Integrating Cybersecurity, AI & Quantum Risk, into Enterprise Risk Management (ERM)

Prinya Hom-anek, Thailand

CISSP, CSSLP, SSCP, CASP, CFE, CBCI, CSX, ITIL Expert, CDPSE
COBIT 5 Foundation, COBIT 5 Implementation

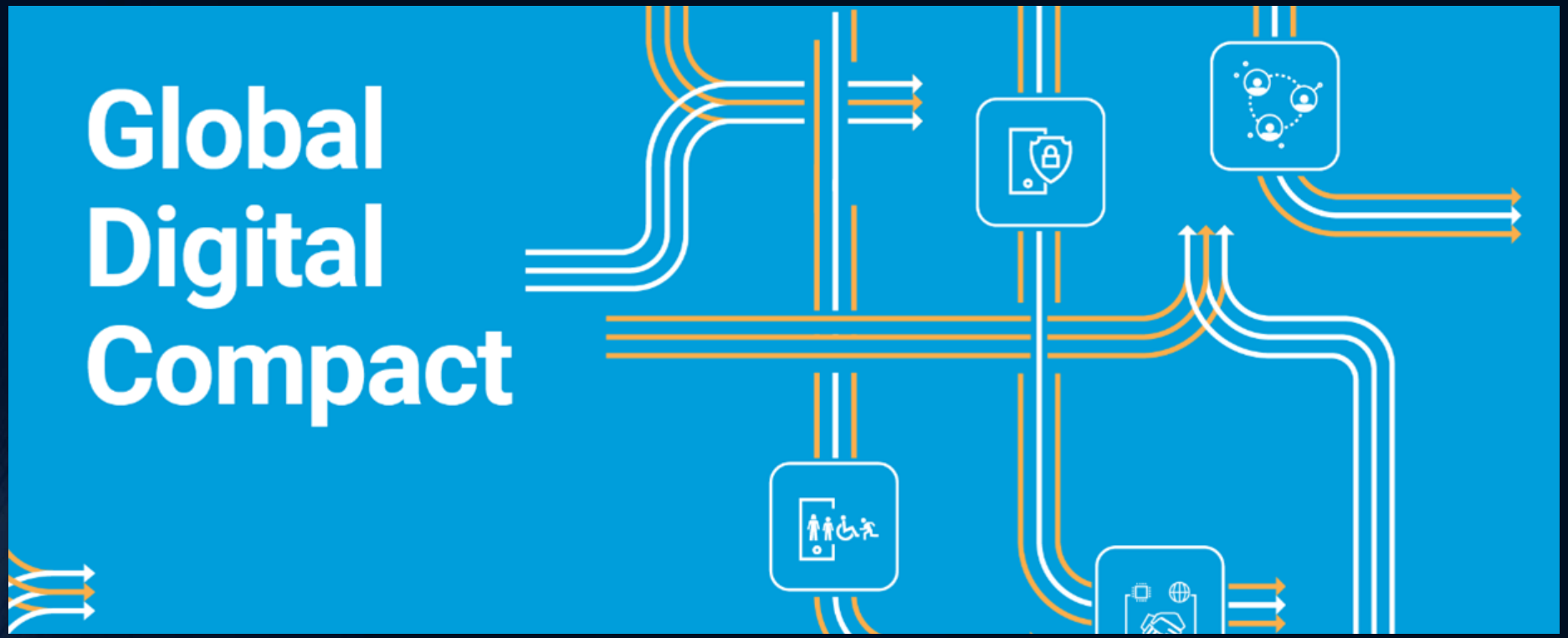
Eisenhower Fellowships 2013, Member of (ISC)² Asian Advisory Council,
ISACA Bangkok, Thailand Information Security Association (TISA) Board Member,
Cybertron Co., Ltd. – ACIS Professional Center – Chairman of Executive Committee

ACIS/Cybertron Privacy & Cyber Security Research LAB

The World Global Trends 2020-2030

ACIS & Cybertron 9 Countries Journey 2023-2024

GLOBAL DIGITAL COMPACT



GDC กับกรอบ 8 เรื่องที่ต้องพัฒนาไปสู่ความยั่งยืน

Topics

- Connectivity
- Avoiding Internet Fragmentation
- Data Protection
- Applying Human Rights Online
- Accountability for Online Content
- Regulating Artificial Intelligence
- Digital Commons
- Others

GDC (Global Digital Compact)

CYBER RESILIENCE LEADERSHIP : SMART GOAL

UN Global Digital Compact (GDC)

1. Digital inclusion and connectivity
2. Internet Governance
3. Data Protection
4. Human Rights Online
5. Digital Trust
6. Regulating Generative AI
7. Global digital commons
8. Accelerating progress towards the SDGs

Future Trends

1. Digital inclusion and Financial Inclusion
2. Embedded Finance
3. Cybersecurity & Generative AI
4. Strategy & Sustainability
5. Digital Trust
6. Open Banking
7. BaaS (Banking as a Service)
8. Fraud and Identity Management (IdM)

The World Hot IT/Cyber Topics in 2024-2025

Cybersecurity Culture	The Rise of Generative AI / LLM	Digital Trust	Data Security Data Privacy	Data Governance	Data Resilience
Digital Literacy/ Digital Inequality	Cyber Dominance	SDG	ESG	GDC	Data Sovereignty
Behavioral Science	Cloud Security	AI Governance	Supply Chain Risks	Behavioral Economic	Human-operate Ransomware
Cyber Resilience	AI-Driven Threats	Cyber Sovereignty	Data Breach	Information Advantage	Reputational Risks

From Digital Transformation to AI Transformation

Megatrends 2025-2030

Genderless	Generative AI/ LLM	AGI	AI Governance	Climate Change and Environmental Sustainability
Multiple Identities	Gig Economy	Aging Society/ Urbanization	Cyber Dominance	Energy Transition
Health consciousness	Attention Economy	ESG/SDG/GDC	Information Advantage	Evolving Global Economic Power

From Digital Transformation to AI Transformation

WORLD ECONOMIC FORUM

The Global Risks 2025

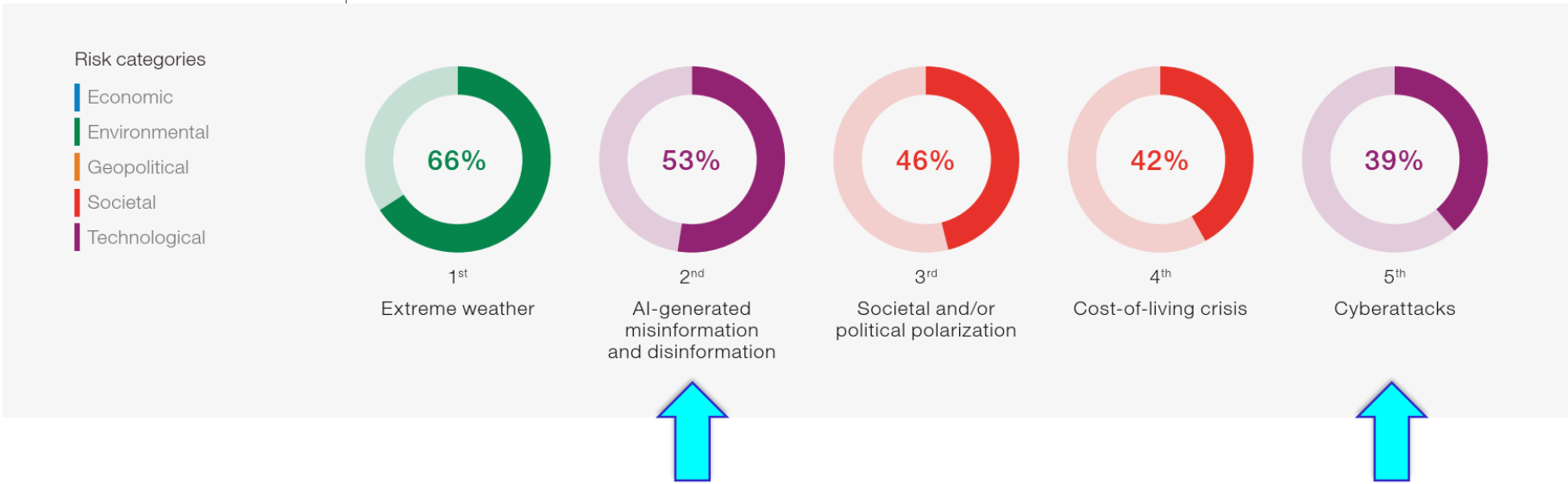
WEF : The Global Risks Report 2024-2025

(cont.)

FIGURE B

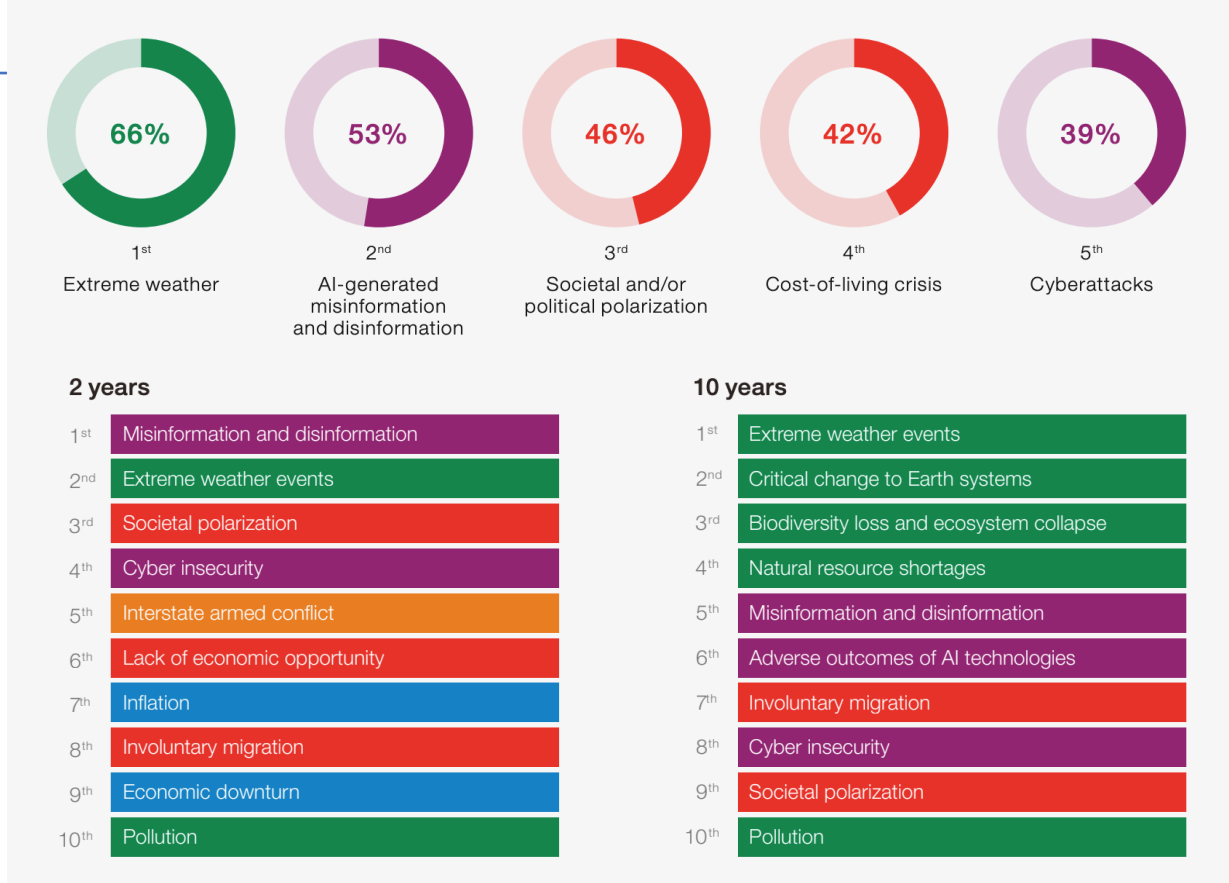
Current risk landscape

"Please select up to five risks that you believe are most likely to present a material crisis on a global scale in 2024."



WORLD ECONOMIC FORUM

Global Risk Landscape and Global Risks Ranked by Severity over Short and Long Term



Risk categories
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

ACIS PROFESSIONAL CENTER | ALL RIGHTS RESERVED

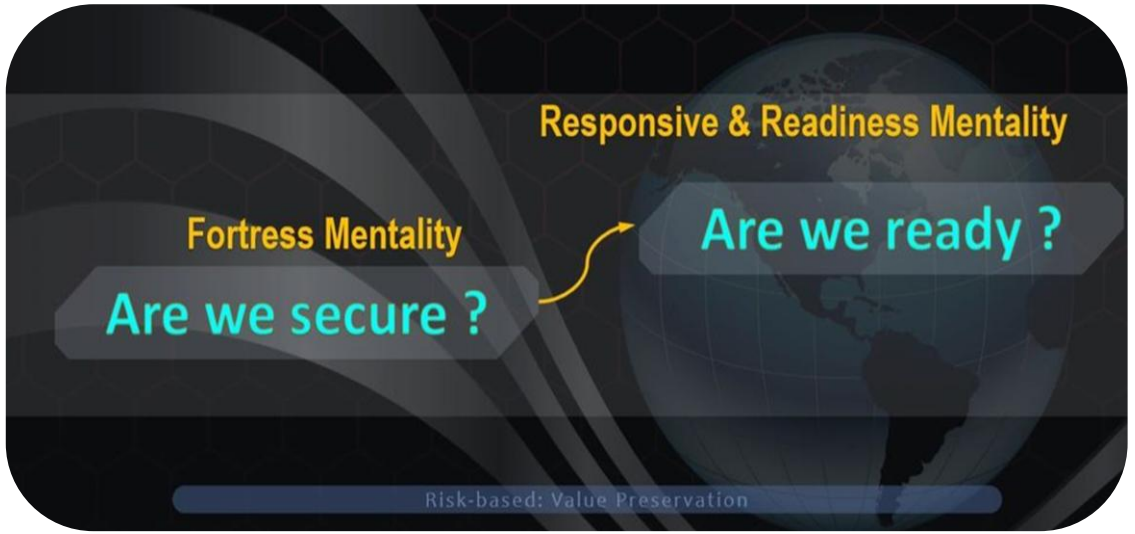

WORLD ECONOMIC FORUM
The Global Risks Report 2026
21st Edition
INSIGHT REPORT


In collaboration
with Accenture
WORLD
ECONOMIC
FORUM
Global Cybersecurity
Outlook 2026
INSIGHT REPORT
JANUARY 2026

History & Revolution of Cyber Domain

1st Generation	2nd Generation	3rd Generation	4th Generation	5th Generation
(1986) Computer Security	(2005) Information Security	(2013) cybersecurity	(2011/2023) Cyber Resilience Data Hacking	(2020/2030) Cyber Dominance Mind Hacking

TOWARDS:
RESPONSIVE SECURITY



History & Revolution of Cyber Domain

1st Gen : Computer Security (1986) (hack system)

2nd Gen : Information Security (2005) (hack data)

3rd Gen : Cybersecurity (2013) (hack data)

4th Gen : Cyber Resilience (2011/2023) (hack data)

5th Gen : Cyber Dominance (2020/2030) (hack mind)

History & Revolution of Cyber Domain

1st Gen : Computer Security (1986) (HW & SW)

2nd Gen : Information Security (2005) (ISO/IEC 27001)

3rd Gen : Cybersecurity (2013) (NIST CSF 1.1->2.0)

4th Gen : Cyber Resilience (2011/2023) (CISA CRR)

5th Gen : Cyber Dominance (2020/2030) (AI to IA, ADP 3-13)

Cybersecurity Risk and ERM Alignment (Cont.)

Comparison of IT Risk, Cyber Risk, and Digital Risk

	IT Risk	Cyber Risk	Digital Risk
Definition	The risk associated with the failure of IT systems, infrastructure, and processes.	The risk of financial loss, disruption, or reputational damage due to cyberattacks or data breaches.	The risk associated with digital transformation, technology adoption, and digital assets.
Scope	Primarily focused on IT systems, hardware, software, and processes.	Specific to cybersecurity threats, including hacking, malware, phishing, and data breaches.	Broader focus, including IT and cyber risks, as well as risks from digital business models, customer interactions, and digital ecosystems.
Key Risks	System failures, data loss, IT process issues, hardware and software obsolescence.	Unauthorized access, data theft, malware, ransomware, phishing attacks.	Technology adoption risks, third-party digital risks, compliance with digital regulations, brand reputation, and digital market changes.
Impact Areas	IT operations, data integrity, system availability.	Data security, business continuity, financial loss, regulatory fines.	Strategic business outcomes, digital customer experiences, operational and reputational impacts.

Cybersecurity Risk and ERM Alignment (Cont.)

Comparison of IT Risk, Cyber Risk, and Digital Risk

	IT Risk	Cyber Risk	Digital Risk
Management Approach	IT governance, system controls, regular maintenance, disaster recovery planning.	Cybersecurity frameworks, threat monitoring, incident response, vulnerability management.	Integrated digital risk management (IDRM), digital strategy alignment, cross-functional risk assessment.
Stakeholders	IT department, system administrators, technology teams.	Cybersecurity teams, risk management, compliance officers.	C-suite, business leaders, digital transformation teams, and IT and cybersecurity departments.
Regulatory Concern	Compliance with IT standards (e.g., ITIL, COBIT).	Compliance with cybersecurity regulations (e.g., NIST, ISO 27001, GDPR).	Compliance with broader digital regulations, including data privacy, e-commerce laws, and emerging tech regulations.
Example	Server crashes, network outages, software bugs.	Ransomware attack, data breach, phishing scams.	Missteps in digital transformation, poor digital customer experience, disruption in digital services.

From Digital Transformation

To

Cyber Resilience Transformation
&
Gen-AI Transformation

Future World Trend : Digital Sovereignty

Future World Trend : Digital Sovereignty

Source: ZEXTRAS

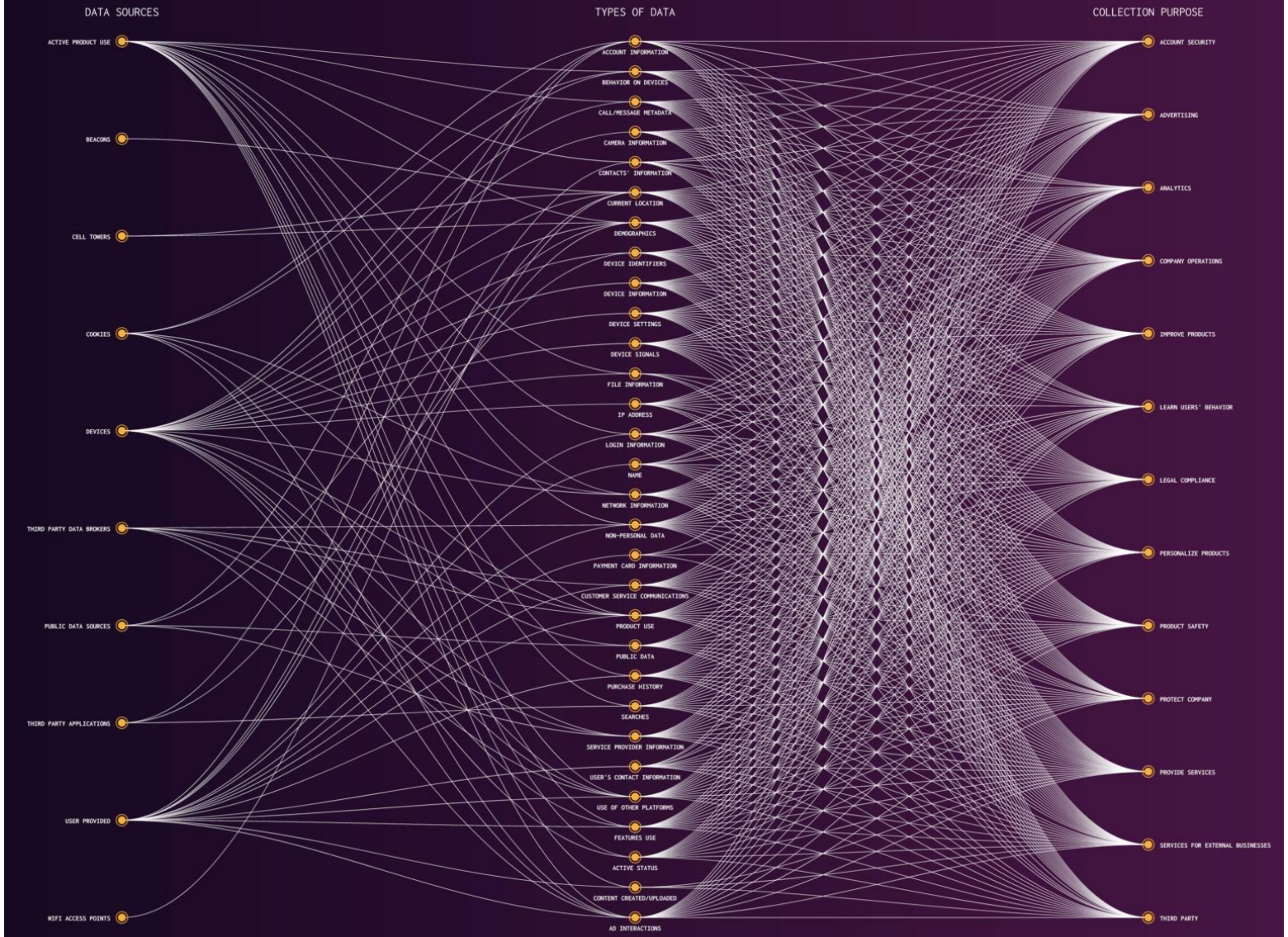
COLUMBIA | SIPA
Technology and Policy Initiative

