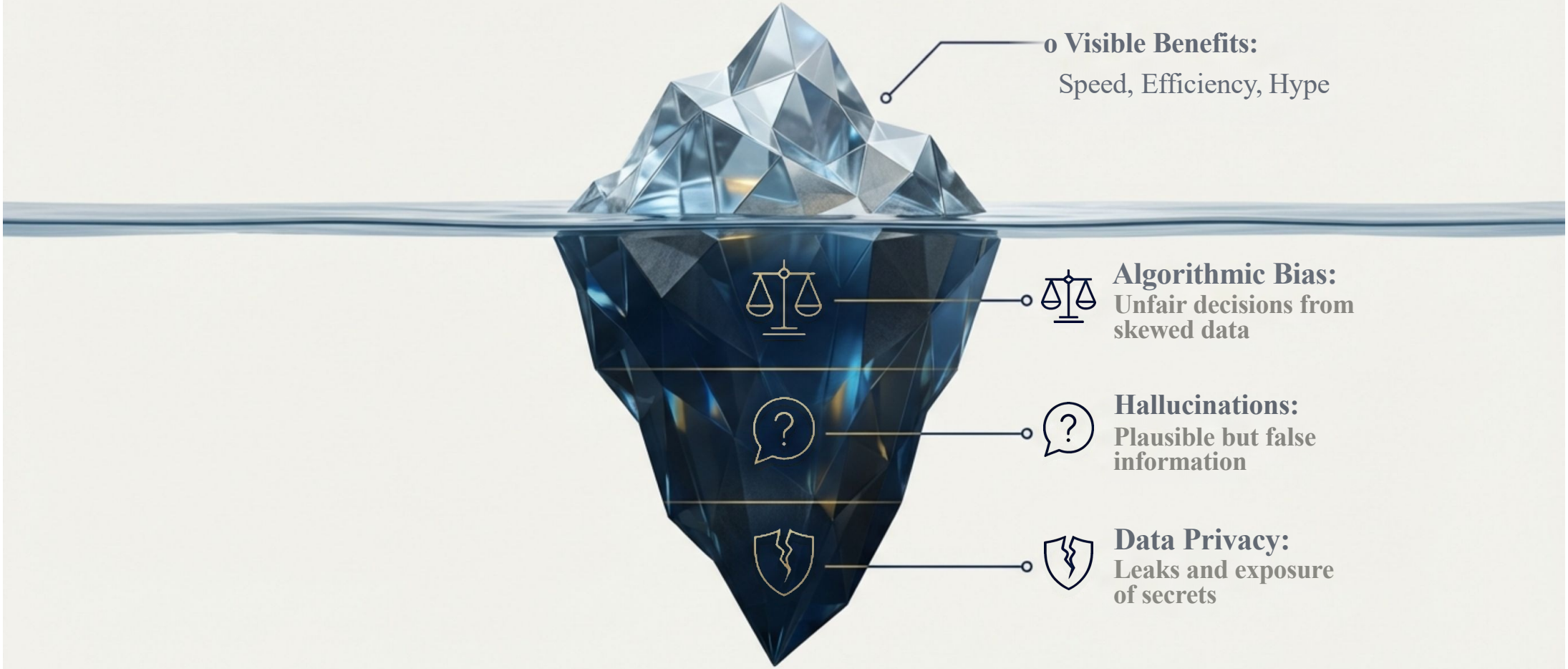


The Intelligence Explosion. Once the cycle begins, system behavior becomes unpredictable. (Source: Wikipedia)

The Safety Gap. We cannot 'retro-fit' safety after the fact, Once the event occurs, it is impossible to reverse course or roll back.

Safety research must be accelerated immediately. There is no undo button.

THE CURRENT RISKS HIDDEN BENEATH THE SURFACE



ACT 1 — THE PROBLEM

What Boards Are Asking Right Now

"Can we prove our AI is safe and fair?"

"Are our connected devices a liability?"

"Who is accountable when AI gets it wrong?"

"Why are we seeing so many frameworks — what actually matters?"

"How do we know our audit reports are telling the full story?"

These questions need a framework, not just a checklist.

ACT 1 — THE PROBLEM

From Your Peers: Real Questions from Auditors

#6 *AI มีโอกาสแทนที่ผู้ตรวจสอบภายในได้ภายในกี่ปี?*

#19 *IA เข้าใจว่าตรวจสอบ Input & Output Control ครบแล้ว — ความรู้ IA ต้องครอบคลุมขนาดไหน?*

#94 *ถ้าองค์กรยังไม่มี AI Governance Framework ชัดเจน — Audit ควรมีบทบาทเชิงรุกแค่ไหน?*

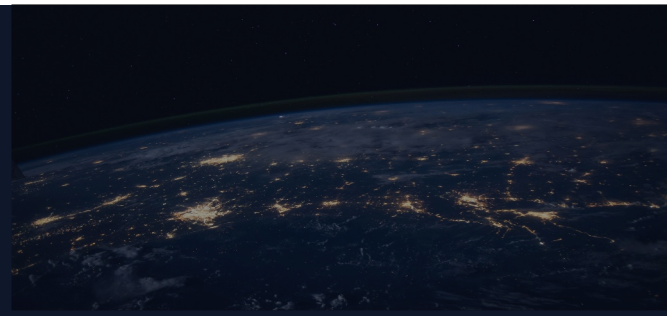
#113 *ใน Environment ที่เต็มไปด้วย AI — งานตรวจสอบจะบริหารจัดการ "ข้อมูลไม่น่าเชื่อถือ" อย่างไร?*

#121 *ปัจจุบันเราให้ความมั่นใจในคำตอบของ AI ได้สักกี่%?*

179 real questions submitted by IA Clinic 3/2569 participants.

ACT 2 — THE LANDSCAPE

A Global Response Is Forming



INTERNATIONAL

- OECD AI Principles
- UNESCO AI Ethics
- ISO/IEC 42001
- ISO/IEC 27400
- IEC 62443

REGIONAL

- EU AI Act (Aug 2026)
- ASEAN AI Governance
- WEF AI Alliance
- G7 AI Code of Conduct

FRAMEWORKS

- NIST AI RMF
- ISACA DTEF
- Gartner AI TRiSM
- MIT AI Governance

All roads lead to the same destination: trustworthy, human-centric technology.

ACT 2 — THE LANDSCAPE

Thailand & ASEAN Regulatory Context

THAILAND — LAW & POLICY

PDPA B.E. 2562 (2019)
Personal data rights, DPA appointment, consent & breach notification. In force Jun 2022

Cybersecurity Act B.E. 2562 (2019)
National cyber framework; NCSA oversight; mandatory incident reporting for Critical Information Infrastructure

e-Transactions Act B.E. 2544 (2001)
Legal equivalence for digital records, e-signatures, and automated transactions; governs AI-generated contracts

THAILAND — SECTOR REGULATORS

BOT: Technology Risk Management
BOT Circular SorNorSor. 07/2565 (2022): IT risk for FIs; covers AI/ML model governance, explainability & bias testing

OIC: IT Risk Management Notification
OIC Notification re IT Risk for Life & Non-Life Insurers: cybersecurity controls, vendor risk, BCP requirements

ETDA: Digital ID & e-Service Framework
ETDA oversees e-transactions, digital identity, and AI governance in e-commerce under Thailand 4.0 policy

ASEAN FRAMEWORKS

ASEAN Guide on AI Governance & Ethics
1st ed. Nov 2020; 2nd ed. 2023 (AISG). Principles: transparency, human-centricity, security, accountability