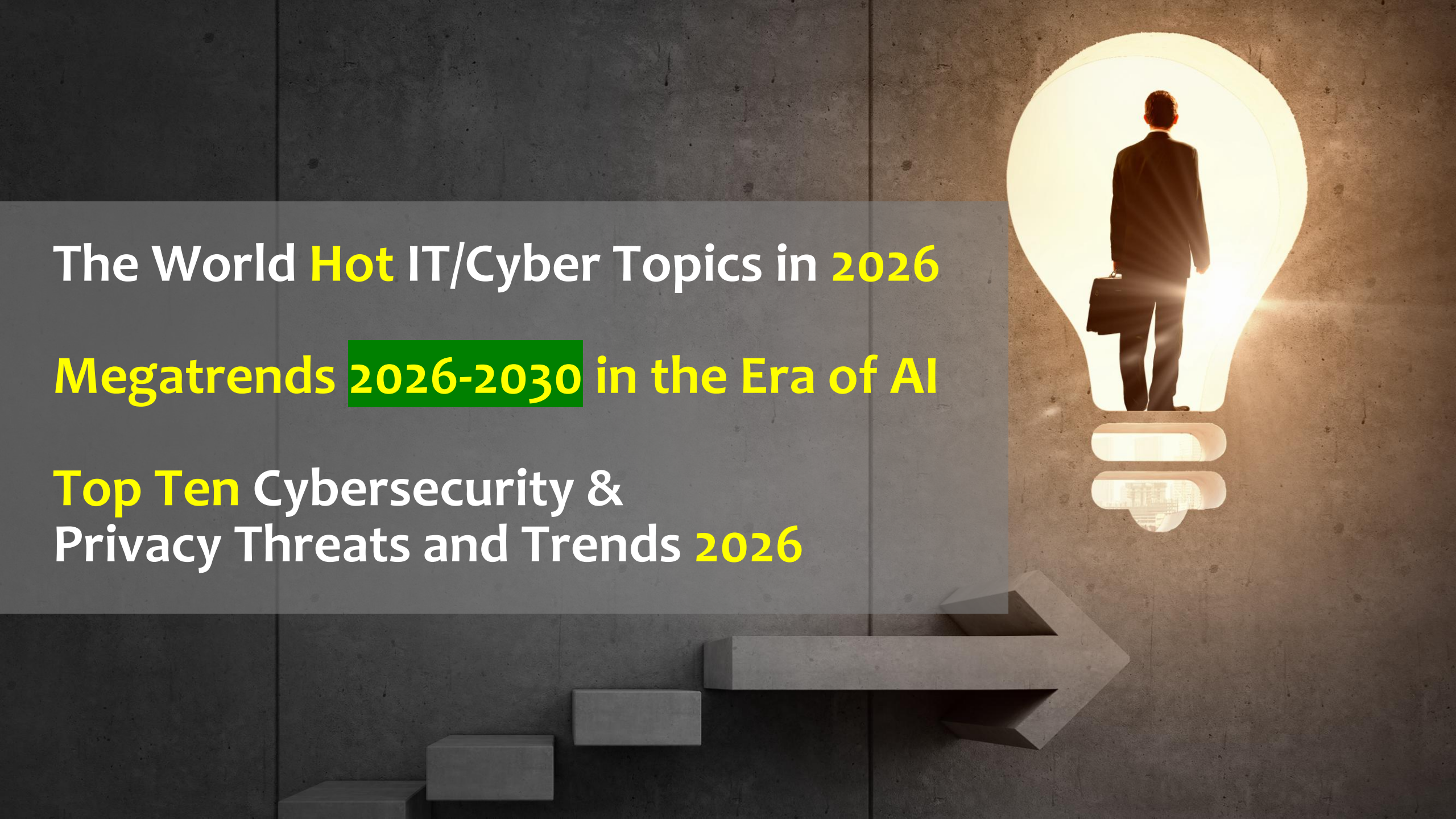
MAPPING DATA FLOWS - ZOOM EDITION

Given its very recent and extraordinary rise as a consumer tool, we decided to apply the Mapping Data Flows approach to Zoom's terms of service as well. You can find our initial findings below.

Return to the "Big Four" visualization.

TYPES OF DATA [All types] COLLECTION PURPOSE [All purposes] COLLECTION METHOD [All Methods] RESET FILTERS





The World Hot IT/Cyber Topics in 2026

Megatrends 2026-2030 in the Era of AI

Top Ten Cybersecurity & Privacy Threats and Trends 2026

The World Hot IT/Cyber Topics in 2026

Digital Sovereignty	From Gen AI to Agentic AI	AGI/ Quantum	AI Sovereignty	AI Governance	Cybersecurity Risk integrate in ERM
AI Literacy/ AI Inequality	Cyber Dominance	SDG	ESG	GDC	Data Sovereignty
Privacy Risks	From IT Risk to Cyber Risk	From Cyber Risk to Digital Risk	Supply Chain Risks	Harvest Now Decrypt Later (HNDL)	Human in the Loop (HITL)
Cyber Resilience	AI Bubble	Digital Trust	Privacy Engineering	Integrating Cyber Risks into Enterprise Risks	Vibe Coding

From Digital Transformation to AI Transformation

The evolving organizational governance landscape

Sustainability

Why Governance?

"sustainable development cannot be realized without…good governance at all levels and transparent, effective and accountable organizations"

(UN Agenda 2030)

Dr Victoria Hurth : Among other achievements she co-led the 5-year development of the first global ISO standard in Governance of Organizations (ISO 37000:2021).

ISO 37000 GOVERNANCE OF ORGANIZATIONS - Notes accompanying Ryerson University CSR Institute "in conversation" session (December 15, 2021)

https://www.torontomu.ca/content/dam/csrinstitute/pdf/Ryerson-Univ-CSR-Institute-ISO37000-Dr-Victoria-Hurth-Dec15-2021.pdf

Global Trends towards 2030 : Sustainability and Governance GDC, ESG, SDGs

Global Digital Compact

UN ICC Report :
Global Digital Compact (GDC)

OBJECTIVES AND ACTIONS :

- **A. Digital Connectivity and Capacity-Building**
- **B. Digital Cooperation to Accerate Progress on the Sustainable Development Goals**
- **C. Upholding Human Rights**
- **D. An Inclusive, Open, Secure, Shared Internet**
- **E. Digital Trust and Security**
- **F. Data Protection and Empowerment**
- **G. Agile Governance of AI and Other Emerging Technologies**
- **H. Global Digital Commons**

ESG

ENVIRONMENTAL	SOCIAL	GOVERNANCE
Energy usage and efficiency	Fair pay and living wages	Corporate governance
Climate change strategy	Equal employment opportunity	Risk management
Waste reduction	Employee benefits	Compliance
Biodiversity loss	Workplace health and safety	Ethical business practices
Greenhouse gas emissions	Community engagement	Avoiding conflicts of interest
Carbon footprint reduction	Responsible supply chain partnerships	Accounting integrity and transparency
	Adhering to labor laws	

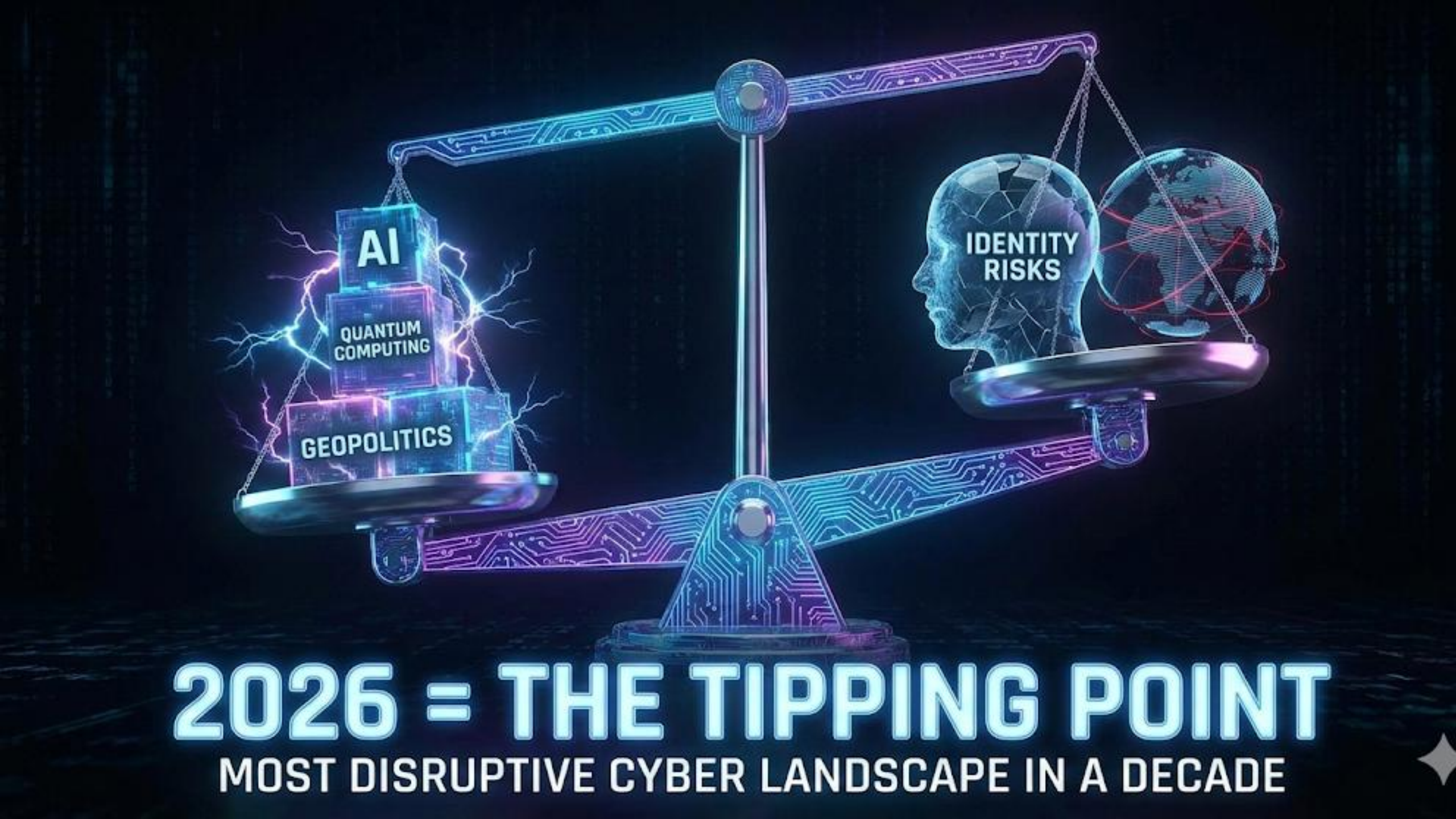
SUSTAINABLE DEVELOPMENT GOALS

17 GOALS TO TRANSFORM OUR WORLD

Megatrends 2026-2030 in the Era of AI

From Knowledge Economy to Trust Economy	From Gen AI to Agentic AI	Mandatory AI Governance & AI Risk Management	AI Governance in Action	Digital Detox & Privacy
Geopatriation (Geo-Politics + Repatriation)	The Blue-Collar Renaissance	Quantum Transition & PQC Mandate	Responsible AI Becomes a Legal Requirement	Energy Transition Reality
Cybersecurity Arms Race 2030	AI Act (AI Infra,AI Sovereignty)	AI-Specific Regulations	Third-Party AI & Vendor Risk Becomes Critical	Climate Adaptation

From Digital Transformation to AI Transformation
"digitize processes" → "intelligent, autonomous enterprise"


AI
QUANTUM COMPUTING
GEOPOLITICS
IDENTITY RISKS
2026 = THE TIPPING POINT
MOST DISRUPTIVE CYBER LANDSCAPE IN A DECADE

TOP TEN CYBERSECURITY & PRIVACY THREATS AND TRENDS 2026

Future Scenarios and Defensive Strategies

Top Ten Cybersecurity & Privacy Threats and Trends 2026

1	**Agentic AI Attacks** (AI Arms Race) Agentic SOC—AI bots defend at machine-speed.
2	**Q-Day & PQC Migration** HNDL Threat Mitigation
3	**Live Deepfake Vishing / Death of the Password** FIDO2 + identity provenance , Liveness/PAD (ISO/IEC 30107-1:2023)
4	**‘Death by AI’ Era** Legal liability for AI-driven physical harm.
5	**Privacy Engineering/Shift to First-Party Data.** Consent-fatigue exploitation

Top Ten Cybersecurity & Privacy Threats and Trends 2026

6	**Non-Human IDs (NHI) Sprawl : API keys, bots, service accounts. Ghost identities with high privileges. => API Security Audit**
7	**Cloud & Hybrid IT misconfigurations + expanding attack surface**
8	**Ransomware, extortion, supply-chain, virtualization/infrastructure attacks**
9	**Disinformation/Deepfake as a Service**
10	**Regulatory Compliance overhaul Geopolitical cyber-warfare**

WEF Future of Jobs report 2025

WORLD ECONOMIC FORUM

Join us | Sign in

Publications | Home | Key Findings | Infographics | Explore the Future of Jobs data | Full report | Download PDF

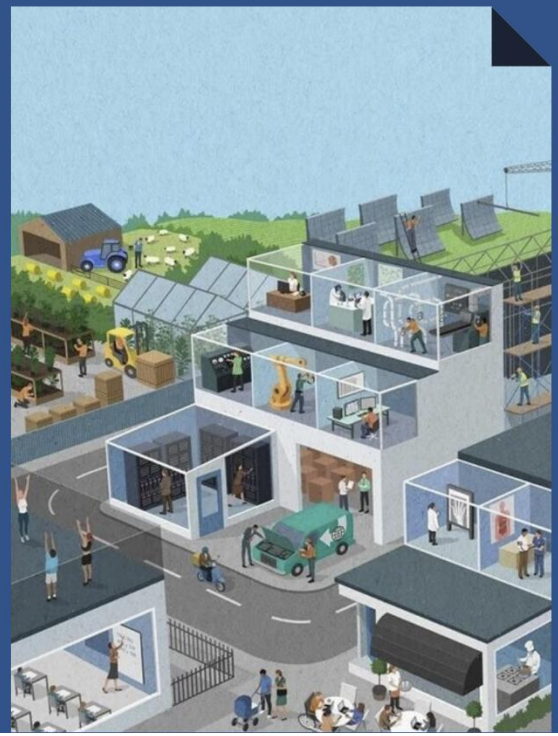
Reports

Published: 7 January 2025

The Future of Jobs Report 2025

Download PDF

Technological change, geoeconomic fragmentation, economic uncertainty, demographic shifts and the green transition – individually and in combination are among the major drivers expected to shape and transform the global labour market by 2030. The *Future of Jobs Report 2025* brings together the perspective of over 1,000 leading global employers—collectively representing more than 14 million workers across 22 industry clusters and 55 economies from around the world—to examine how these macrotrends impact jobs and skills, and the workforce transformation strategies employers plan to embark on in response, across the 2025 to 2030 timeframe.



WEF Future of Jobs report 2025

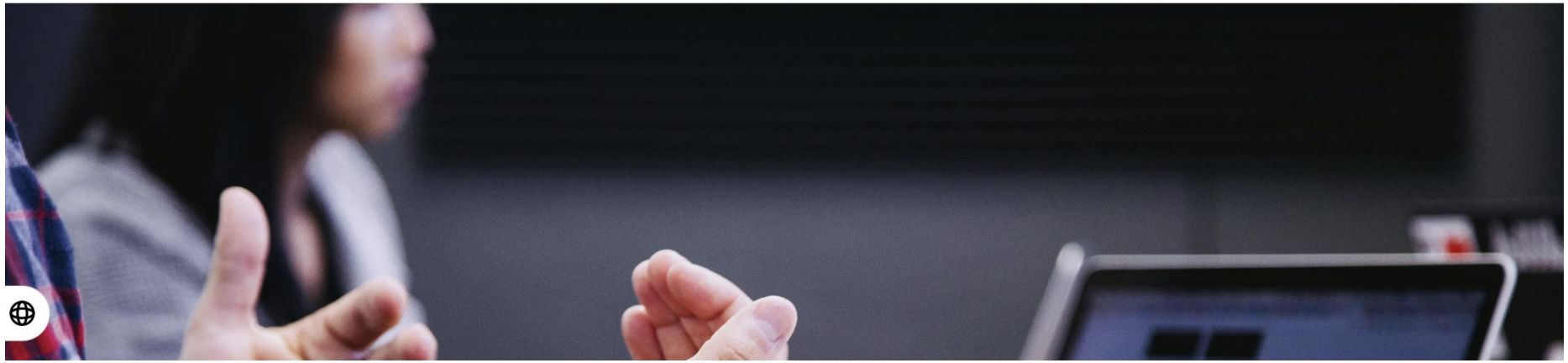
WORLD ECONOMIC FORUM

Join us Sign in

JOBS AND THE FUTURE OF WORK

Future of Jobs Report 2025: These are the fastest growing and declining jobs

Jan 9, 2025



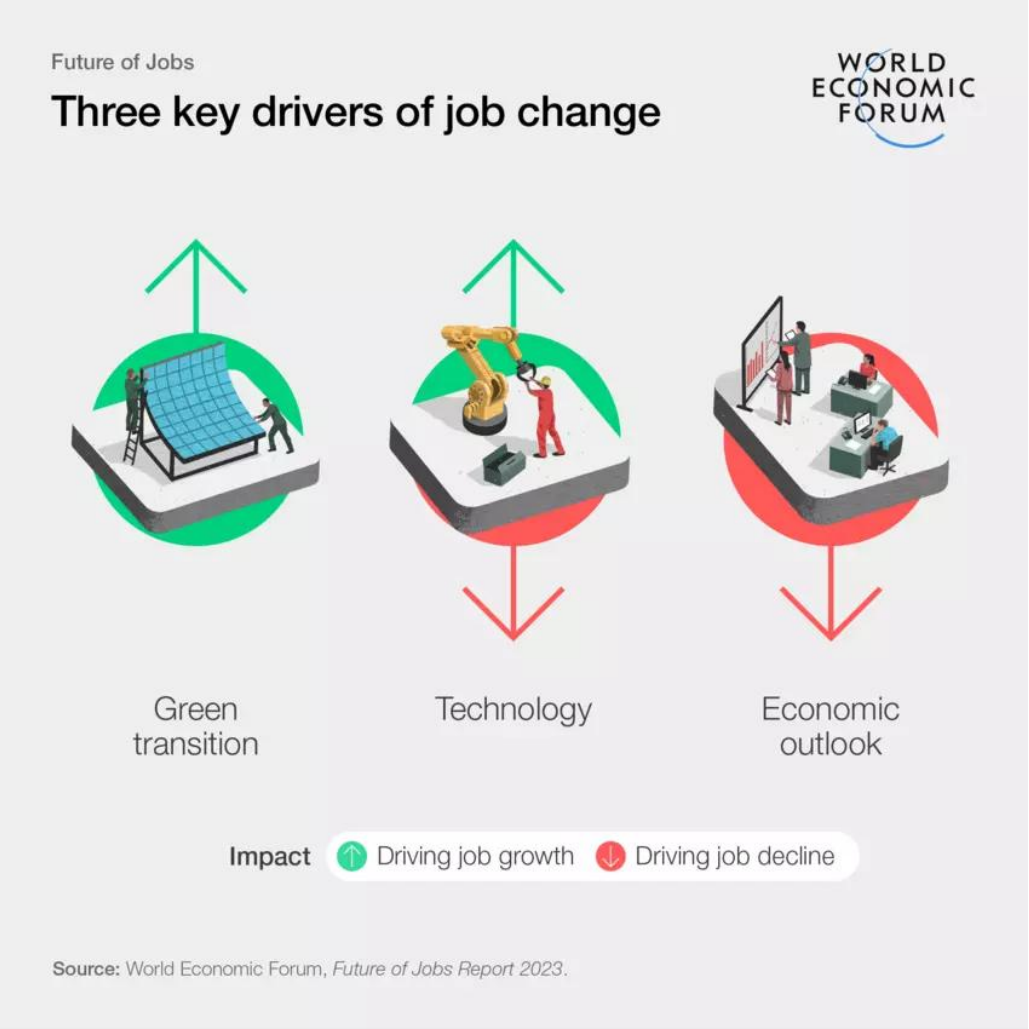
WEF Future of Jobs report 2025

WORLD ECONOMIC FORUM

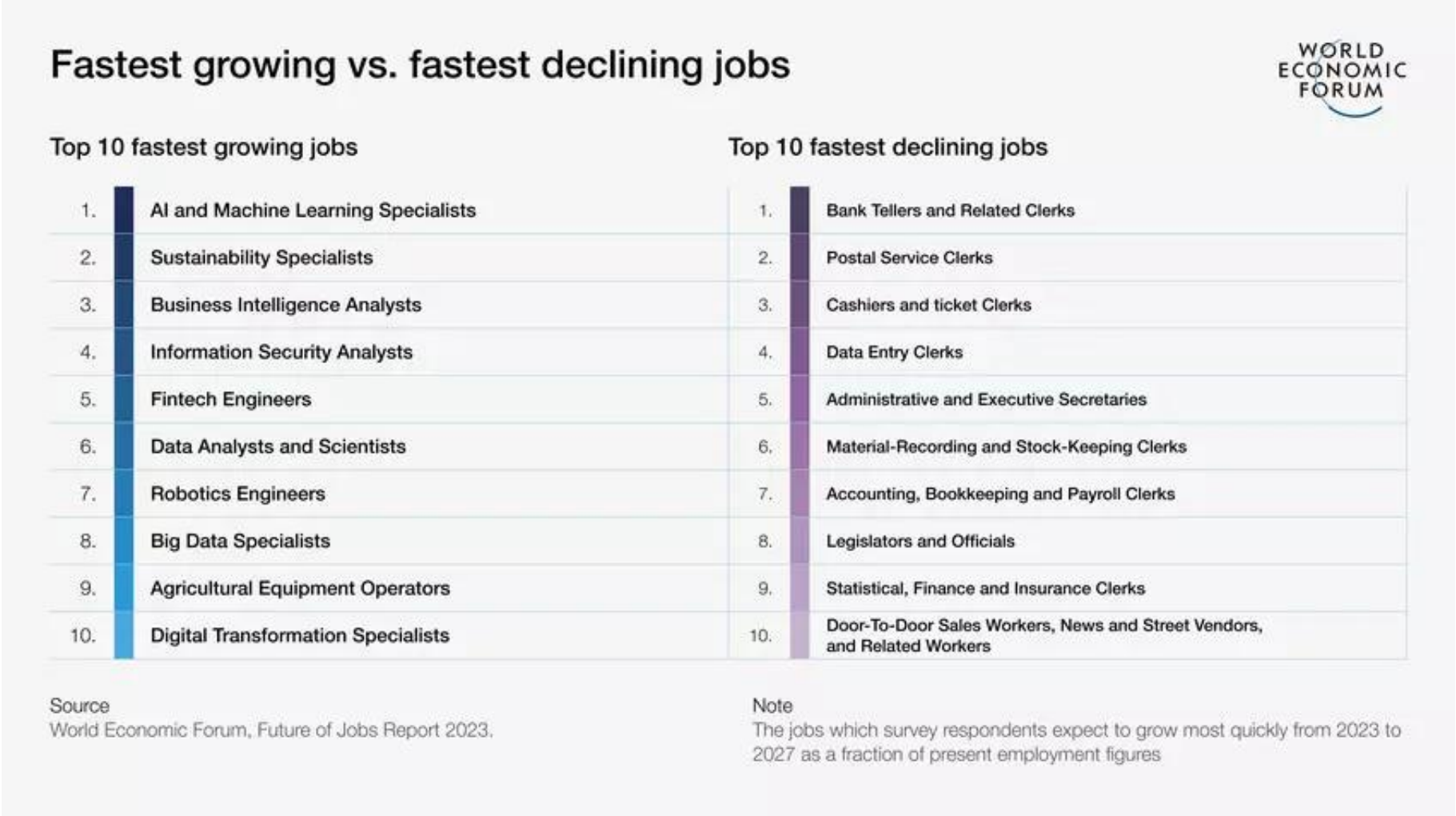
Join us | Sign in

	Top fastest growing jobs		Top fastest declining jobs
1	Big data specialists	1	Postal service clerks
2	FinTech engineers	2	Bank tellers and related clerks
3	AI and machine learning specialists	3	Data entry clerks
4	Software and applications developers	4	Cashiers and ticket clerks
5	Security management specialists	5	Administrative assistants and executive secretaries
6	Data warehousing specialists	6	Printing and related trades workers
7	Autonomous and electric vehicle specialists	7	Accounting, bookkeeping and payroll clerks
8	UI and UX designers	8	Material-recording and stock-keeping clerks
9	Light truck or delivery services drivers	9	Transportation attendants and conductors
10	Internet of things specialists	10	Door-to-door sales workers, news and street vendors, and related workers
11	Data analysts and scientists	11	Graphic designers
12	Environmental engineers	12	Claims adjusters, examiners and investigators
13	Information security analysts	13	Legal officials
14	DevOps engineers	14	Legal secretaries
15	Renewable energy engineers	15	Telemarketers