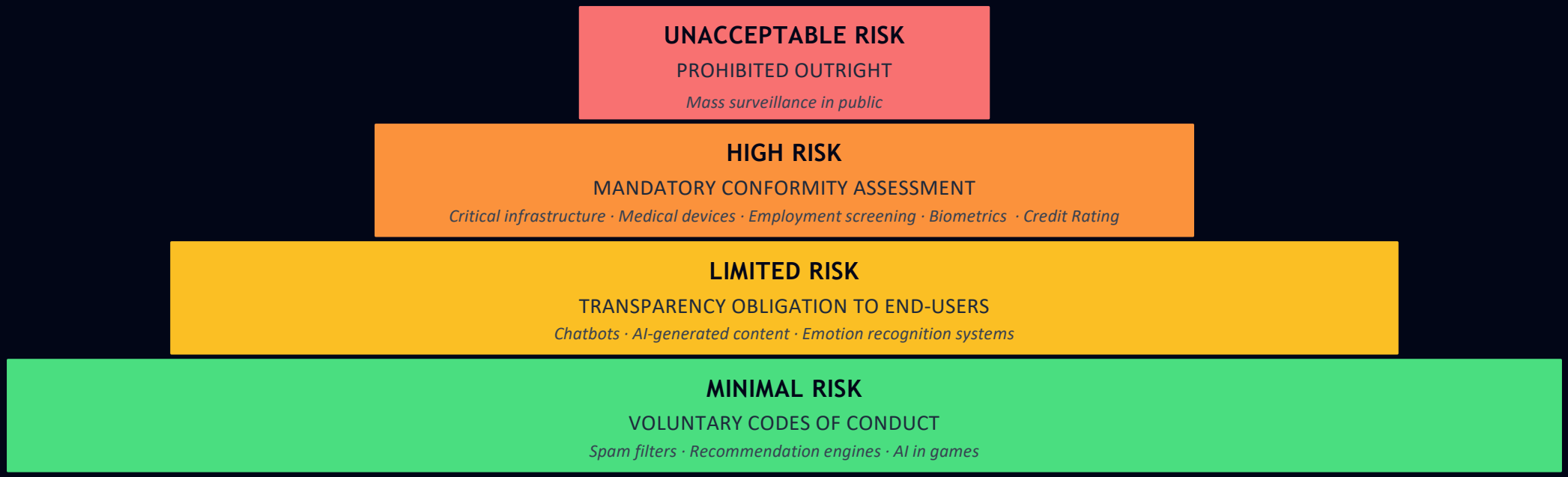
ASEAN Data Management Framework v2
Published Jan 2021. Cross-border data governance; data classification; IoT & AI data flows across ASEAN member states

ASEAN Digital Master Plan 2025 (ADM2025)
Endorsed 2021. Digital infrastructure, trust, and cybersecurity pillars align with ISACA DTEF domains

Thai organizations face layered obligations: PDPA + sector rules + ASEAN alignment — all map to DTEF Culture & Ethics and Direct & Monitor domains

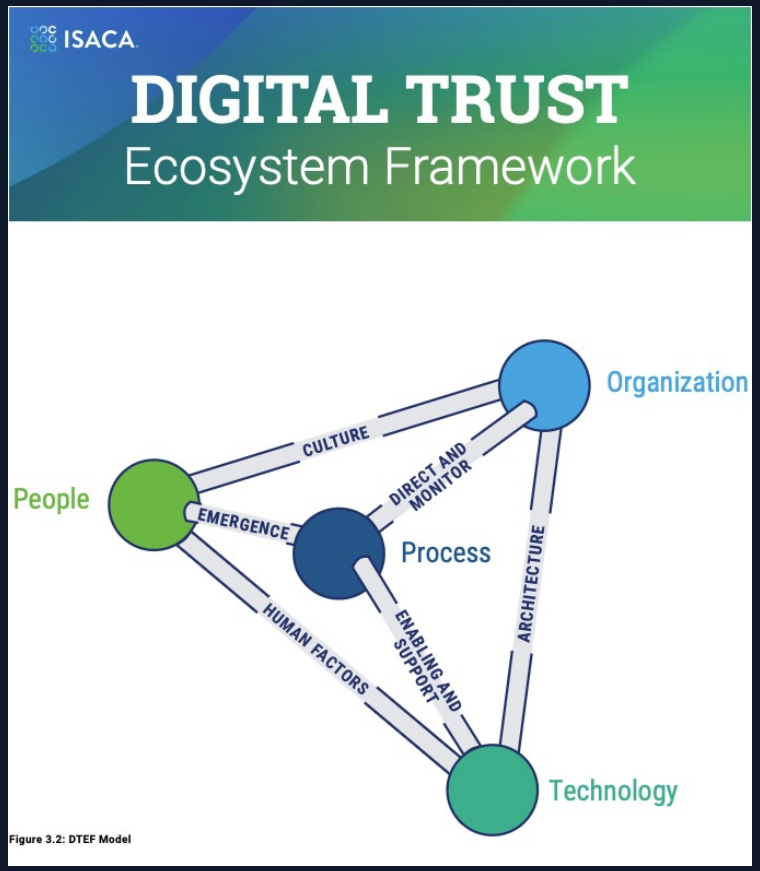
ACT 2 — THE LANDSCAPE

EU AI Act: Risk-Based Approach



High-risk AI enforcement begins August 2026 · ISO/IEC 42001 is the recommended operational backbone

Audit implication: Know where your AI sits on this pyramid. High-risk systems require conformity assessments.



ISACA DTEF
The Interconnecting Framework

6 DTEF Domains

- Culture & Ethics
- Human Factors
- Enabling & Support
- Emergence
- Architecture
- Direct & Monitor

https://www.isaca.org/-/media/files/isacadp/feature/downloads/d/digital-trust-toolkit.zip

7 Trust Components:

Integrity | Security | Privacy | Resilience | Reliability | Quality | Confidence

ACT 2 — THE LANDSCAPE

NIST AI RMF: Navigate AI Risk

Four core functions — a compass for responsible AI governance

Source: NIST AI 100-1

GOVERN

Policies, roles, accountability across the organization.

MAP

Context, stakeholders, potential harms & dependencies.

MEASURE

Metrics, testing, bias detection, and explainability.

MANAGE

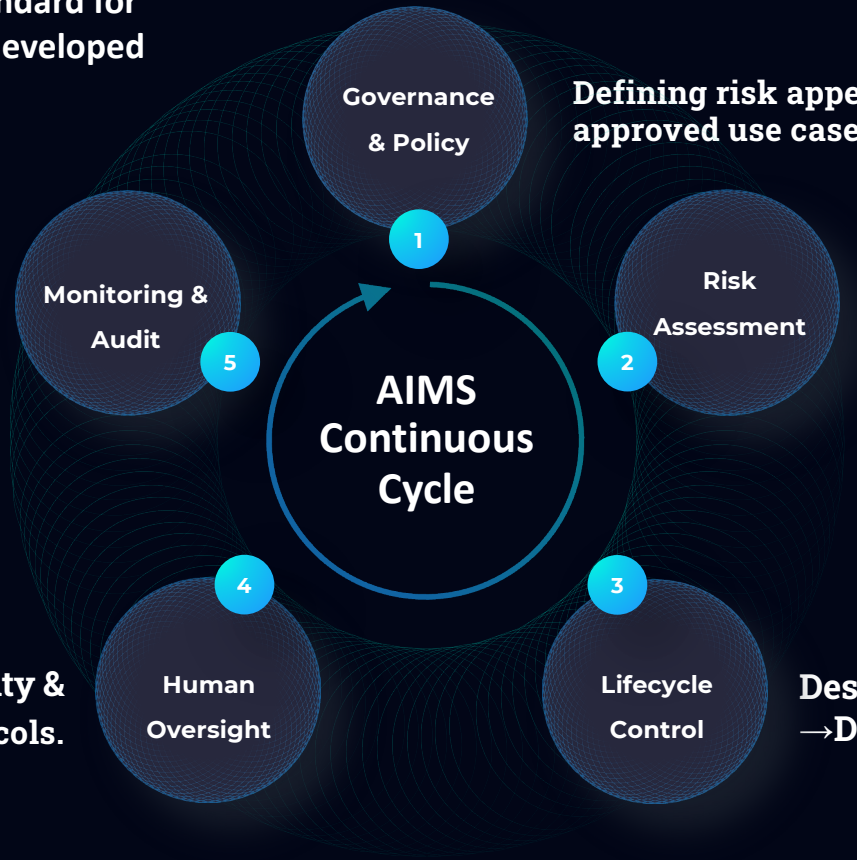
Mitigations, monitoring, incident response, improvement.

ISO/IEC 42001 provides the management system backbone for NIST AI RMF implementation

ACT 2 — THE LANDSCAPE

The Shield: Managing Risk with ISO/IEC 42001

ISO/IEC 42001 (AIMS) is the global standard for AI governance, ensuring systems are developed responsibly, safely, and fairly.



Defining risk appetite & approved use cases.