WEF Future of Jobs report 2025



WEF Future of Jobs report 2025



Fastest growing vs. fastest declining jobs

WORLD ECONOMIC FORUM

Top 10 fastest growing jobs

1.	AI and Machine Learning Specialists
2.	Sustainability Specialists
3.	Business Intelligence Analysts
4.	Information Security Analysts
5.	Fintech Engineers
6.	Data Analysts and Scientists
7.	Robotics Engineers
8.	Big Data Specialists
9.	Agricultural Equipment Operators
10.	Digital Transformation Specialists

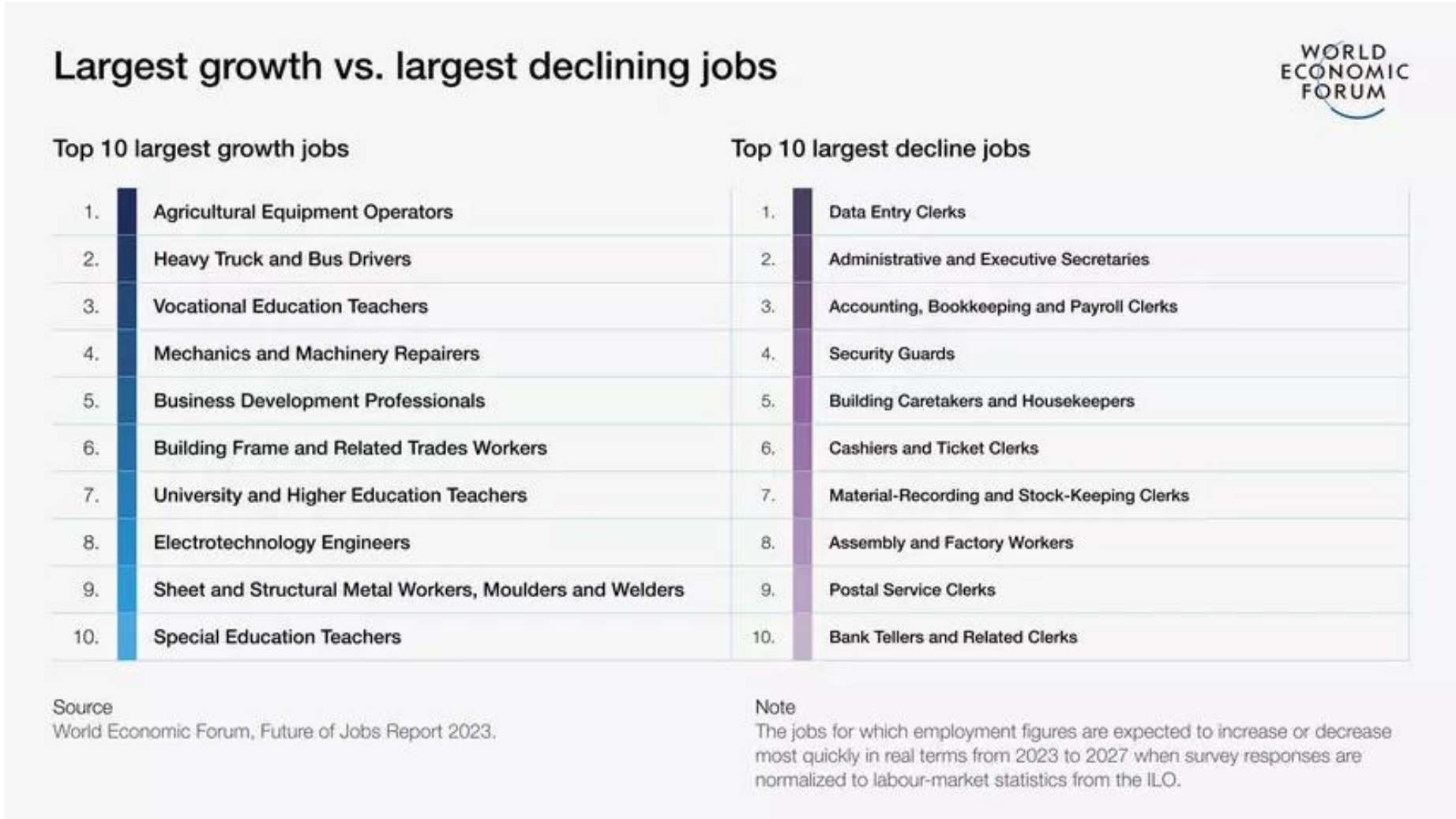
Top 10 fastest declining jobs

1.	Bank Tellers and Related Clerks
2.	Postal Service Clerks
3.	Cashiers and ticket Clerks
4.	Data Entry Clerks
5.	Administrative and Executive Secretaries
6.	Material-Recording and Stock-Keeping Clerks
7.	Accounting, Bookkeeping and Payroll Clerks
8.	Legislators and Officials
9.	Statistical, Finance and Insurance Clerks
10.	Door-To-Door Sales Workers, News and Street Vendors, and Related Workers

Source
World Economic Forum, Future of Jobs Report 2023.

Note
The jobs which survey respondents expect to grow most quickly from 2023 to 2027 as a fraction of present employment figures

WEF Future of Jobs report 2025



Largest growth vs. largest declining jobs

WORLD ECONOMIC FORUM

Top 10 largest growth jobs

1.	Agricultural Equipment Operators
2.	Heavy Truck and Bus Drivers
3.	Vocational Education Teachers
4.	Mechanics and Machinery Repairers
5.	Business Development Professionals
6.	Building Frame and Related Trades Workers
7.	University and Higher Education Teachers
8.	Electrotechnology Engineers
9.	Sheet and Structural Metal Workers, Moulders and Welders
10.	Special Education Teachers

Top 10 largest decline jobs

1.	Data Entry Clerks
2.	Administrative and Executive Secretaries
3.	Accounting, Bookkeeping and Payroll Clerks
4.	Security Guards
5.	Building Caretakers and Housekeepers
6.	Cashiers and Ticket Clerks
7.	Material-Recording and Stock-Keeping Clerks
8.	Assembly and Factory Workers
9.	Postal Service Clerks
10.	Bank Tellers and Related Clerks

Source
World Economic Forum, Future of Jobs Report 2023.

Note
The jobs for which employment figures are expected to increase or decrease most quickly in real terms from 2023 to 2027 when survey responses are normalized to labour-market statistics from the ILO.

WEF Future of Jobs report 2025

CYBERTRON

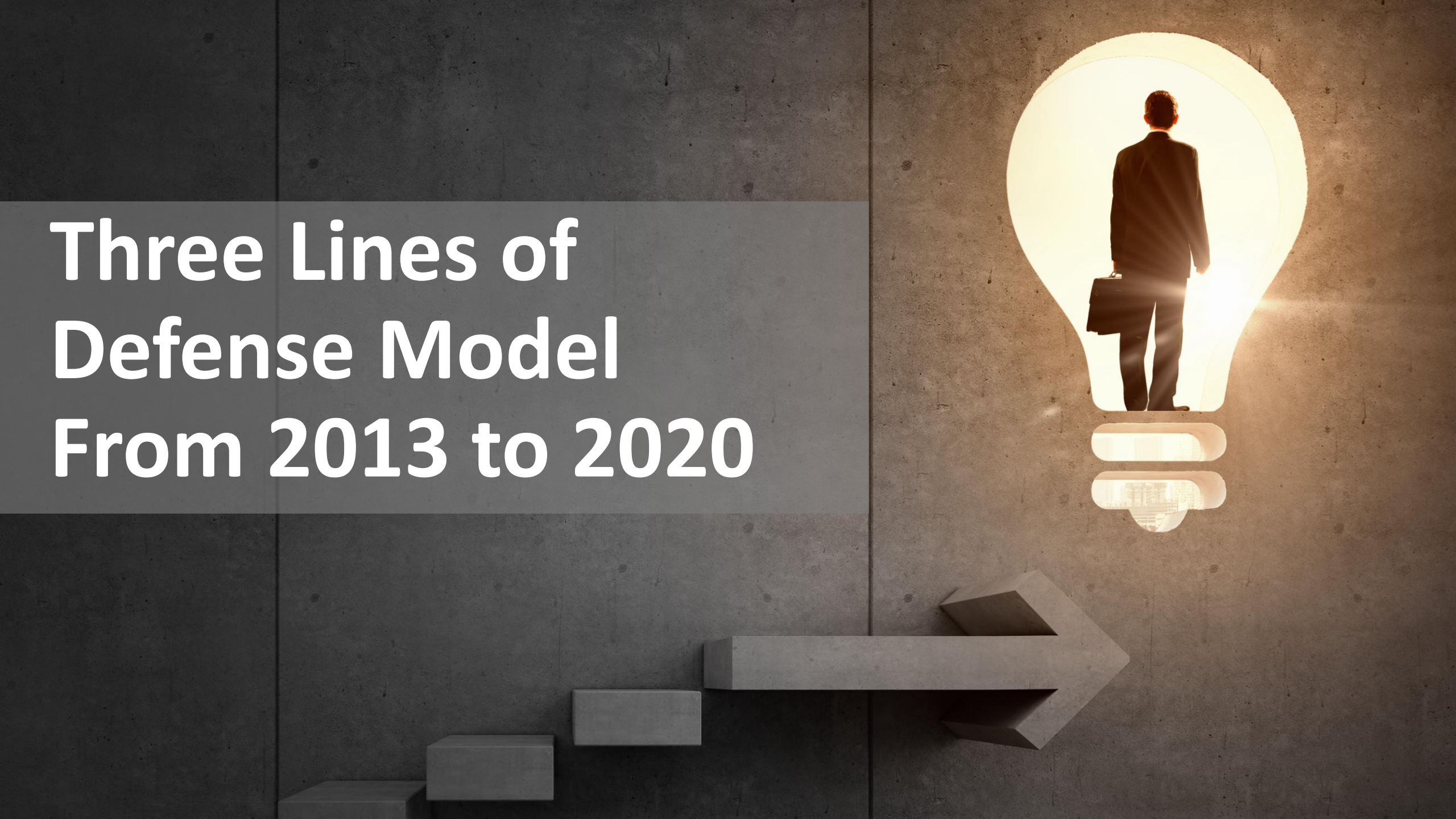
7 Digital RISKs

2024-2025

How Thailand & Singapore fighting SCAM Networks

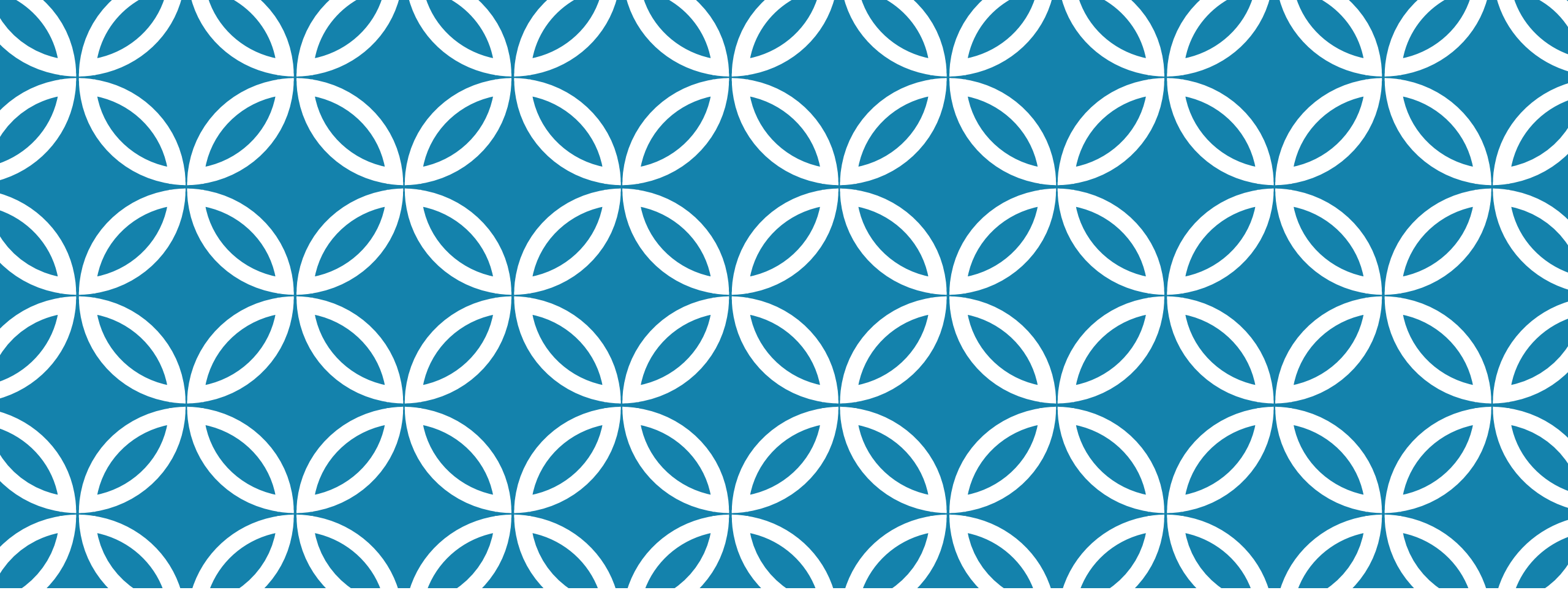
Source: Bloomberg

Three Lines of Defense Model From 2013 to 2020



The Three Lines of Defense Model

A comprehensive framework for effective risk management, governance and internal control in organisations



ORIGIN OF THE THREE LINES MODEL

Who created it and how it evolved

WHO INVENTED THE THREE LINES OF DEFENSE?

- Developed and formalized by the Institute of Internal Auditors (IIA)
- First published in January 2013
- Introduced through the paper:

"The Three Lines of Defense in Effective Risk Management and Control"

- Designed to clarify roles and responsibilities in risk management and internal control

2020 UPDATE: THREE LINES MODEL

- Updated in July 2020 by IIA
- New title: “The Three Lines Model” (dropped 'Defense')
- Key enhancements:
  - Focused on value creation, not just risk protection
  - Promoted collaboration among lines
  - Emphasized flexibility and governance alignment
- Still widely used in governance, risk, and compliance (GRC)

Understanding the Three Lines of Defense

The Three Lines of Defense (3LoD) model is a widely recognised framework for risk management and internal control, commonly employed in governance, compliance, and auditing contexts. Its primary purpose is to clarify roles and responsibilities for managing risks within an organisation.

This model provides a structured approach to risk management, ensuring that risks are properly identified, managed, monitored, and reported through clearly defined responsibilities.

Why Organisations Need the 3LoD Model

- Creates clarity in risk-related responsibilities
- Prevents gaps or duplications in risk coverage
- Improves risk management effectiveness
- Strengthens organisational governance

Benefits of Implementation

- Enhanced risk awareness throughout the organisation
- Improved control environment
- Greater assurance to stakeholders
- Better regulatory compliance

The First Line of Defense: Operational Management

The first line owns and manages risks directly as part of daily operations.

Key Responsibilities

- Identifying, assessing and actively managing operational risks
- Implementing and maintaining effective internal controls
- Executing risk and control procedures on a day-to-day basis
- Addressing control deficiencies and implementing corrective actions
- Reporting risk information up the organisation

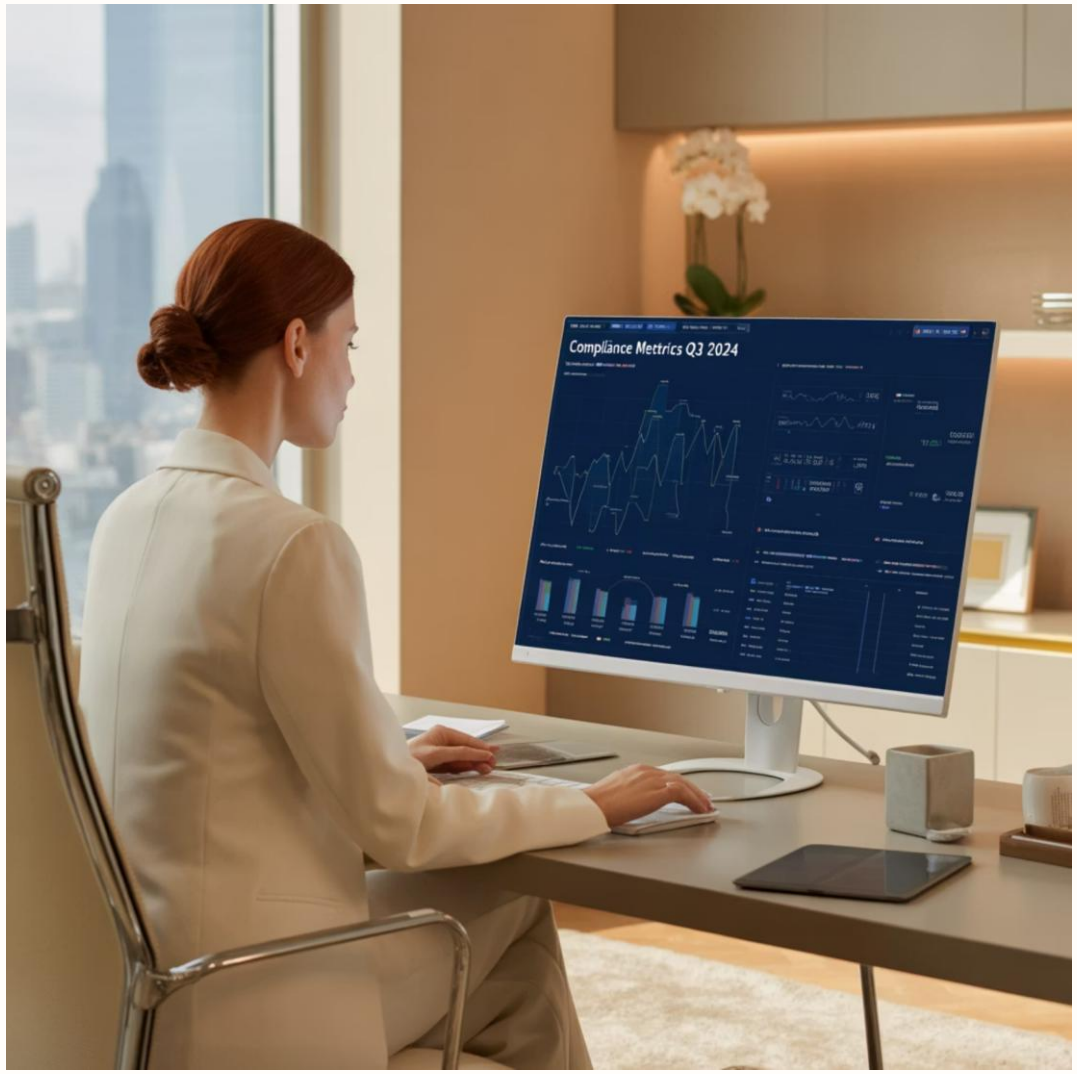
Examples: Department managers, operational staff, business unit leaders

The Second Line of Defense: Risk Management & Compliance

Key Responsibilities

- Developing and implementing risk management frameworks and policies
- Supporting and monitoring first line risk activities
- Providing expertise, tools and training on risk management
- Ensuring compliance with regulations and policies
- Reporting on risk-related matters to senior management

Examples: Risk management teams, compliance functions, legal departments, quality control



The second line oversees risks and provides specialised expertise to support effective risk management practices.

The Third Line of Defense: Internal Audit

Key Responsibilities

- Evaluating the effectiveness of the first and second lines
- Providing independent assurance to the Board and Audit Committee
- Assessing whether key risks are properly controlled
- Identifying improvement opportunities
- Maintaining independence from operational management

Unlike the first two lines, internal audit reports directly to the Board or Audit Committee, ensuring true independence.

The third line provides independent and objective assurance on the effectiveness of

Comparative Analysis of the Three Lines

Characteristic	First Line	Second Line	Third Line
Primary Focus	Risk ownership & execution	Risk oversight & guidance	Independent assurance
Independence Level	Low (embedded in operations)	Medium (separate from operations)	High (reports to Board/Audit Committee)
Authority	Operational decisions	Policy setting & monitoring	Evaluation & recommendations
Main Challenge	Balancing operations with control duties	Maintaining appropriate influence without ownership	Ensuring coverage of key risks without losing independence

Independence and objectivity increase from the first to the third line, whilst direct operational involvement decreases.

Key Characteristics of an Effective 3LoD Model

1

Clear Accountability

Roles and responsibilities are well-defined with no significant gaps or unnecessary overlaps. Each line understands its boundaries and accountabilities.

2

Appropriate Resources

Each line is adequately resourced with professionals possessing the right skills, experience and tools to fulfil their respective responsibilities effectively.

3

Effective Communication

Information flows efficiently both vertically (up to Board level) and horizontally (across the three lines), ensuring that risk insights are shared appropriately.

4

Continuous Improvement

The model adapts to changing business environments, emerging risks, and lessons learned from internal and external events.

Updated Guidance: The IIA's 2020 Revision

In 2020, The Institute of Internal Auditors (IIA) updated the Three Lines of Defense model to reflect contemporary risk management practices. The revised model, now called "The Three Lines Model," introduces several important changes:

From Rigid Structure to Flexible Principles

The update recognises that organisations may adapt the model to their specific needs rather than rigidly implementing a standard structure.

From Defense to Value Creation

Greater emphasis on risk management as an enabler of organisational success, not just a protective measure.

From Separation to Collaboration

Enhanced focus on coordination, cooperation and communication between all three lines, whilst maintaining appropriate independence.

Implementation Challenges and Best Practices

Common Implementation Challenges

- **Unclear delineation of responsibilities between lines**
- **Inadequate resources or expertise within specific lines**
- **Poor communication between the three lines**
- **Resistance to change from established practices**
- **Difficulty adapting the model to complex organisational structures**

Best Practices for Successful Implementation

- **Secure explicit Board and executive sponsorship**
- **Conduct comprehensive stakeholder mapping**
- **Document clear responsibilities in formal charters**
- **Establish regular coordination mechanisms**
- **Provide continuous training and awareness**
- **Review and refine the model periodically**

Successful implementation requires a tailored approach that considers the organisation's size, complexity, industry, and risk maturity level.

Key Takeaways

Comprehensive Risk Coverage

The Three Lines of Defense model provides a comprehensive framework for managing risks across the organisation, ensuring nothing falls through the cracks.

Clear Role Definition

By clearly defining roles and responsibilities, the model eliminates confusion and reduces both gaps and overlaps in risk management activities.

Collaboration Is Essential

While maintaining appropriate independence, effective risk management requires collaboration and communication between all three lines.

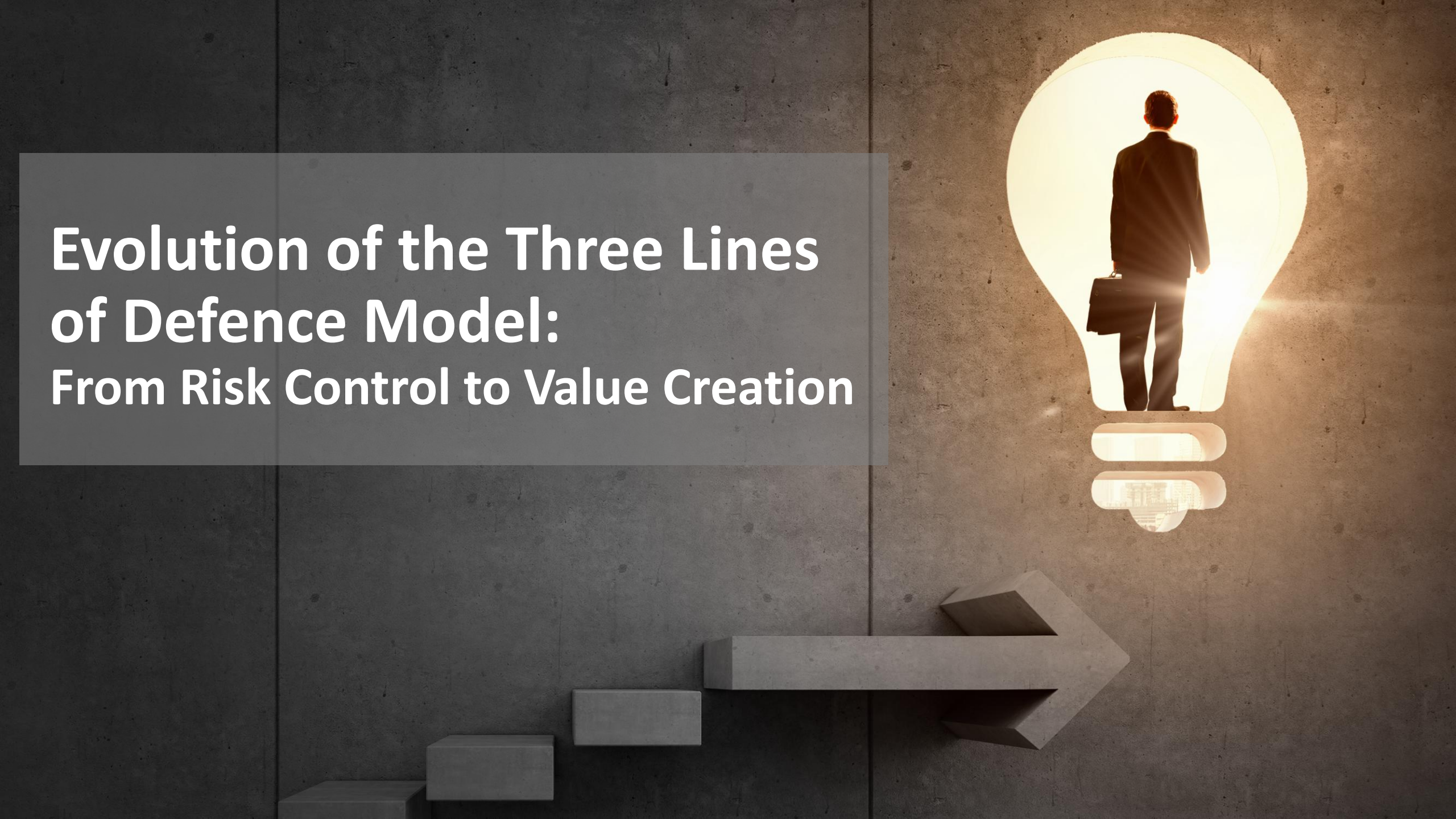
Evolving Framework

The 2020 IIA update reflects the need for the model to evolve, focusing on value creation and adaptable principles rather than rigid structures.

Implementation should be tailored to your organisation's specific context, but the underlying principles remain valuable for all risk management professionals.

Evolution of the Three Lines of Defence Model:

From Risk Control to Value Creation



Evolution of the Three Lines of Defence Model: From Risk Control to Value Creation

An exploration of how the Three Lines of Defence model has transformed from a rigid framework into an integrated approach that supports organisational resilience and value creation.

The Journey of the 3LoD Model

The Three Lines of Defence (3LoD) model has undergone a significant transformation since its inception, evolving from a militaristic, siloed approach to a more collaborative framework focused on value creation and governance.

Early Model (Pre-2020)

Established as a rigid structure with clear separation between lines, primarily focused on risk management and internal control. Limited collaboration between lines was emphasised to maintain independence.

1

Transition Period

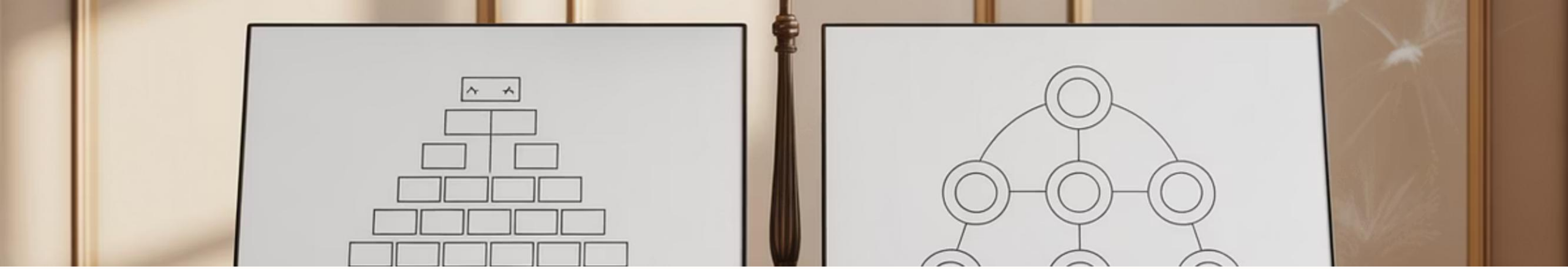
Recognition of limitations in the original model led to discussions about its effectiveness in complex organisations. Calls for greater flexibility and collaboration emerged across the risk management community.

2

Current Model (IIA 2020 Update)

Redesigned with an emphasis on flexibility, integration with governance, and value creation. The updated model promotes collaboration whilst maintaining appropriate independence.

3



Structure and Focus: A Fundamental Shift

Early Model Structure

- Rigid separation between the three lines
- Linear, siloed approach to risk management
- Primary focus on risk control and mitigation
- Often interpreted as a militaristic "defence" system
- Limited emphasis on cross-functional collaboration

Current Model Structure

- Flexible and adaptable to organisational context
- Integrated approach to governance
- Dual focus on risk management and value creation
- Neutral language emphasising "roles" over "defence"
- Explicit encouragement of collaboration between lines

First Line: From Risk Ownership to Objective Achievement

Early Model Approach

Operational management owns and manages risk

- Focus primarily on control activities
- Responsibility for implementing procedures
- Often viewed as separate from strategy

Current Model Approach

Still owns risk, but with greater focus on achieving objectives

- Integration of risk management with strategy
- Emphasis on achieving organisational goals
- Proactive approach to identifying opportunities

The transformation of the first line reflects a broader shift from viewing risk management as a compliance activity to seeing it as integral to business performance and value creation.

Second Line: From Monitoring to Collaboration

Early Model Approach

In the pre-2020 model, the second line functioned primarily as a monitoring mechanism:

- Risk management and compliance functions oversaw the first line
- Emphasis on maintaining separation from operations
- Often perceived as a policing function
- Limited advisory capacity

Current Model Approach

The 2020 update transformed the second line into a more collaborative partner:

- Provides expertise, support, and monitoring
- Encouraged to offer advisory support, not just oversight
- Works alongside first line to enhance capabilities
- Facilitates improvement in risk management processes

Third Line: Enhanced Integration Whilst Maintaining Independence

Early Model Role

Internal audit provided independent assurance with:

- Strong emphasis on separation from other lines
- Limited involvement in strategic discussions
- Focus primarily on compliance and control effectiveness
- Reporting relationships sometimes unclear

Current Model Role

Internal audit maintains independence whilst being better integrated:

- Clear reporting line to governing body
- Broader focus on governance and value creation
- More strategic contribution to organisational objectives
- Improved coordination with other assurance providers

The evolution of the third line demonstrates how independence can be preserved whilst enhancing the strategic value that internal audit provides to the organisation.

Leadership and Governance: A New Emphasis

Early Model Oversight

The role of the board and executive leadership was not explicitly highlighted in the original model, creating ambiguity about ultimate responsibility for risk governance.

Current Model Oversight

The updated model clearly defines the role of governing bodies and senior management in providing oversight, setting objectives and ensuring accountability throughout all lines.

This shift recognises that effective risk management and governance must start at the top, with clear accountability and commitment from organisational leadership.

Key Benefits of the Current Model

Improved Collaboration

Encourages coordinated effort between all roles to manage risks effectively whilst maintaining appropriate independence

Enhanced Accountability

Emphasises responsibility at all levels of the organisation for better risk outcomes

Value Creation Focus

Goes beyond risk mitigation to support performance, resilience, and sustainability

Clearer Governance

Clarifies roles of governing bodies, senior management, and assurance providers for better accountability

Strategic Alignment

Integrates risk and control activities with the organisation's objectives and strategic direction

Flexible Structure

Allows tailoring of roles based on organisation size, industry, and complexity for optimal effectiveness

Practical Implementation Considerations

Organisational Assessment

Before implementing the updated model, organisations should:

- Evaluate current risk management maturity
- Identify existing strengths and weaknesses
- Assess organisational culture and readiness for change
- Review current governance structures

Implementation Strategies

Successful adoption of the current model requires:

- Clear communication about the purpose of changes
- Training on new roles and responsibilities
- Leadership support and visible commitment
- Phased implementation approach
- Regular review and refinement

Key Takeaways: The Evolution Continues

From Rigid to Flexible

The 3LoD model has evolved from a rigid structure to an adaptable framework that can be tailored to organisational context.

From Control to Value

The focus has shifted from purely risk control to balancing risk management with value creation and strategic alignment.

From Separation to Collaboration

Whilst maintaining necessary independence, the updated model emphasises the importance of coordination and collaboration between all roles.

From Implicit to Explicit Leadership

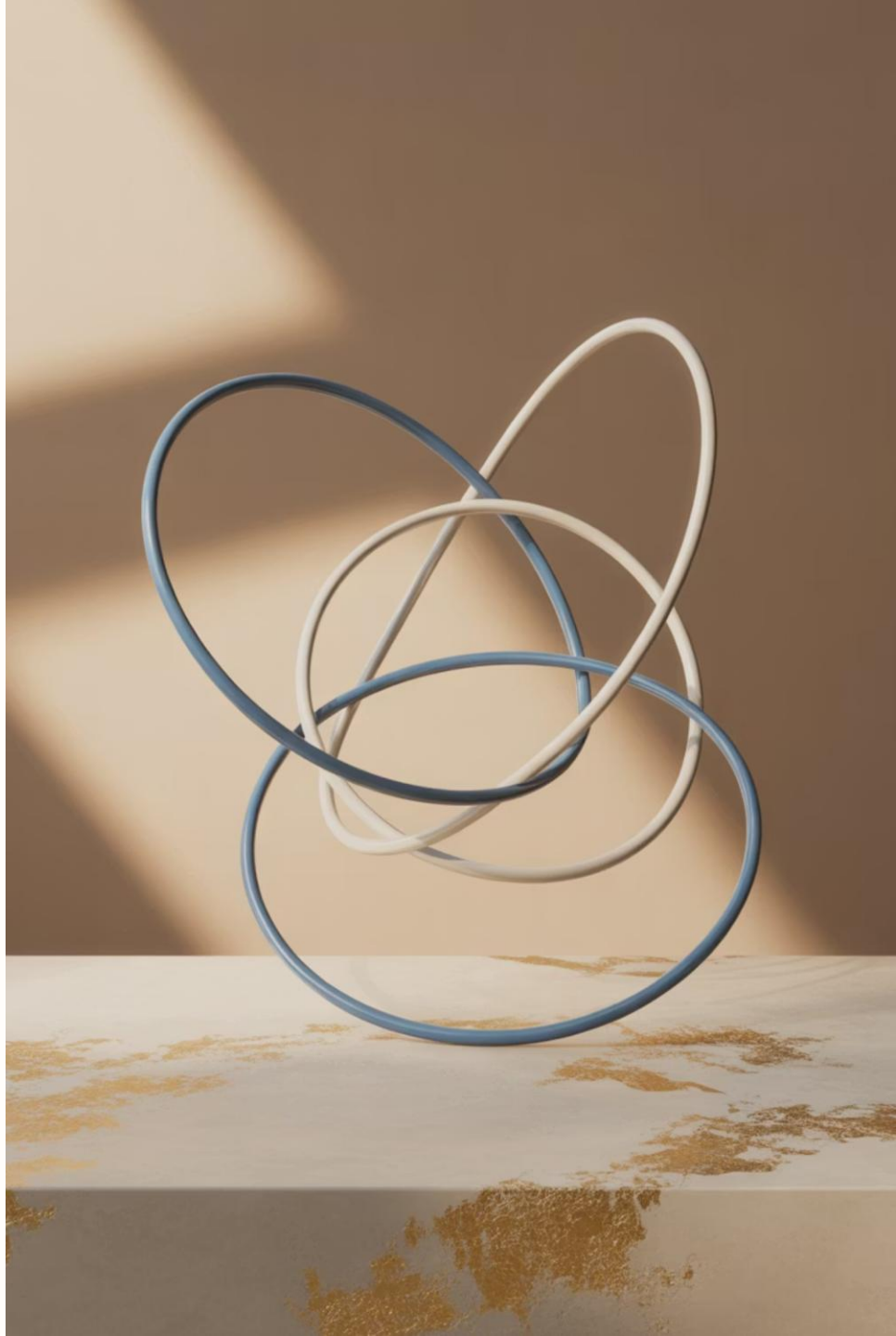
The role of governing bodies and senior management is now clearly articulated, highlighting the importance of tone from the top.

The evolution of the Three Lines of Defence model represents a significant advancement in risk management thinking. Organisations that embrace this updated approach can build more resilient governance structures that not only protect value but actively contribute to its creation.

Three Lines Model: Global & Thai Best Practices in Risk Governance

Three Lines Model: Global & Thai Best Practices in Risk Governance

A comprehensive analysis of how leading organisations have successfully implemented the Three Lines Model to enhance risk management, governance and control. This presentation explores international and Thai case studies, examining their practical approaches and measurable outcomes.



The Three Lines Model: Foundation for Effective Risk Governance

The Three Lines Model provides a structured approach to risk management and governance through clearly defined roles and responsibilities:

- **1st Line:** Business operations that own and manage risks
- **2nd Line:** Functions that oversee risk, provide expertise and challenge
- **3rd Line:** Internal audit providing independent assurance

This presentation examines how organisations have operationalised this model to achieve tangible benefits in risk management and operational resilience.

Global Best Practice: Nestlé

Implementation Approach

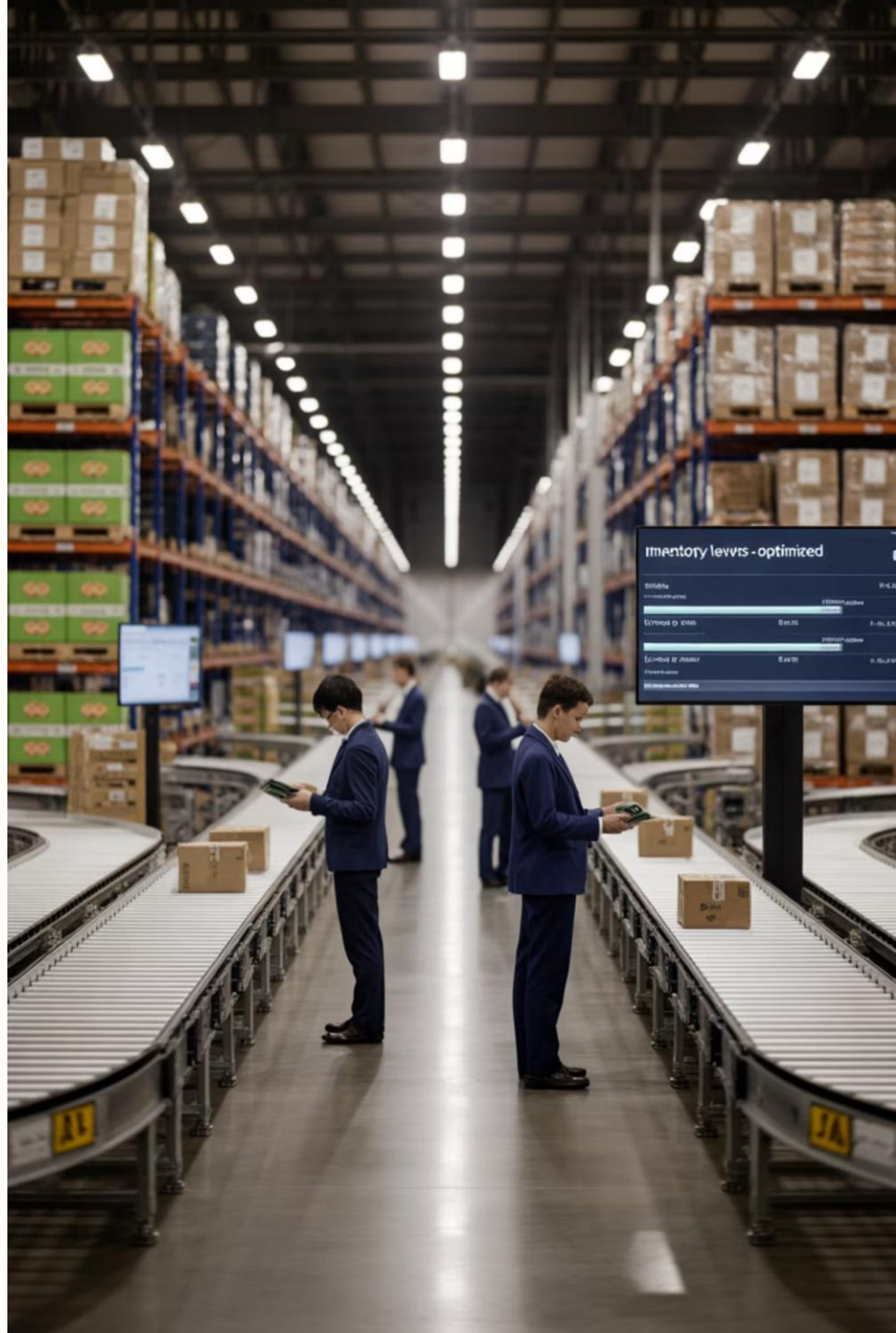
Nestlé deployed a comprehensive Three Lines strategy with clearly defined responsibilities across its global business units, embedding risk ownership at every operational level.