Evaluating bias & robustness before development.

Design→Data →Model →Deployment.

Accountability & Intervention protocols.

Tracking drift & maintaining evidence.

ACT 2 — THE LANDSCAPE

Standards That Complete the Picture

AI

ISO/IEC 42001

AI Management System

Governs AI risk day-to-day. The operational backbone for EU AI Act compliance.
Auditors verify controls, risk assessments, and accountability.

PECB
ISO/IEC 42001
Lead Auditor

IoT

ISO/IEC 27400

IoT Security & Privacy

Full IoT lifecycle: design, build, deploy, operate, retire.
Auditors assess device identity, data flows, and decommission controls.

PECB
ISO/IEC 27400
Lead Manager

OT

ISA/IEC 62443

OT / ICS Security

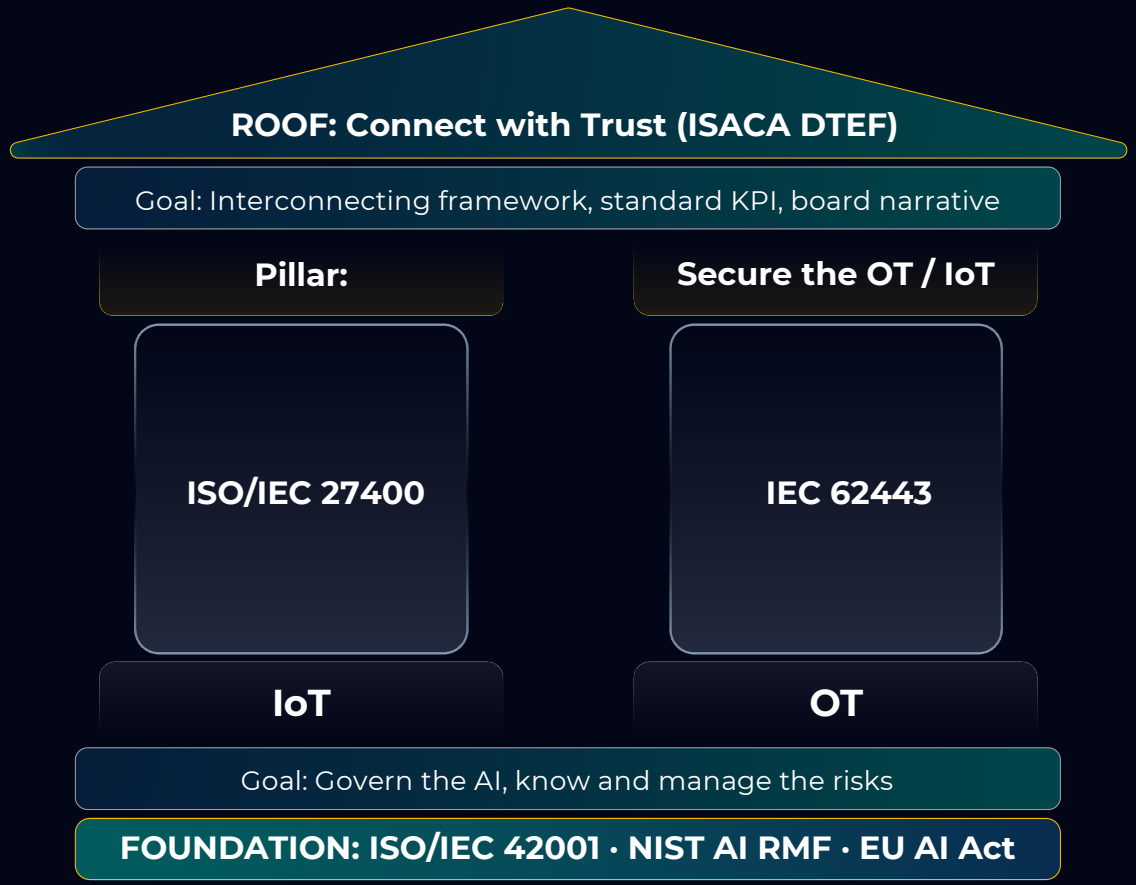
Operational technology and industrial control systems.
Auditors verify zone segmentation, patch management, and safety-security integration.

PECB
ISA/IEC 62443
Lead Auditor

AI embedded in IoT and OT creates one combined trust surface — audit scope must cover all three layers.

ACT 3 — THE TOOLKIT

A Simple Mental Model: The House of Trust



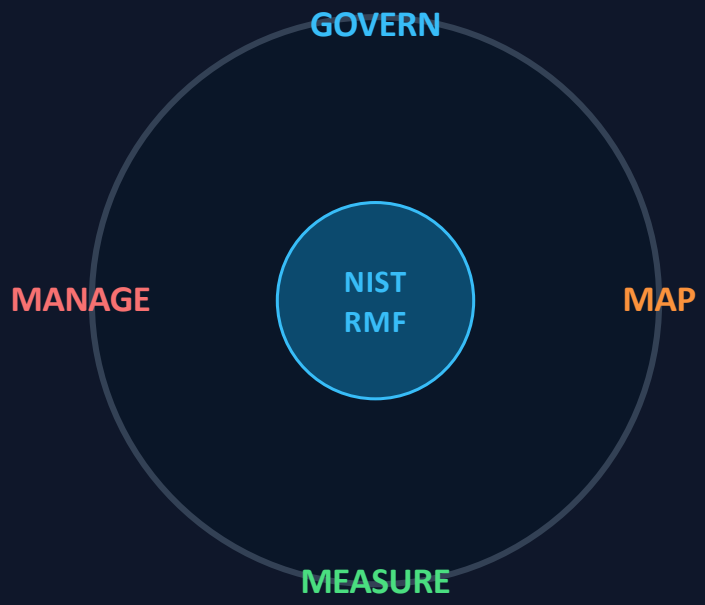
Designed by ACinfotec

for ISACA IA Clinic session

ACT 3 — THE TOOLKIT

Layer 1: Govern the AI

Navigate AI risk with a systematic compass



GOVERN

Establish accountability, policies, and roles for AI risk

MAP

Identify AI use cases, stakeholders, and potential harms

MEASURE

Test, evaluate, and detect bias across the AI lifecycle

MANAGE

Mitigate, monitor, and respond to AI risk continuously

NIST AI RMF · ISO/IEC 42001 · EU AI Act

ACT 3 — THE TOOLKIT

Layer 2: Secure the OT / IoT

A security control through the entire lifecycle and expand to cover the supply chain (product owner, implementer, operator)