Key Practices

- 1st Line: Embedded risk owners at factory and business unit level with clear accountability
- 2nd Line: Centralised risk team providing assessment tools and compliance oversight
- 3rd Line: Internal Audit conducting thematic, risk-based audits across the organisation

Measurable Results

- Demonstrated supply chain resilience during COVID-19 disruptions
- Enhanced capability to identify emerging risks in sustainability and packaging
- Improved cross-functional collaboration on risk mitigation strategies



Global Best Practice: HSBC

HSBC's global risk governance framework exemplifies how financial institutions can

1st Line Implementation

Deployed dedicated business risk officers and financial crime teams with direct accountability for risk controls

2nd Line Approach

Risk management functions oversee risk appetite alignment and provide regulatory expertise and updates

3rd Line Innovation

Internal Audit provides real-time assurance on risk mitigation effectiveness through continuous auditing techniques

Results: Enhanced risk ownership across departments with significant reduction in regulatory fines and compliance breaches

Global Best Practice: United Nations Development Programme

1st Line: Project Delivery

Programme managers maintain detailed risk registers and implement controls within project delivery. Each project manager serves as a risk owner with clear accountability for risk identification and mitigation.

2nd Line: Oversight Functions

Risk management and ethics teams provide expert guidance, monitor compliance with UN standards and offer specialist support to high-risk initiatives. This includes deployment of risk assessment frameworks tailored to development contexts.

3rd Line: Independent Assurance

Independent evaluations and audits assess project governance effectiveness and control adequacy. Findings feed directly into organisational learning and future programme design.

Key Outcome: UNDP has achieved improved accountability and transparency in international aid whilst more effectively aligning operations with Sustainable Development Goal targets.

Thai Best Practice: PTT Group

PTT Group, Thailand's leading energy and petrochemical conglomerate, has implemented a group-wide risk governance framework using the Three Lines Model.

Implementation Highlights:

- Comprehensive risk ownership at business unit level (1st Line)
- Enterprise Risk Management and Legal teams operating as robust 2nd Line
- Internal Audit functions at both group and subsidiary levels (3rd Line)

This integrated approach has strengthened PTT's ESG compliance and contributed to the group consistently achieving listing on the Dow Jones Sustainability Indices (DJSI).

"Our implementation of the Three Lines Model has transformed how we approach governance and

Thai Best Practice: Siam Cement Group (SCG)

First Line Innovation

SCG has uniquely embedded risk ownership within innovation processes. Operational teams are trained to identify and mitigate both operational and innovation-related risks, creating a dual focus on control and advancement.

Digital Risk Management

The 2nd Line provides support through digital risk platforms that enable real-time monitoring and rapid response. These platforms connect operational data with risk indicators, allowing for more sophisticated risk oversight.

Targeted Assurance

SCG's 3rd Line focuses strategically on cyber, fraud, and project assurance, using data analytics to target high-risk areas and provide value-adding insights rather than compliance-focused audits.

This approach has delivered measurable results for SCG, including reduced fraud losses and an increased success rate for innovation projects. The integration of risk thinking into operational processes has enhanced both control and business performance.

Thai Best Practice: Bank of Thailand

The Bank of Thailand has adapted the Three Lines Model for monetary policy and financial oversight, creating a robust framework for national financial stability.

Regulatory First Line

Policy and supervision departments function as the 1st Line, with direct responsibility for controlling risks within their regulatory functions. This includes embedding risk considerations within monetary policy decisions and banking supervision activities.

Centralised Risk Oversight

A dedicated risk office and legal compliance teams serve as the 2nd Line, maintaining independence whilst providing expert guidance on emerging financial system risks and regulatory requirements.

Tech-Enabled Auditing

The 3rd Line uses technology-enabled auditing approaches to provide independent assurance on the effectiveness of the Bank's risk management and control processes, helping identify systemic financial risks early.

This implementation has resulted in a more resilient regulatory system and timely identification of systemic financial risks in the Thai economy.

Key Success Factors Across Organisations

1

Clear Role Definition

Organisations with precisely defined responsibilities across all three lines reported improved accountability and risk ownership at all levels.

2

Strong 2nd Line Support

Effective implementation featured robust 2nd Line functions that enabled rather than obstructed, fostering a proactive risk culture.

3

Integrated Audit Approach

The most successful organisations positioned 3rd Line audit as a value-adding function providing early warning of issues rather than a "gotcha" audit approach.

4

Technology Utilisation

Leading implementers leveraged technology for real-time risk monitoring and data-driven decisions across all three lines.

5

Leadership Commitment

Executive sponsorship ensured alignment between risk governance and strategic objectives, embedding risk thinking in performance metrics.

Implementation Roadmap & Recommendations

Assess Current State

Conduct an honest evaluation of existing risk governance structures and identify gaps against the Three Lines Model

Design Future State

Define clear roles and responsibilities for each line with appropriate authority and resources

Implement & Embed

Roll out new structures with training, communication and performance measures that reinforce risk ownership

Final Recommendations

- Begin with clarifying roles and responsibilities across all three lines
- Secure visible leadership commitment and role modelling
- Invest in risk management capabilities at the 1st Line
- Position 2nd Line as business partners rather than police
- Ensure 3rd Line provides value-adding insights
- Measure and report on the effectiveness of your Three Lines implementation

Overview of Risk Management Approaches

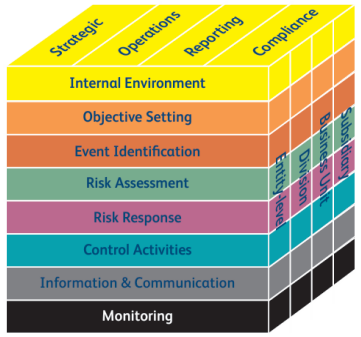
Risk Management provides a **structured** approach for organizations to **identify, assess, and manage risks** that could impact business objectives. Frameworks like **COSO ERM** and **ISO 31000** define risk as "the effect of uncertainty on objectives" and lay out principles for integrating risk practices across an organization.

COSO ERM frameworks

The COSO ERM framework is one of the most widely used risk management approaches globally (including in Thai corporate governance).

COSO's 2017 update, Enterprise Risk Management – Integrating with Strategy and Performance, defines ERM as the "culture, capabilities, and practices [integrated] with strategy-setting and [applied] when carrying out that strategy, with a purpose of managing risk in creating, preserving, and realizing value"

2004



2017

A key evolution in 2017 was distinguishing ERM from mere internal control and highlighting concepts like **risk appetite** and the **integration of risk considerations into performance management**. The framework introduced **five interrelated components of ERM**, each supported by principles

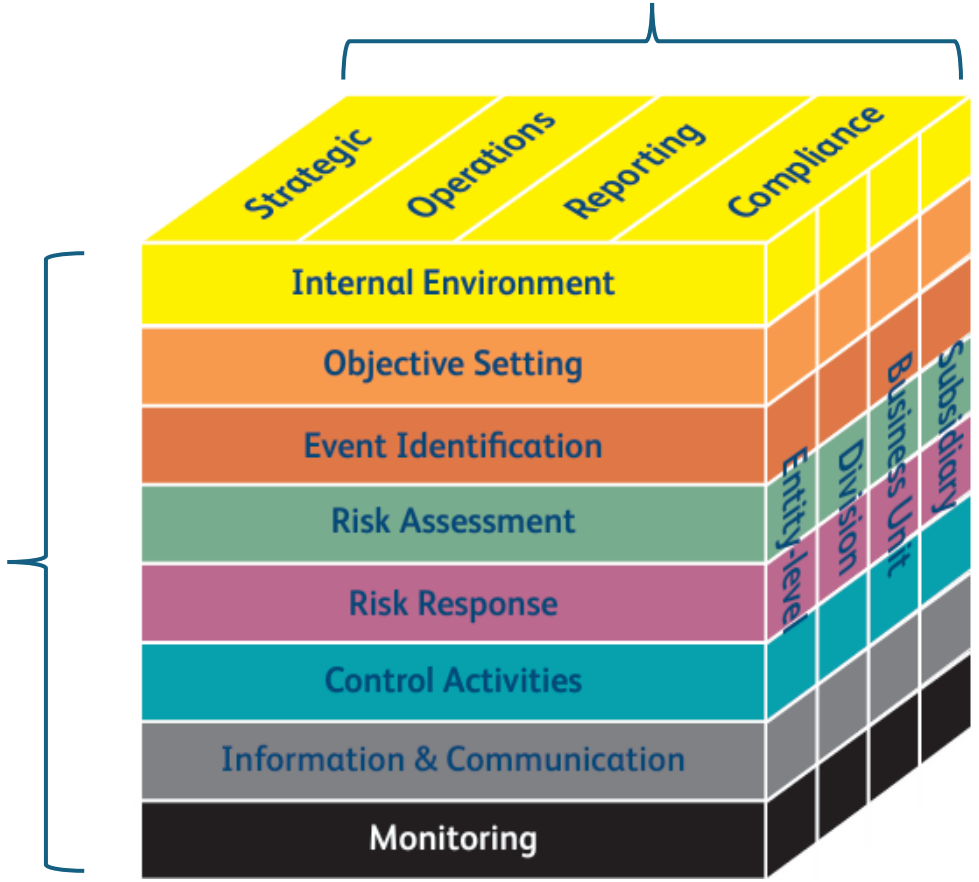
*ERM should be embedded in **day-to-day business activities**, from strategy formulation to execution*

Overview of Risk Management Approaches (Cont.)

COSO ERM (2004)

COSO ERM Cube (2004 version) illustrates the earlier framework's 3-dimensional view

4 categories of objectives (top)



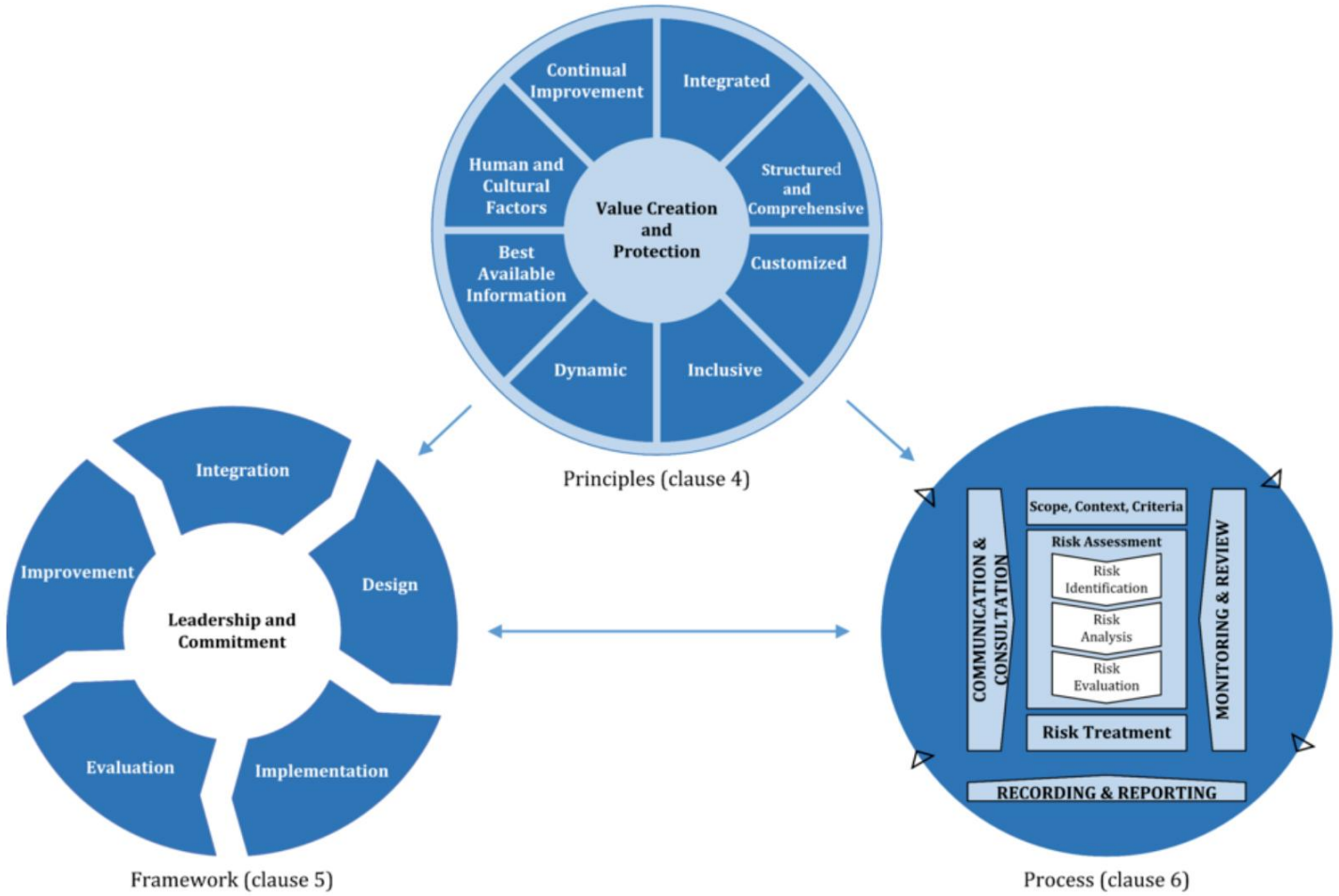
8 components (front face)

4- level of organization (side)

Overview of Risk Management Approaches (Cont.)

ISO 31000:2018 Risk Management

ISO 31000 is the international standard for risk management. It provides **principles**, **framework**, and **process guidelines** for managing risk in any organization, regardless of size, activity, or sector.



Overview of Risk Management Approaches (Cont.)

ISO 31000 vs COSO 2004 vs COSO 2017

Key Differences:

- **ISO 31000** is a high-level guide focused purely on managing risk, intended to be adaptable across sectors and organizational types. It emphasizes principles and a process-based approach without prescriptive structure.

- **COSO ERM 2004** (ERM – Integrated Framework) focuses on internal control and categorizing risk across the enterprise. It uses an 8-component model ("the cube") and emphasizes risk response and control activities, aligning more with a compliance/control environment.

- **COSO ERM 2017** (ERM – Integrating with Strategy and Performance) updates the framework to integrate risk with strategic planning and performance. It introduces 5 components supported by 20 principles, with stronger emphasis on governance, culture, and enterprise value.

Clause	Annex SL heading	COSO ERM cube (2004)	COSO framework 2017
4.	**Context of the organization**		
4.1	Understanding the organisation and its context	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 3: Event Identification includes internal and external events that could have positive or negative impact on objectives	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 2: Strategy & Objective-Setting includes context, risk appetite and setting of strategy and business objectives
4.2	Understanding the needs and expectations of stakeholders		
4.3	Determining the scope of the management system		
4.4	The management system		
5.	**Leadership**		
5.1	Leadership and commitment	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 2: Objective Setting includes mission and setting objectives consistent with risk appetite	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities
5.2	Policy		
5.3	Organisational roles, responsibilities and authorities		
6.	**Planning**		
6.1	Actions to address risks and opportunities	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 2: Objective Setting includes mission and setting objectives consistent with risk appetite	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 2: Strategy & Objective-Setting includes context, risk appetite and setting of strategy and business objectives
6.2	Management system objectives and planning to achieve them		

Overview of Risk Management Approaches (Cont.)

ISO 31000 vs COSO 2004 vs COSO 2017

Clause	Annex SL heading	COSO ERM cube (2004)	COSO framework 2017
6.	**Planning**		
6.1	Actions to address risks and opportunities	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 2: Objective Setting includes mission and setting objectives consistent with risk appetite	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 2: Strategy & Objective-Setting includes context, risk appetite and setting of strategy and business objectives
6.2	Management system objectives and planning to achieve them		
7.	**Support**		
7.1	Resources	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 7: Information & Communication includes need for relevant quality information to be captured and communicated	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 5: Information, Communication & Reporting includes communication, use and reporting of risk information
7.2	Competence		
7.3	Awareness		
7.4	Communication		
7.5	Documented information		
8.	**Operation**		
8.1	Operational planning and control	Component 4: Risk Assessment includes determination of impact, likelihood and inter-relationships of risks Component 5: Risk Response includes actions to align portfolio of risks with risk tolerance and risk appetite	Component 3: Performance includes risk identification and assessment, risk response and inter-relationship of risks
9.	**Performance evaluation**		
9.1	Monitoring, measurement, analysis and evaluation	Component 6: Control Activities includes actions to ensure risk responses are effective and efficient Component 8: Monitoring includes need to monitor and modify the management system and review performance	Component 4: Review & Revision includes assessment of change, monitoring of risk performance and continual improvement
9.2	Internal audit		
9.3	Management review		
10.	**Improvement**		
10.1	Non-conformity and corrective action	Component 8: Monitoring includes need to monitor and modify the management system and review performance	Component 4: Review & Revision includes assessment of change, monitoring of risk performance and continual improvement
10.2	Continual improvement		

Overview of Risk Management Approaches (Cont.)

Common Risk Management Process

1. Risk Identification
- Identify external factors that might affect the organization
- Gather perspectives from across the organization
- Use threat assessment templates

2. Risk Analysis
- Evaluate likelihood of occurrence
- Assess potential negative impact
- Prioritize high-probability, high-impact risks first

3. Risk Mitigation Planning

Choose response strategy
- Avoid: Bypass the risk entirely
- Transfer: Share risk through insurance
- Mitigate: Reduce likelihood/impact
- Accept: Live with low-probability, low-impact risks

4. Implementation
- Exercise risks through scenarios
- Challenge, isolate, or buffer risks as appropriate
- Create contingency plans for when initial strategies fail

5. Review and Tracking
- Monitor ongoing situations
- Document everything and develop KPIs
- Communicate with stakeholders
- Maintain risk registers
- Conduct periodic assessments and after-action reviews
- Keep plans current as a "living document"

Cybersecurity Risk and ERM Alignment

Modern Risk Management Approaches : Cybersecurity Risk and ERM Alignment

What is Cybersecurity risk?

Cybersecurity or cyber risk refers to the potential for loss, damage, or disruption caused by threats to digital systems, networks, or data.

It encompasses risks like data breaches, cyberattacks (e.g., malware, phishing, ransomware), system failures, or unauthorized access, **which can lead to other risks (financial, operational, strategic or Compliance.**

Example of Cyber Risks

- Phishing and ransomware
- Supply chain attacks
- Deepfake fraud
- Cloud misconfigurations
- Insider threats
- AI-driven attacks

Comparison of IT Risk, Cyber Risk, and Digital Risk

Cyber risk is often mistakenly confined to IT. Unlike general **IT risks** (e.g., system outages), **cyber risk** stems from malicious attacks, leading to data theft, financial losses, and operational disruption. It demands specialized security expertise, legal compliance, and impacts the entire organization, far beyond just technical fixes. Moreover, **digital risk** is a broader strategic concern, encompassing business survival in a digital landscape, including customer experience failures and competitive disruption.

Modern Risk Management Approaches : Cybersecurity Risk and ERM Alignment

Organizations' increasing reliance on technology over 50 years has created specialized ICT risk programs (e.g., cybersecurity, supply chain, privacy), but their rapid evolution causes miscommunication and inefficiencies with ERM.

Enhance coordination to align ICT programs with ERM, supporting organizational goals by consolidating risks into registers, quantifying impacts (financial, mission, reputational), and prioritizing resources.

- Cybersecurity (or "cyber risk") has emerged as a top risk area that demands alignment with traditional ERM.

Cybersecurity risk management operates in a technical silo, handled by IT security teams with their own frameworks (e.g., ISO 27001) focusing on system-level issues (e.g., firewalls).

ERM program operates at a higher organizational level, focusing on strategic and enterprise risks reviewed by executives and the board.

Aligning cybersecurity risk with ERM means treating cyber risks as an integral part of the enterprise risk portfolio, using the same lens of impact on business objectives and appetite.

Modern Risk Management Approaches : Cybersecurity Risk and ERM Alignment

Why Aligning Cybersecurity with ERM

Cyber risks are business risks

Cyber incidents can lead to financial loss, reputational damage, operational disruption, and regulatory penalties.

Strategic Alignment

ERM ensures that cybersecurity priorities are tied to the organization's strategic objectives and risk appetite.

Integrated Risk View

ERM provides a holistic view of all risks—financial, operational, reputational, and cybersecurity—allowing for better decision-making and resource allocation.

Enhanced Risk Reporting

Boards and executives need cyber risk data in business terms (impact, probability, ROI on controls).

From IT Risk to Cyber Risk, From Cyber Risk to Digital Risk

Comparison of IT Risk, Cyber Risk, and Digital Risk

	IT Risk	Cyber Risk	Digital Risk
Definition	The risk associated with the failure of IT systems, infrastructure, and processes.	The risk of financial loss, disruption, or reputational damage due to cyberattacks or data breaches.	The risk associated with digital transformation, technology adoption, and digital assets.
Scope	Primarily focused on IT systems, hardware, software, and processes.	Specific to cybersecurity threats, including hacking, malware, phishing, and data breaches.	Broader focus, including IT and cyber risks, as well as risks from digital business models, customer interactions, and digital ecosystems.
Key Risks	System failures, data loss, IT process issues, hardware and software obsolescence.	Unauthorized access, data theft, malware, ransomware, phishing attacks.	Technology adoption risks, third-party digital risks, compliance with digital regulations, brand reputation, and digital market changes.
Impact Areas	IT operations, data integrity, system availability.	Data security, business continuity, financial loss, regulatory fines.	Strategic business outcomes, digital customer experiences, operational and reputational impacts.