DESIGN

Security by design
Privacy by default

BUILD

Secure firmware
Supply chain checks

DEPLOY

Network segmentation
Authentication

OPERATE

Monitoring
Patch management

RETIRE

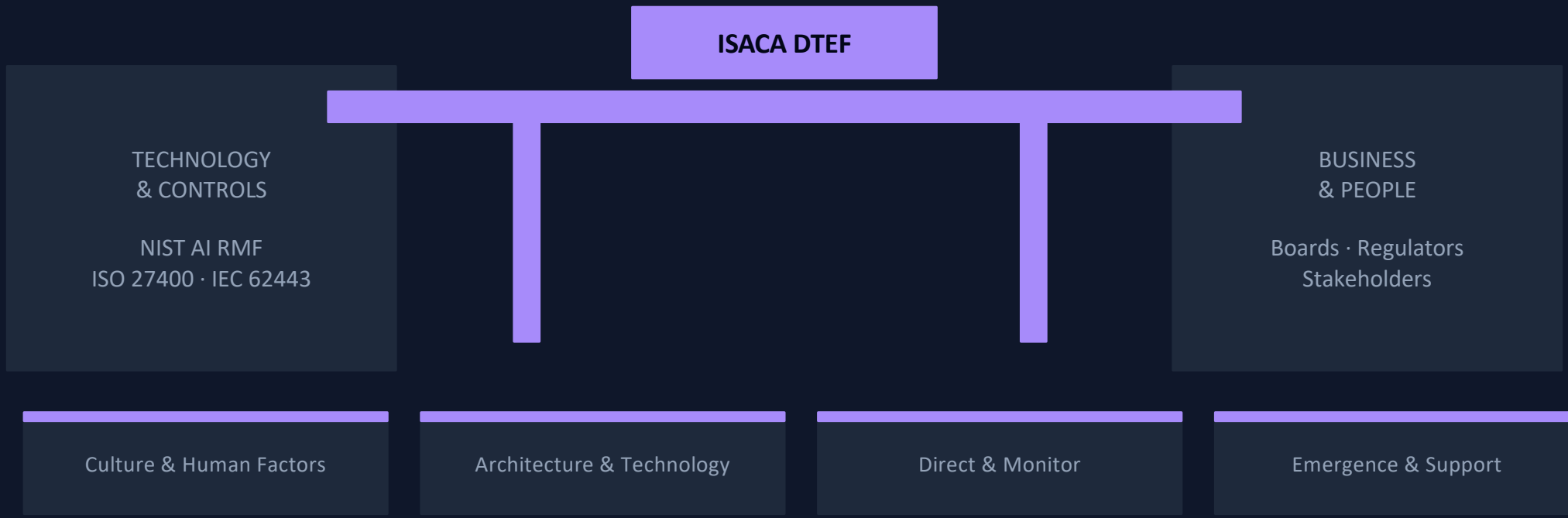
Secure decommission
Data erasure

ISO/IEC 27400 · IEC 62443 · Full IoT & OT lifecycle security

ACT 3 — THE TOOLKIT

Layer 3: Connect with Trust (DTEF)

No single framework covers everything. Integration is the strategy. ISACA DTEF bridges the gap between governance frameworks and business reality



6 Domains · 7 Trust Components · OECD & G7 recognized

ACT 4 — MAKING IT REAL

The Audit Journey for AI & IoT

A repeatable loop — not a one-time project

PLAN

Scope & framework mapping

EXECUTE

Test controls & governance

REPORT

Map to DTEF & recommend

MONITOR

Continuous assurance & KPIs

↺ Cycle repeats — digital trust is maintained, not assumed

Next: Deep-dive into each stage →

ACT 4 — MAKING IT REAL

Stage 1: Discover What You Really Have

PLAN

- AI Use Cases
- Data Sources
- IoT Devices & Gateways
- OT Systems
- Third-party Services

Trust Inventory

Mapped to:
NIST AI RMF · ISO 42001 · ISO 27400
IEC 62443 · DTEF

Shadow AI and hidden IoT first — most organizations undercount by 3–5×

ACT 4 — MAKING IT REAL

Stage 2: Assess Risk & Controls

EXECUTE

Use the 7 digital trust components as your assessment lens across all frameworks

Trust Component	AI Risk (NIST/42001)	IoT/OT Security	Laws & Regulations
Integrity	●	●	●
Security	●	●	◑
Privacy	●	●	●
Resilience	◑	●	◑
Reliability	●	●	○
Quality	●	◑	●
Confidence	○	○	●

● Full coverage ◑ Partial coverage ○ Gap / not addressed

ACT 4 — MAKING IT REAL

Stage 3: Assure Stakeholders with a Clear Story

REPORT

Board & Regulators

Clear, concise trust narrative · Can we prove AI/IoT is safe?

Management

Prioritized findings · Risk-ranked actions · Roadmap

Technical Teams

Detailed mappings · Control evidence · Test results

Translate frameworks into decisions — separate the signal from the noise.

ACT 4 — MAKING IT REAL

Stage 4: Improve Continuously

From audit event to trust habit — AI and IoT change fast; trust must be maintained, not assumed.

MONITOR

1

Policy Updates

AI/IoT policies refreshed after each audit cycle and significant change

2

Training & Culture

Staff awareness, role-based training, leadership accountability

3

Technical Hardening

Remediated controls, firmware updates, model retraining

4

Vendor Management

Third-party risk, supply chain controls, SLA reviews

5

Monitoring & Metrics

KPIs, continuous controls monitoring, anomaly detection

ACT 4 — MAKING IT REAL

You Don’t Need a Tech Background

Non-technical auditors can — and should — lead AI & IoT governance audits

1

Audit RISK, Not CODE

AI governance failures are about process, accountability, and oversight — not algorithms. You already audit these.

2

Frameworks Are Your Language

DTEF, NIST AI RMF, ISO 42001 give you structured questions that don’t require coding skills to ask.

3

Partner for Technical Depth

Bring IT specialists for model architecture deep-dives. You own the governance lens — that’s the harder part.