From IT Risk to Cyber Risk, From Cyber Risk to Digital Risk

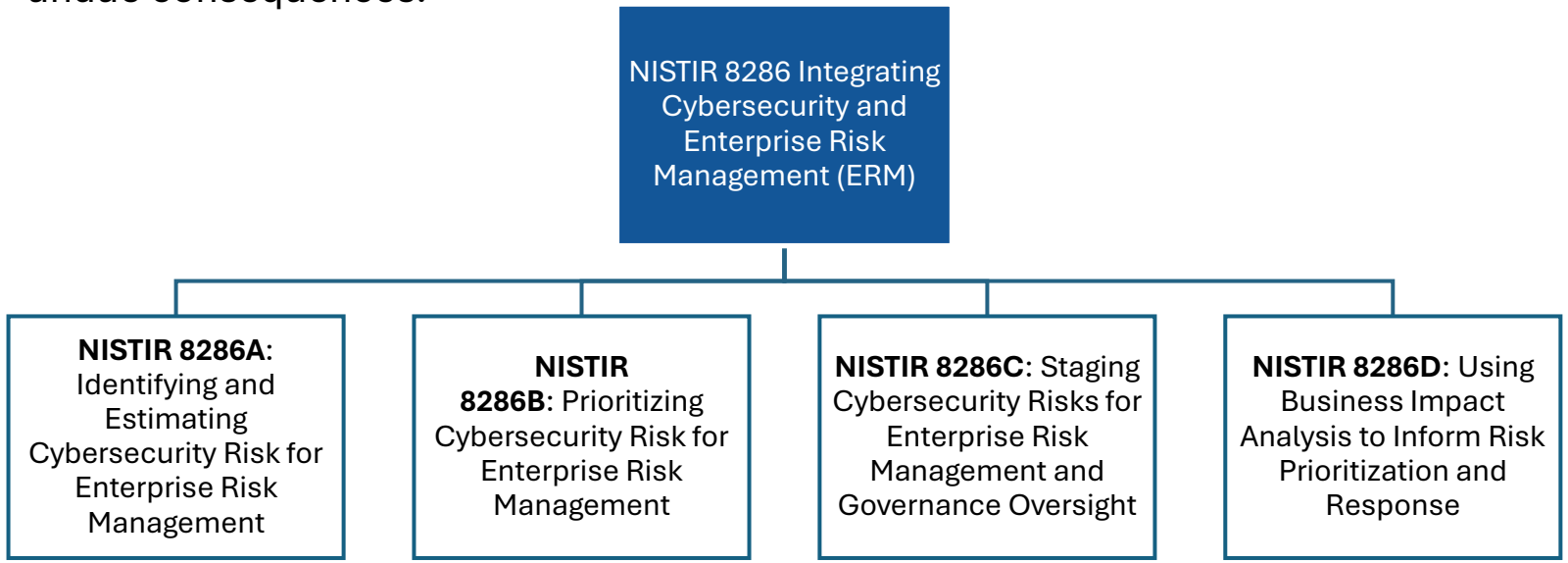
Comparison of IT Risk, Cyber Risk, and Digital Risk

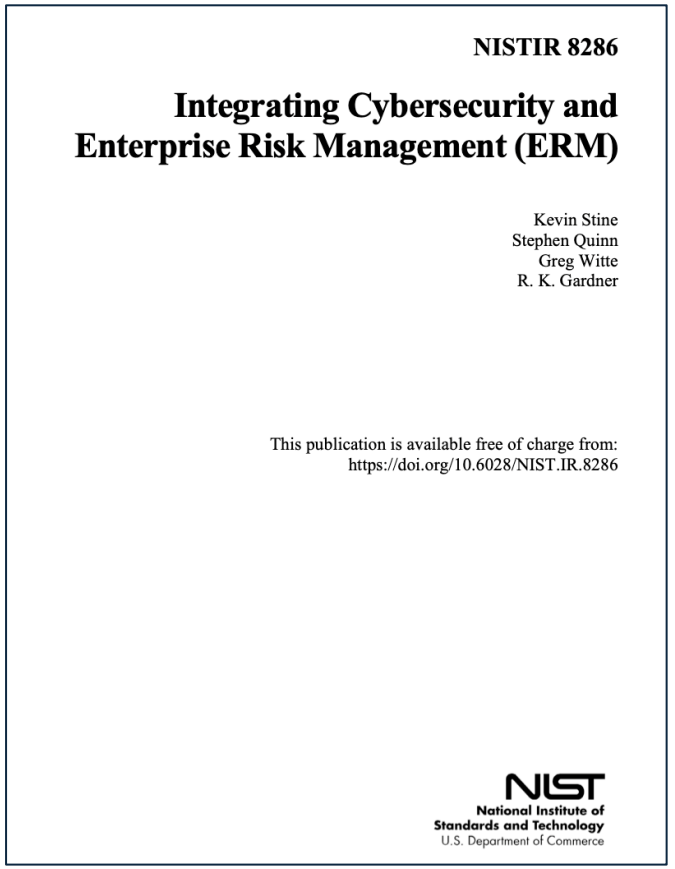
	IT Risk	Cyber Risk	Digital Risk
Management Approach	IT governance, system controls, regular maintenance, disaster recovery planning.	Cybersecurity frameworks, threat monitoring, incident response, vulnerability management.	Integrated digital risk management (IDRM), digital strategy alignment, cross-functional risk assessment.
Stakeholders	IT department, system administrators, technology teams.	Cybersecurity teams, risk management, compliance officers.	C-suite, business leaders, digital transformation teams, and IT and cybersecurity departments.
Regulatory Concern	Compliance with IT standards (e.g., ITIL, COBIT).	Compliance with cybersecurity regulations (e.g., NIST, ISO 27001, GDPR).	Compliance with broader digital regulations, including data privacy, e-commerce laws, and emerging tech regulations.
Example	Server crashes, network outages, software bugs.	Ransomware attack, data breach, phishing scams.	Missteps in digital transformation, poor digital customer experience, disruption in digital services.

Cybersecurity Risk and ERM Alignment (Cont.)

NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)

The gap between Cybersecurity Risk Management (CSRM) output and Enterprise Risk Management (ERM) input, as outlined in NISTIR 8286, stems from the challenge of aligning cybersecurity risk information with enterprise-wide risk management objectives. Effective CSRM balances the benefits of technology with potential risks to avoid innovation or exposing the enterprise to undue consequences.




NISTIR 8286

Integrating Cybersecurity and Enterprise Risk Management (ERM)

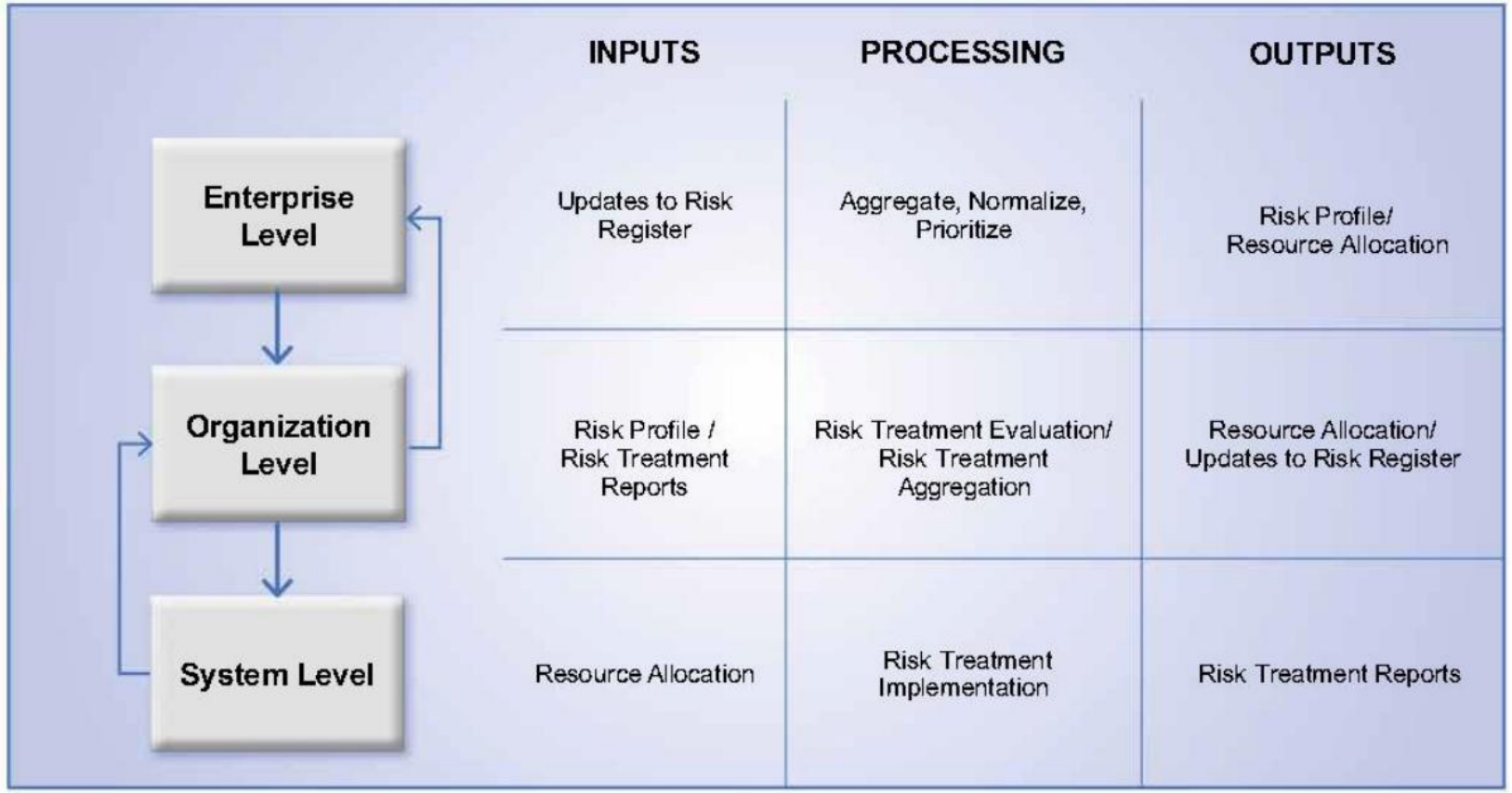
Kevin Stine
Stephen Quinn
Greg Witte
R. K. Gardner

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

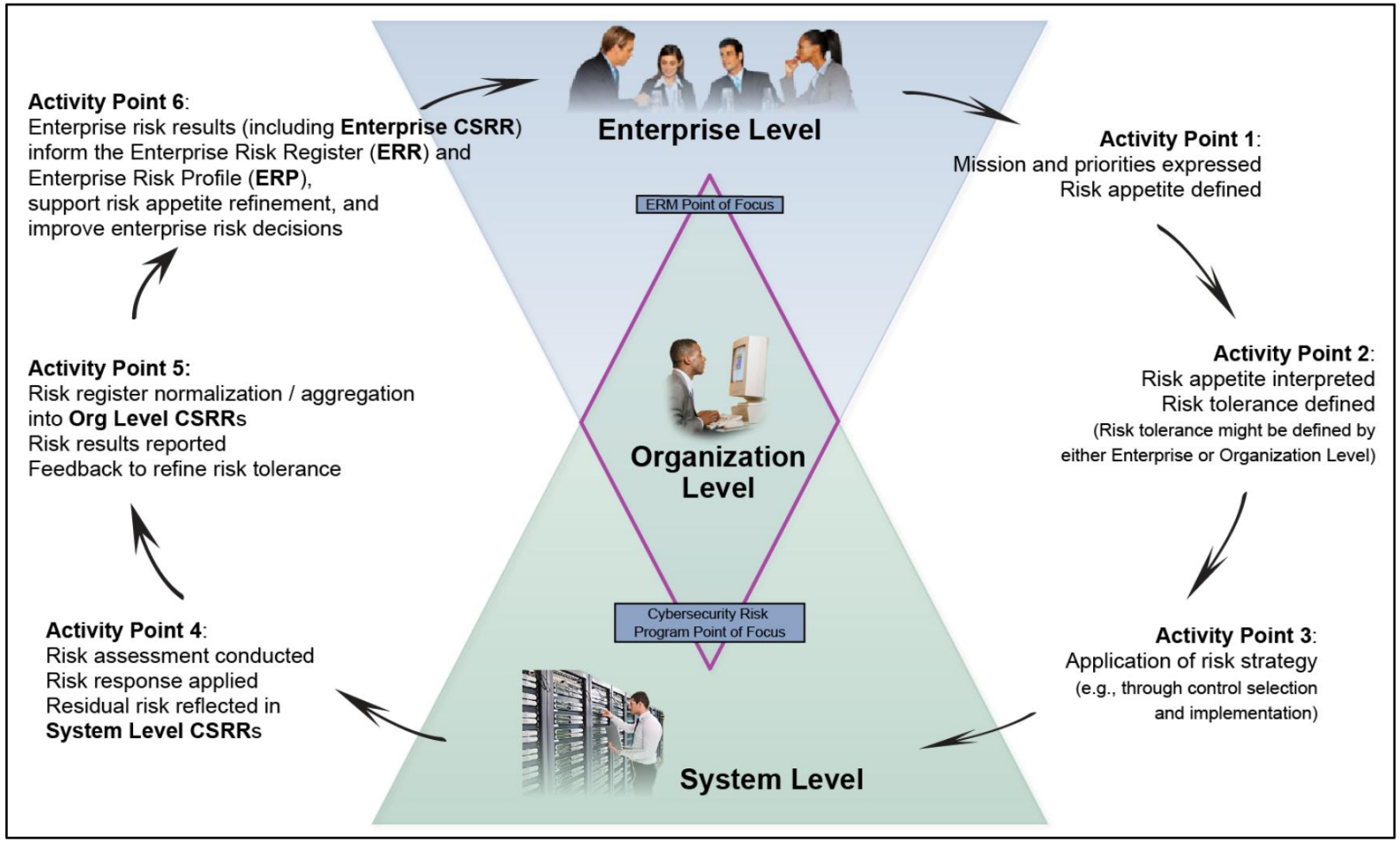
Cybersecurity Risk and ERM Alignment (Cont.)

NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)



Cybersecurity Risk and ERM Alignment (Cont.)

NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)



Enterprise Strategy for Cybersecurity Risk Coordination

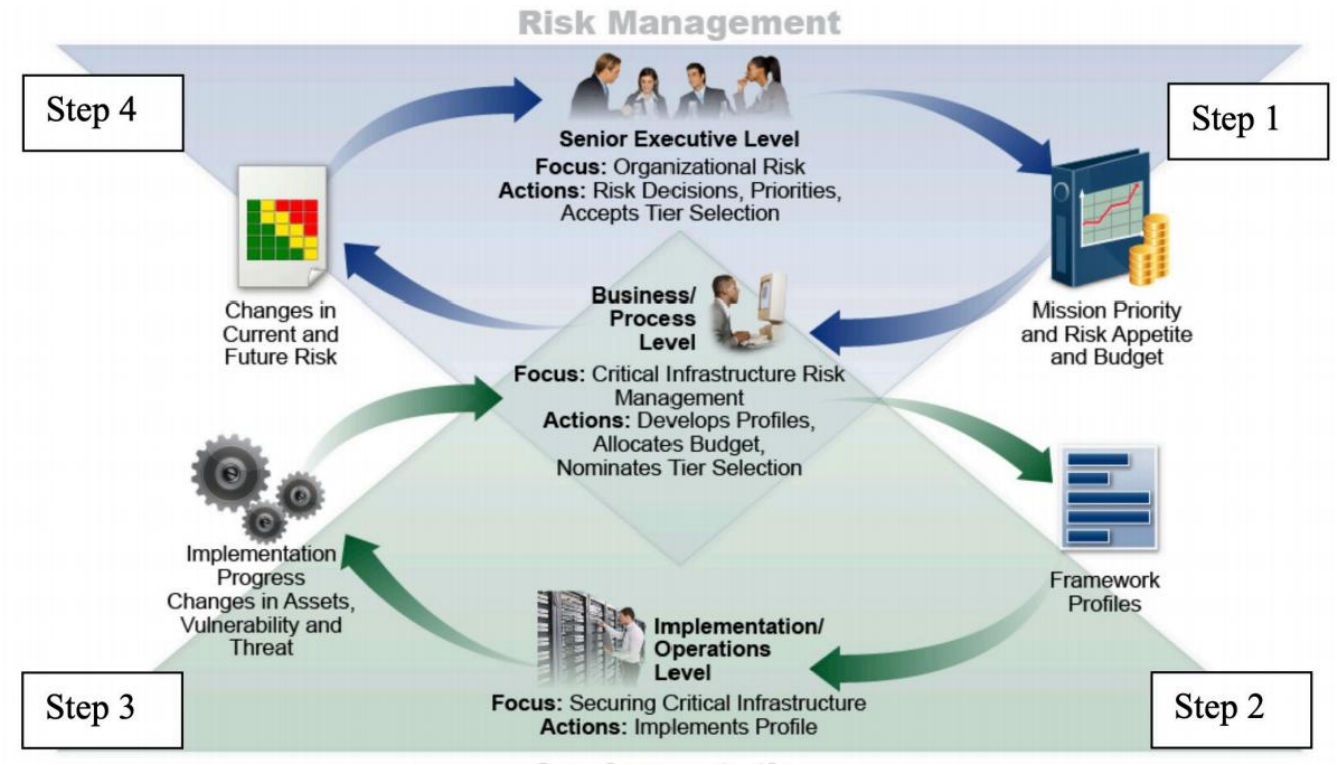
- Illustrates risk integration and coordination activities

Cybersecurity Risk and ERM Alignment (Cont.)

NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)

NIST IR 8286r1 ipd (Initial Public Draft)
February 2025

Integrating Cybersecurity and
Enterprise Risk Management



Cybersecurity Risk and ERM Alignment (Cont.)

NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)

The integration of Cybersecurity Risk Management (CSRM) into Enterprise Risk Management (ERM) per NISTIR 8286 involves six concise steps to manage cybersecurity risks in alignment with enterprise goals, with clear responsibilities.

Identify the Context: Define the enterprise environment (internal: mission, technology; external: regulations) and cybersecurity's role in supporting objectives by identifying critical assets and risk appetite (e.g., email downtime).

Identify the Risks: Catalog cybersecurity risks (threats like malware, vulnerabilities like unpatched software, assets like data) using NIST SP 800-30 and MITRE ATT&CK, documenting in a Cybersecurity Risk Register (CSRR).

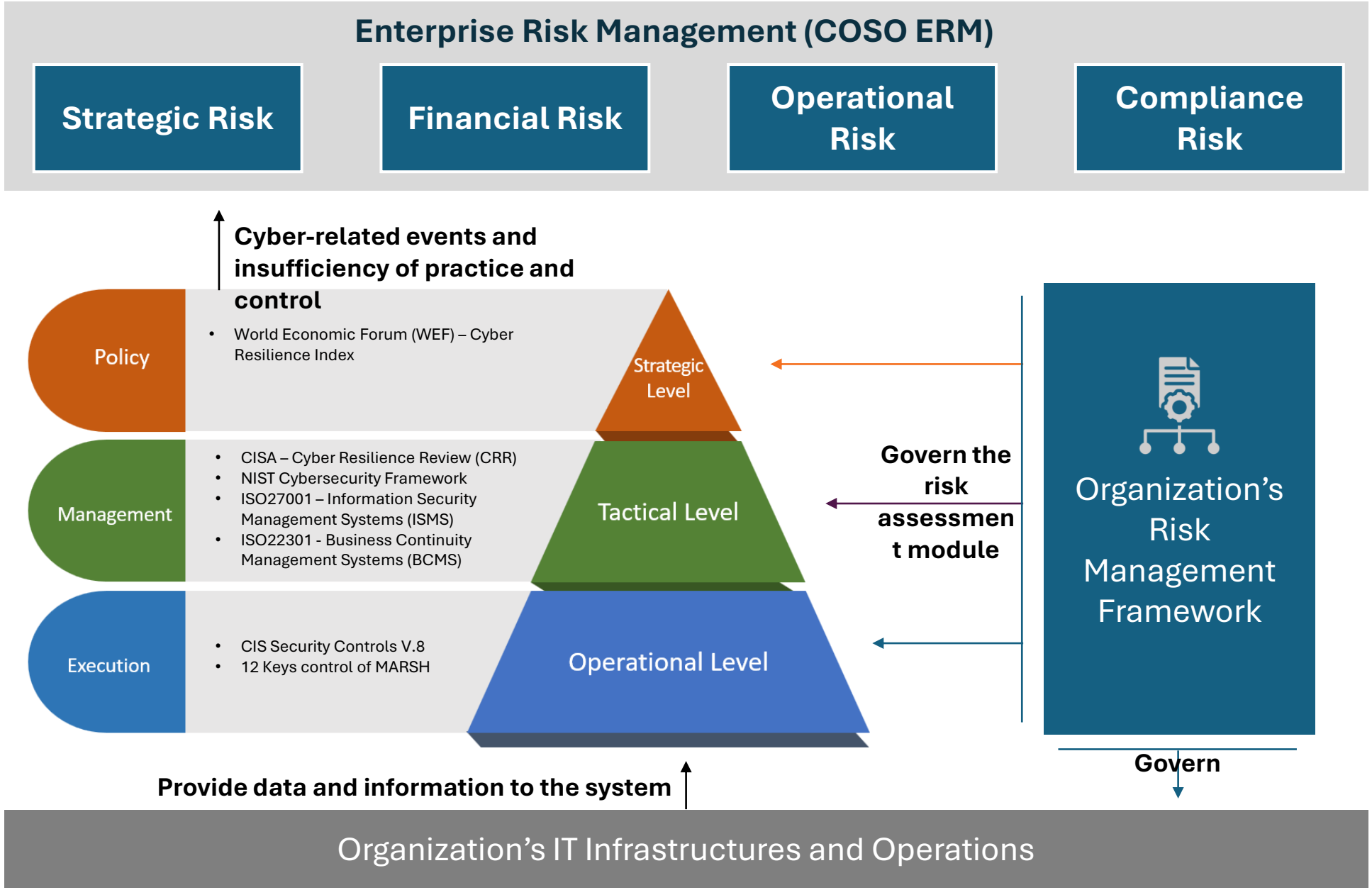
Analyze the Risks: Assess risk likelihood and impact, updating CSRR with exposure ratings.