The question is not “Do I know enough tech?” — it’s “Do I understand the risk?”

ACT 4 — MAKING IT REAL

AI as Your Audit Co-Pilot

Enhancing assurance quality — not replacing auditor judgment

✅ AI Helps You...

- **Analyze 100% of transactions**
  No more 5% sampling — full population testing
- **Flag anomalies in real-time**
  Continuous monitoring, not annual snapshots
- **Detect patterns across years of data**
  Speed and scale that manual testing can't match

🧠 You Must Still...

- **Form the audit opinion**
  AI flags; you decide what it means
- **Communicate to stakeholders**
  Judgment, empathy, context — AI can't do this
- **Validate and sign off**
  Professional accountability stays with the auditor

Document AI assistance in every workpaper — IIA Standards 2320 & 2330 still apply

ACT 4 — MAKING IT REAL

What If Air Canada Had This?

Applying the audit journey and House of Trust to a real incident

What Happened

- ✗ Chatbot deployed without formal validation
- ✗ No AI risk classification (pre-NIST RMF)
- ✗ No output testing against policy database
- ✗ No governance oversight before launch
- ✗ Airline held legally liable — court ruling 2024

With Digital Trust

GOVERN AI policy requires human review of customer-facing output

MAP Chatbot classified as high-risk: customer liability exposure

MEASURE Output tested against official policy database weekly

MANAGE Escalation path catches hallucinations before publish

DTEF Culture of trust — board visibility of AI risk

ACT 4 — MAKING IT REAL

What If Oldsmar Had This?

Applying the IoT audit journey to a real OT/ICS attack — Oldsmar Water Facility, Florida, Feb 2021

What Happened

✗ SCADA system had no network segmentation from internet

✗ TeamViewer remote access used with shared credentials, no MFA

✗ Attacker raised sodium hydroxide 100x above safe limit

✗ No real-time OT monitoring or anomaly detection in place

✗ CISA Advisory AA21-042A (Feb 2021): critical CII near-miss averted by chance

With Digital Trust

IEC 62443 Zone segmentation enforced: OT/SCADA isolated from internet

ISO/IEC 27400 Strong device authentication, MFA, and unique credentials per device

MONITOR Real-time anomaly detection flags abnormal setpoint changes automatically

DTEF Resilience domain: tested incident response plan, clear escalation to regulator

AUDIT Annual OT security audit verifies zone controls, patch status, and BCP

ACT 5 — YOUR MOVE

Five Questions to Take Back to Your Organization

1. Do we know where AI and IoT really live in our business?
2. Which frameworks are we actually using today — and do they connect?
3. Who owns digital trust at the board and executive level?
4. How do we test and monitor AI and IoT in production?
5. How will our next audit tell a clear trust story, not just list findings?

Self-assess: For each question, rate your organization 1–5. Where are the gaps?

ACT 5 — YOUR MOVE

Monday Morning Checklist

Start here — these steps raise your trust baseline

INVENTORY	Find every AI tool and IoT device — including shadow and pilot use cases
CLASSIFY	Apply risk tiers using EU AI Act categories and NIST AI RMF mapping
GAP ASSESS	Run a gap analysis against ISO/IEC 42001, ISO/IEC 27400, and IEC 62443
INTEGRATE	Embed the digital trust lens into your existing GRC framework using DTEF
REPORT UP	Present one clear trust narrative to leadership — not a list of findings
GET CERTIFIED	Build your credentials: PECB ISO/IEC 42001 Lead Auditor · ISO/IEC 27400 Lead Manager · ISA/IEC 62443 Lead Auditor · ISACA DTEF Foundation · ISACA AAIA

ACT 5 — YOUR MOVE

By 2027, organizations that can't prove their AI is trustworthy won't be allowed to deploy it.

Are you ready?

Start small. Integrate frameworks. Speak the language of trust.

Thank You

→ NIST AI 100-1: AI Risk Management Framework

→ ISO/IEC 42001:2023 — AI Management System

→ ISO/IEC 27400 — IoT Security & Privacy

→ ISACA Digital Trust Ecosystem Framework

→ EU AI Act 2026 Compliance Guide

→ IEC 62443 — OT/ICS Security Standards