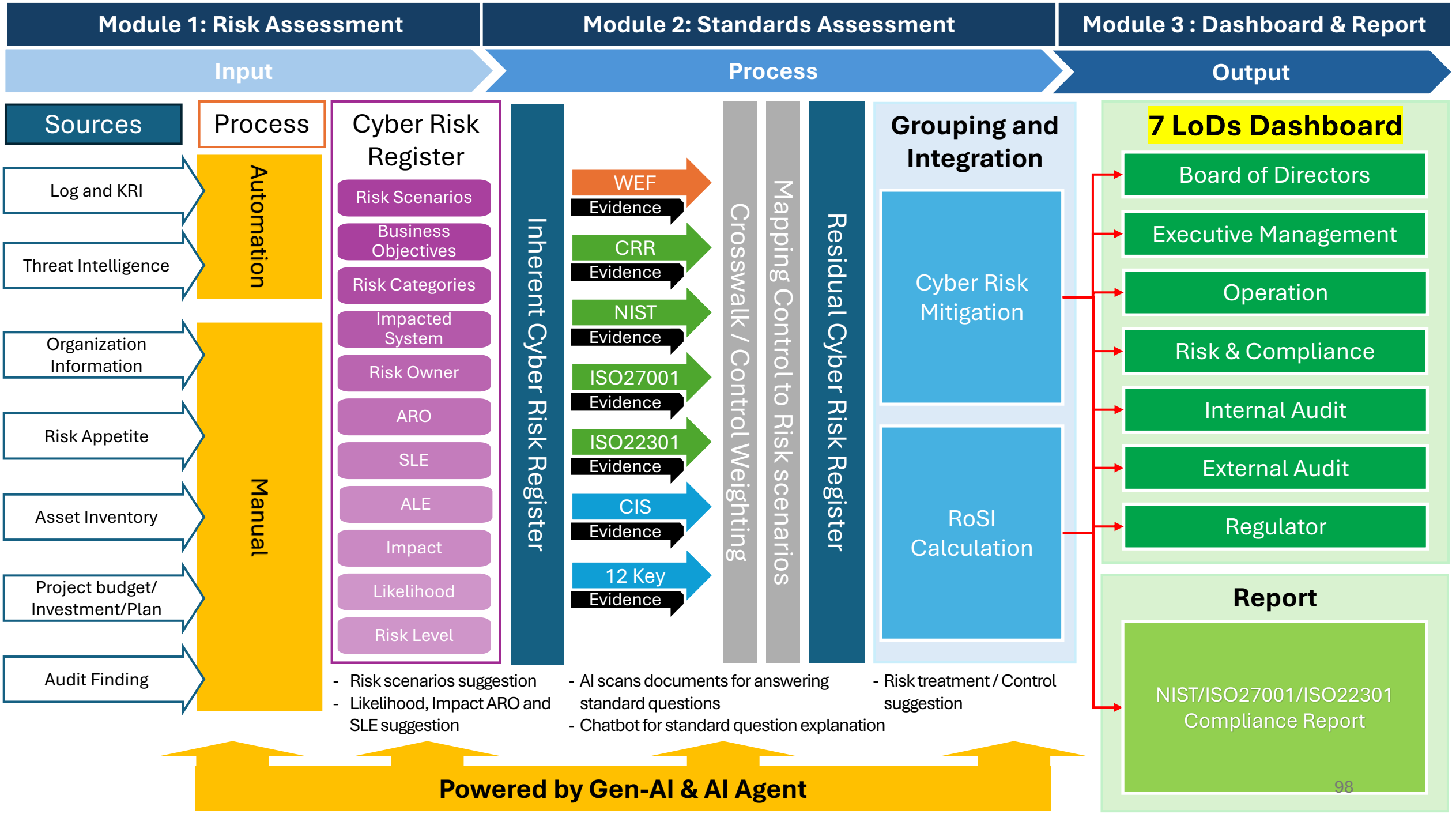
Prioritize the Risks: Rank risks by impact and likelihood using a risk matrix, considering risk appetite (e.g., prioritize high-impact ransomware), and document in CSRR.

Plan and Execute Risk Responses: Develop and apply strategies (e.g., firewalls, multi-factor authentication) to mitigate, accept, transfer, or avoid risks, or enhance opportunities, documenting controls, residual risks, and owners in CSRR.

Monitor, Evaluate, and Adjust: Track risks using key risk indicators (KRIs) and monitoring, adjust strategies for new threats, and update CSRR.

Cybersecurity Risk and ERM Alignment Conceptual Framework




Module 1: Risk Assessment
Module 2: Standards Assessment
Module 3 : Dashboard & Report
Input
Process
Output
Sources
Log and KRI
Threat Intelligence
Organization Information
Risk Appetite
Asset Inventory
Project budget/ Investment/Plan
Audit Finding
Process
Automation
Manual
Cyber Risk Register
Risk Scenarios
Business Objectives
Risk Categories
Impacted System
Risk Owner
ARO
SLE
ALE
Impact
Likelihood
Risk Level
Inherent Cyber Risk Register
WEF Evidence
CRR Evidence
NIST Evidence
ISO27001 Evidence
ISO22301 Evidence
CIS Evidence
12 Key Evidence
Crosswalk / Control Weighting
Mapping Control to Risk scenarios
Residual Cyber Risk Register
Grouping and Integration
Cyber Risk Mitigation
RoSI Calculation
7 LoDs Dashboard
Board of Directors
Executive Management
Operation
Risk & Compliance
Internal Audit
External Audit
Regulator
Report
NIST/ISO27001/ISO22301 Compliance Report
- Risk scenarios suggestion
- Likelihood, Impact ARO and SLE suggestion
- AI scans documents for answering standard questions
- Chatbot for standard question explanation
- Risk treatment / Control suggestion
Powered by Gen-AI & AI Agent

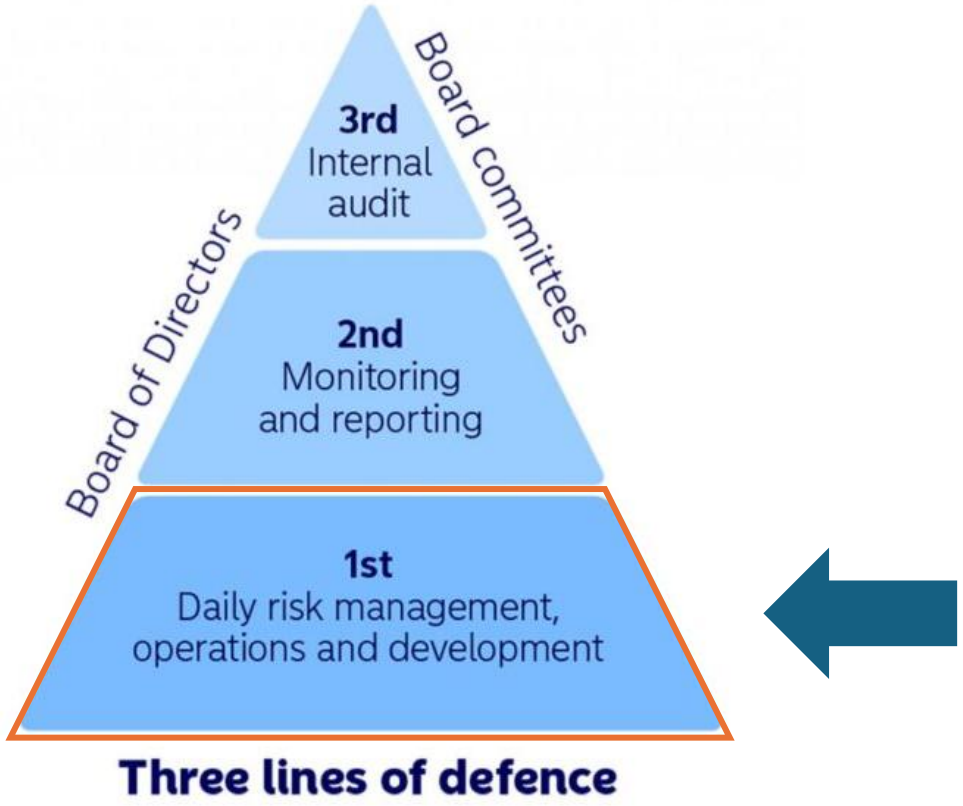
Integration Challenges and Considerations

3 Lines of Defense Model

The Three Lines of Defense (3LOD) Model, developed by the Institute of Internal Auditors (IIA), is a framework for effective governance, risk management, and internal control within organizations. It defines clear roles and responsibilities across three lines to ensure robust risk management while promoting collaboration and alignment with organizational objectives.

Integration Challenges and Considerations (Cont.)

3 Lines of Defense Model



First Line of Defense: Operational Management

Role: The first line consists of operational units, including business units, IT teams, and system owners, responsible for owning and managing cybersecurity risks in day-to-day operations.

Responsibilities for Cyber Risk:

- Identify and assess cybersecurity risks at the operational level, including system vulnerabilities and threats to data confidentiality, integrity, and availability
- Implement security controls and protective measures (e.g., firewalls, encryption, access controls)
- Execute risk response strategies within established risk appetite and tolerance parameters
- Maintain Cybersecurity Risk Registers (CSRRs) documenting risk descriptions, likelihood assessments, and potential impacts (e.g., financial, operational, reputational)

Integration Challenges and Considerations (Cont.)

3 Lines of Defense Model

Second Line of Defense: Risk Management & Compliance Functions

Role: The second line includes risk management and compliance functions responsible for overseeing and supporting the first line's risk management activities.

Responsibilities for Cyber Risk:

- Develop comprehensive cybersecurity risk frameworks, policies, and governance structures that integrate with Enterprise Risk Management (ERM) objectives
- Provide methodologies, tools, and training to support first-line risk management activities
- Normalize and aggregate system-level risks into organizational risk profiles for enterprise-level decision making and reporting
- Ensure regulatory compliance and adherence to industry standards and frameworks

Integration Challenges and Considerations (Cont.)

3 Lines of Defense Model

Third Line of Defense: Internal Audit

Role: The third line consists of internal audit or independent assurance functions, providing objective oversight to ensure the effectiveness of the first and second lines.

Responsibilities for Cyber Risk:

- Conduct objective audits of cybersecurity controls and risk management processes to verify effectiveness and compliance
- Validate that first and second lines accurately identify, assess, and mitigate cyber risks.
- Provide independent reporting to senior leadership and board regarding cybersecurity risk management effectiveness and gaps
- Recommend continuous improvements to enhance CSRM integration with enterprise risk management

Integration Challenges and Considerations (Cont.)

Examples of the percentage of responsibilities of each line for each risk management step

The chart illustrates the relative responsibilities of each line across key risk management activities.

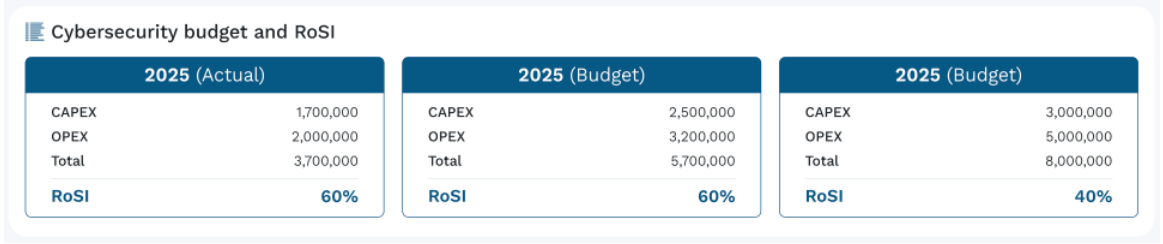
- First line has primary responsibility for identifying and mitigating risks,
- Second line focuses on assessing and monitoring
- Third line emphasizes independent reporting and validation

The percentages are illustrative, reflecting the varying intensity of each line's involvement.

Risk Reporting and Communication (Cont.)

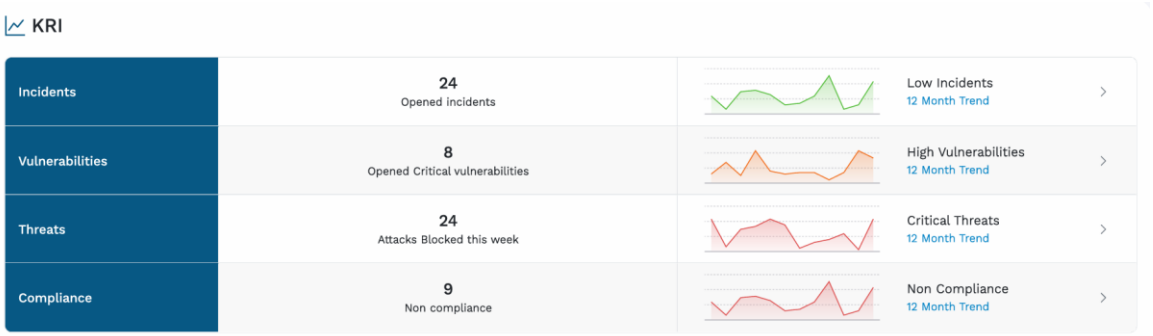
Example of Risk Dashboard

- Overall cyber risk posture of the organization
- Numbers of cyber risk scenarios by risk categories
- Current risk situation (Appetite vs current risk score by risk categories)



2025 (Actual)		2025 (Budget)		2025 (Budget)	
CAPEX	1,700,000	CAPEX	2,500,000	CAPEX	3,000,000
OPEX	2,000,000	OPEX	3,200,000	OPEX	5,000,000
Total	3,700,000	Total	5,700,000	Total	8,000,000
RoSI	60%	RoSI	60%	RoSI	40%

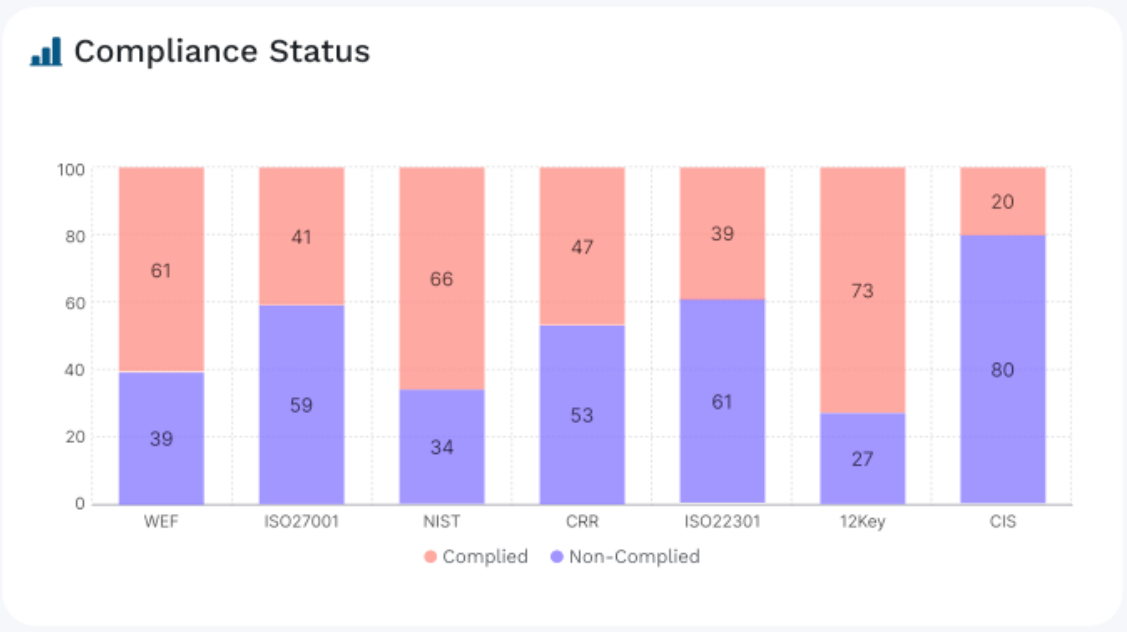
- Cybersecurity budget and actual of the organization
- Comparative return on cybersecurity investment (RoSI)

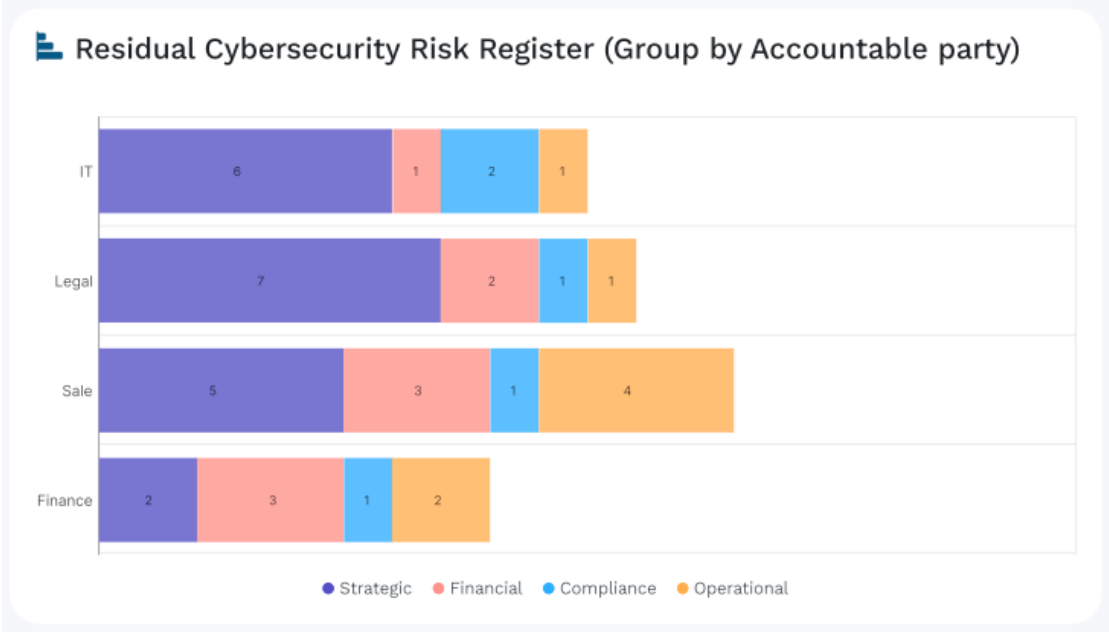


- Key risk indicators

Risk Reporting and Communication (Cont.)

Example of Risk Dashboard

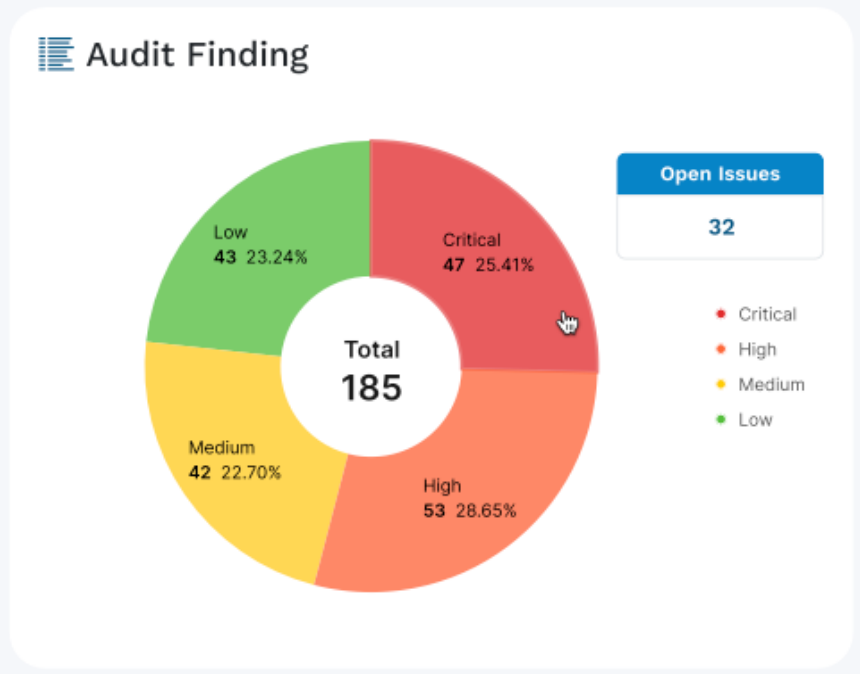




- Internation standards compliance score
- Cyber risk scenarios by accountable parties

Risk Reporting and Communication (Cont.)

Example of Risk Dashboard



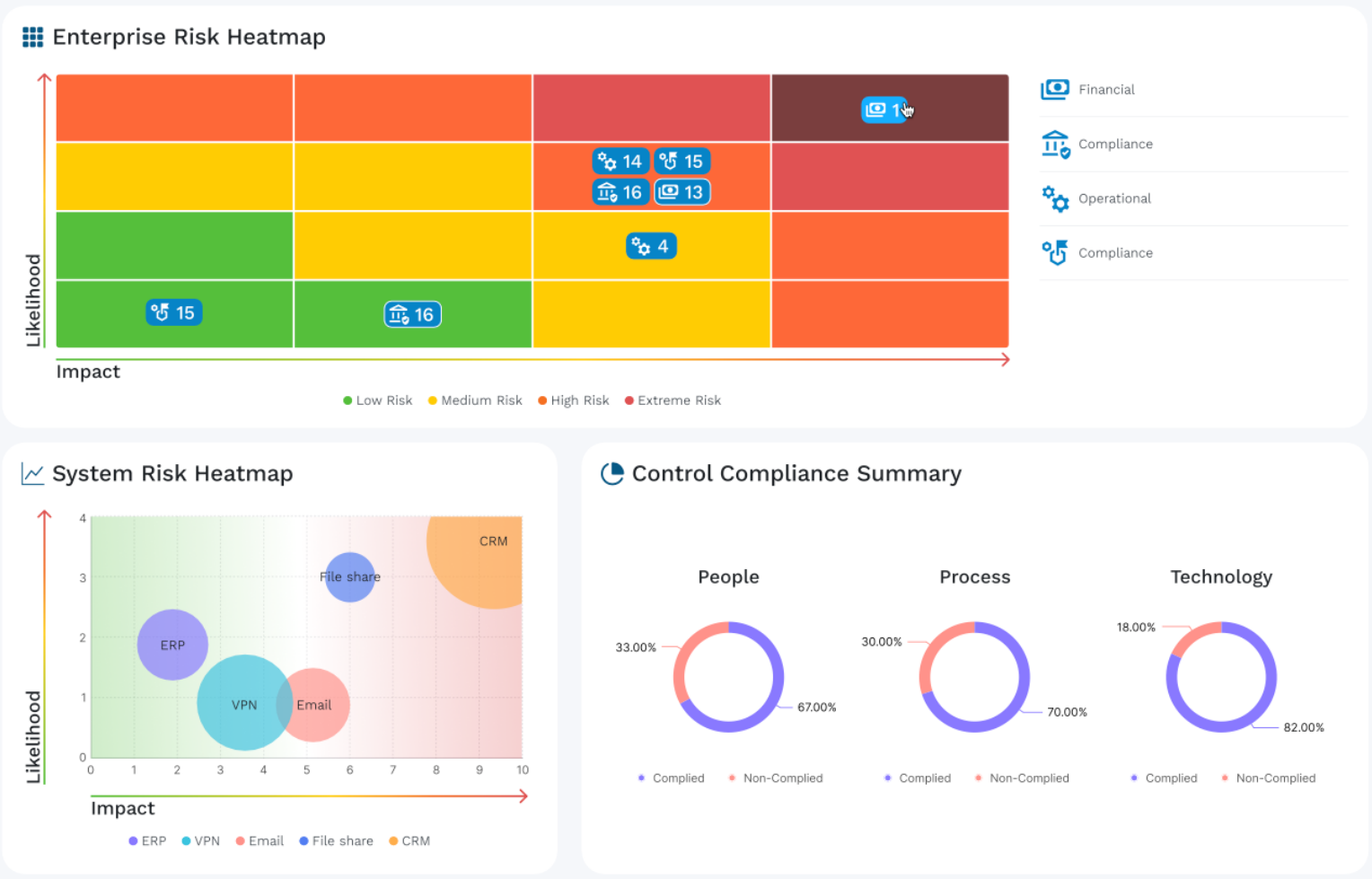
- Cyber audit findings by level of severities

Function	Category	Identifier	Maturity Level	Industry	Target
Govern (GV)	Organizational Context	GV.OC	2.34	3.4	4
	Risk Management Strategy	GV.RM	1.2	4.2	4
	Roles, Responsibilities, and Authorities	GV.RR	3.2	3.2	4
	Policy	GV.PO	2	2.5	4
	Oversight	GV.OV	4.1	3	4
	Cybersecurity Supply Chain Risk Management	GV.SC	3	4	4
Identity (ID)	Asset Management	ID.AM	3	2.4	3.5
	Risk Assessment	ID.RA	2	4.3	3.5
	Improvement	ID.IM	2.3	4.1	3.5
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA	2.4	2.2	3.5
	Awareness and Training	PR.AT	3.1	3.5	3.5
	Data Security	PR.DS	2.46	3.3	3.5
	Platform Security	PR.PS	3.32	3.8	3.5
	Technology Infrastructure Resilience	PR.IR	3.33	3.9	3.5
Detect (DE)	Technology Infrastructure Resilience	DE.CM	4.4	4.5	5
	Continuous Monitoring	DE.AE	4.2	4	5
Response (RS)	Incident Management	RS.MA	1.0	2	3
	Incident Analysis	RS.AN	3.9	3	3
	Incident Response Reporting and Communication	RS.CO	2.4	2.5	3
	Incident Mitigation	RS.MI	3.11	2.6	3
Recover (RC)	Incident Recovery Plan Execution	RC.RP	3.44	4	4
	Incident Mitigation	RC.CO	2.22	4	4

- Current cybersecurity maturity level

Risk Reporting and Communication (Cont.)

Example of Risk Dashboard

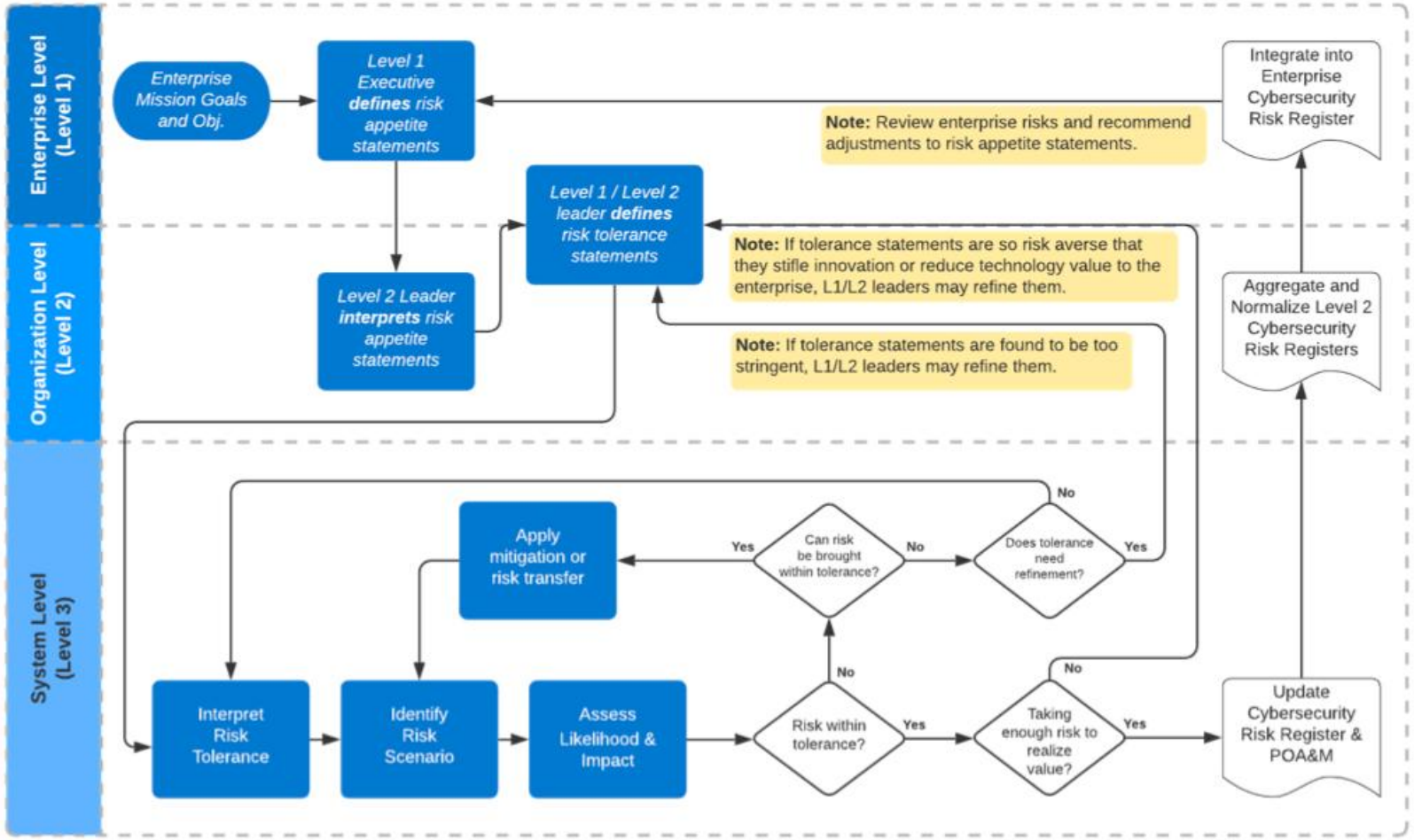


- Enterprise cyber risk heatmap

- System risk heatmap
- Control compliance score (people, process, & technology)

Cybersecurity Risk and ERM Alignment (Cont.)

NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)

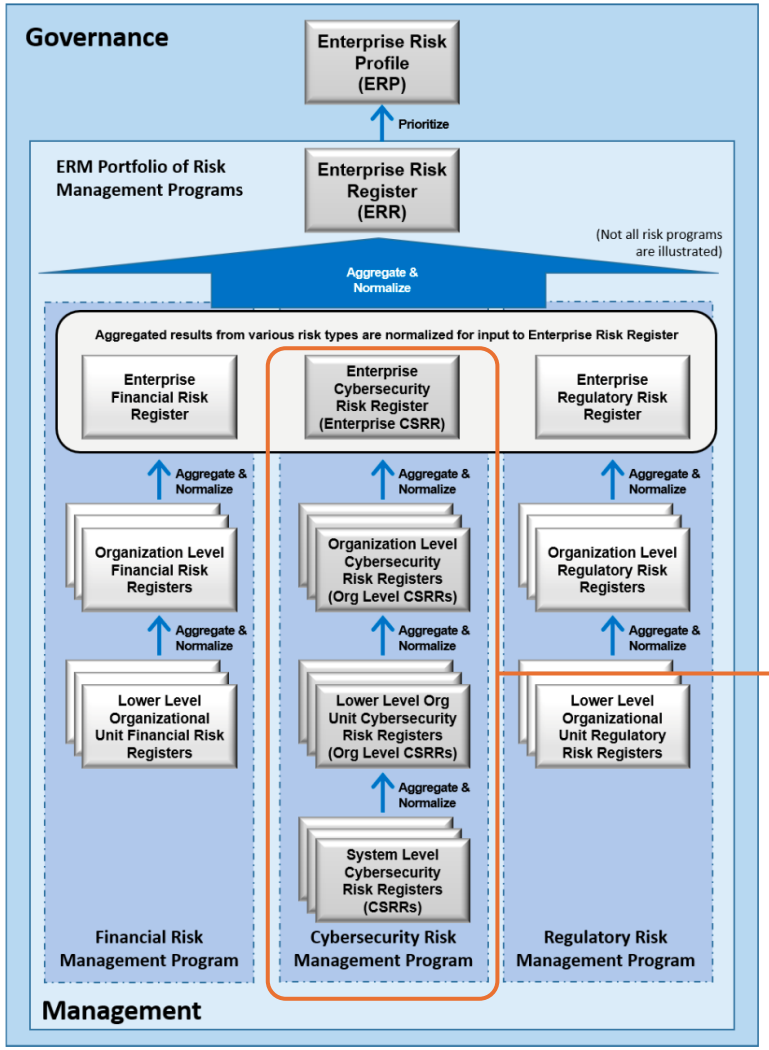


Detailed Risk Integration Strategy

- Highlights the integration of ERM and CSRM
- Cybersecurity risks are documented through cybersecurity risk registers (CSRRs), aggregated at appropriate levels
- CSRRs used to create an enterprise cybersecurity risk register, which provides input into the broader Enterprise Risk Register (ERR)

Cybersecurity Risk and ERM Alignment (Cont.)

NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM)



Cybersecurity Risk Register (CSRR)

Notional Cybersecurity Risk Register											
ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1											
2											
3											
4											
5											

Example of CSRR

Risk Events	Risk Category	Impacted system	3rd parties	ARO	SLE	Impact	Likelihood	Inherent Risk	Annual Loss Exp
Event A	Info protection	001	Vendor X	10%	1m	Low	Unlikely	Risk AA	100k
Event B	Physical security	002	Vendor G	20%	0.5m	High	Likely	Risk BB	100k
Event C	Continuity	003	Vendor S	15%	0.7m	Critical	Rare	Risk CC	105k
Event D	Governance	004	Vendor L	50%	1.5m	Medium	Certain	Risk DD	750k

Cybersecurity Risk and ERM Alignment

Cybersecurity risks in alignment with Enterprise risk management

The integration of Cybersecurity Risk Management (CSRM) into Enterprise Risk Management (ERM) per NISTIR 8286 involves six concise steps to manage cybersecurity risks in alignment with enterprise goals, with clear responsibilities.

Identify the Context: Define the enterprise environment (internal: mission, technology; external: regulations) and cybersecurity's role in supporting objectives by identifying critical assets and risk appetite (e.g., email downtime).

Identify the Risks: Catalog cybersecurity risks (threats like malware, vulnerabilities like unpatched software, assets like data) using NIST SP 800-30 and MITRE ATT&CK, documenting in a Cybersecurity Risk Register (CSRR).

Analyze the Risks: Assess risk likelihood and impact, updating CSRR with exposure ratings.

Prioritize the Risks: Rank risks by impact and likelihood using a risk matrix, considering risk appetite (e.g., prioritize high-impact ransomware), and document in CSRR.

Plan and Execute Risk Responses: Develop and apply strategies (e.g., firewalls, multi-factor authentication) to mitigate, accept, transfer, or avoid risks, or enhance opportunities, documenting controls, residual risks, and owners in CSRR.

Monitor, Evaluate, and Adjust: Track risks using key risk indicators (KRIs) and monitoring, adjust strategies for new threats, and update CSRR.

Cybersecurity Risk and ERM Alignment (Cont.)

Techniques for Aligning Cybersecurity Risk with ERM

Risk Registers: Key tool to document, communicate, and manage cyber risks at all levels; IT teams record threats (e.g., ransomware, data breaches) in Cybersecurity Risk Register (CSRR), aggregated into Enterprise Risk Register (ERR) and Profile (ERP).

Language Alignment: Translate technical metrics (e.g., CVSS scores) into business impacts (e.g., financial loss, reputation harm) using COSO's four objectives (Strategic, Operations, Reporting, Compliance).

Cyber risk should be expressed in business terms: Cyber risks affect multiple categories thus ERM alignment requires understanding and communicating those cross-cutting impacts. (e.g., operations disruption, compliance violations).

Risk Cross-Functional Team: Form a team with IT security, risk management, compliance, and business leaders to assess cyber risks for both IT and business impacts, entering them into the corporate risk register.

Corporate Risk Register Documentation: Evaluate and document cyber risks (e.g., breaches) in business terms (e.g., financial loss) for integrated tracking.

Cyber Risk Appetite Statements: Develop specific thresholds, e.g., "zero tolerance for data loss" or "<1 major breach/year," to guide strategy.

Cyber Metrics Alignment: Tie metrics like high-severity incidents or patching timelines to appetite statements for monitoring and response.

Cybersecurity Risk and ERM Alignment (Cont.)

Approach to Model Cybersecurity Risks and Threats

1) Model Risks with Scenario Analysis

Identify and quantify risks by creating scenarios for critical assets (e.g., customer data) and threats (e.g., ransomware, $4.88M cost) using MITRE ATT&CK, Verizon 2024 DBIR (60% breaches via phishing), and a risk matrix (4/5 likelihood, 5/5 impact) with Monte Carlo simulations.

2) Leverage Industry Benchmarks

Use industry metrics like $200–$400/record, $4.88M/breach (IBM 2024), and MFA's 99% phishing reduction (NIST), aligning spending (5–10% IT budget, Gartner) with sector trends.

3) Use Threat Intelligence

Detect emerging threats with data from Recorded Future, CrowdStrike (68% ransomware rise, 2024), and MITRE ATT&CK, monitoring dark web and deploying SIEM (Splunk, $10K–$100K/year) with threat feeds.

4) Conduct Tabletop Exercises

Test incident response through quarterly simulations (e.g., ransomware) with IT, legal, and executives, aiming for <4-hour recovery.

5) Leverage External Expertise

Engage consultants for penetration testing, MSSPs for 24/7 SOC, and ISACA for AI-driven threat intel.

Risk Reporting and Communication

Risk Reporting and Communication

Risk Registers as Communication Tools

A risk register is fundamentally a reporting tool – a structured repository of risk information. In the context of cyber risk, NIST highlights the risk register as *"a key tool to document, communicate, and manage cybersecurity risk at each level of the enterprise"*. These are critical tools for documenting and communicating cybersecurity risks.

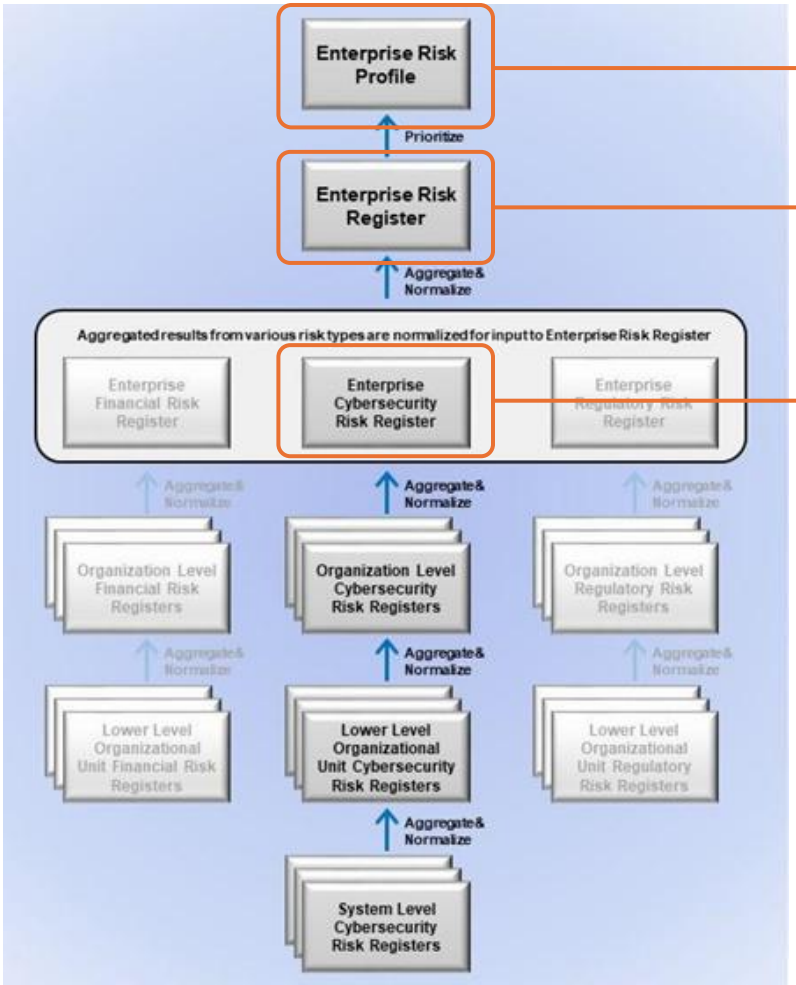
Notional Cybersecurity Risk Register Template (NISTIR 8286)

Notional Cybersecurity Risk Register											
ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1											
2											
3											
4											
5											
Continually Communicate, Learn and Update											

Risk Register:	ID (Risk Identifier)
	Priority
	Risk Description
	Risk Category
	Current Assessment—Likelihood
	Current Assessment—Impact
	Current Assessment—Exposure Rating
	Risk Response Type
	Risk Response Cost
	Risk Response Description
	Risk Owner
	Status

Risk Reporting and Communication (Cont.)

Creating and Maintaining an Enterprise-Level Cybersecurity Risk Register



Cybersecurity Risk Registers (CSRRs) → Enterprise Risk Register (ERR) → Enterprise Risk Profile (ERP)

Enterprise Risk Profile (ERP)

A prioritized subset of risks from the ERR, used by senior leaders to make informed decisions on resource allocation and risk responses

Enterprise Risk Register (ERR)

Aggregates and normalizes CSRRs and other risk registers to provide a portfolio view of risks across the enterprise.

Cybersecurity Risk Registers (CSRRs)

CSRRs track risk descriptions, impacts, likelihood, mitigation strategies, and owners, serving as inputs to the ERM process.

Risk Reporting and Communication (Cont.)

Best Practice and Communication Technique

1. Tailor Communication to Stakeholders

- **Board of Directors**: Provide high-level insights and assurance on cyber risk management.
- **Executives**: Link cyber risks to strategic goals and resource needs.
- **Business Unit Leaders**: Offer actionable steps to manage risks in their domains.
- **Risk Practitioners**: Share consistent, structured data for risk management.

2. Use Clear and Accessible Methods

- **Employ Visuals**: Use heat maps and dashboards for quick comprehension.
- **Leverage Storytelling**: Present what-if scenarios and case studies for relatability.
- **Avoid Jargon**: Simplify technical terms for non-expert audiences.

3. Ensure Two-Way Communication

- **Upward Reporting**: Share risk status and progress with leadership.
- **Address Concerns**: Respond to specific stakeholder questions with data.
- **Encourage Feedback**: Invite input to identify and address gaps.

4. Establish Regular Reporting Schedule

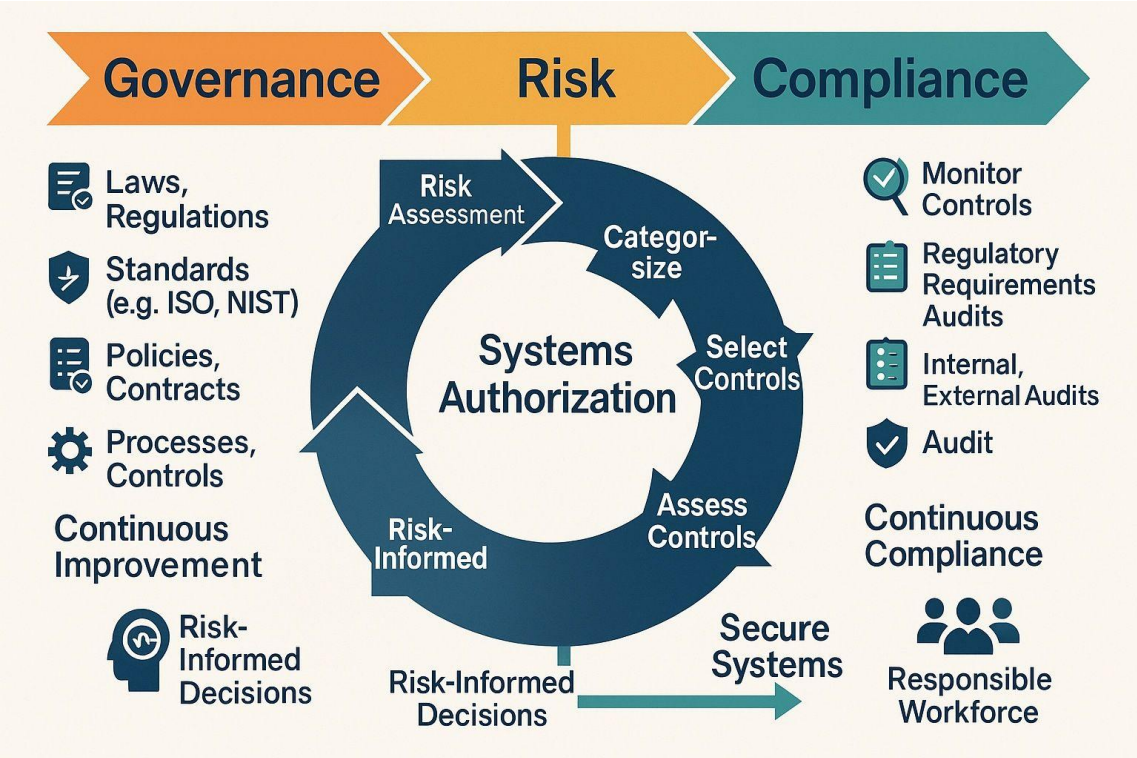
- **Set Reporting Schedule**: Provide quarterly reports and monthly updates.
- **Integrate with Enterprise Discussions**: Link cyber risks to business objectives.
- **Use Technology**: Leverage GRC platforms for automated reporting.

Recommendations for Organizations

Recommendations for Organizations

Aligning governance, risk, and compliance

Governance, Risk, and Compliance (GRC) are no longer distinct silos in the complicated business world of today; rather, they are all connected that guarantee an organization's continued security, compliance, and resilience.



Governance sets the rules and direction. It ensures that:

- Laws and regulations are respected
- Industry standards (like ISO, NIST) are followed
- Policies and contracts align business goals with ethical obligations
- Processes and controls are clearly defined and enforced

Risk management isn't about avoiding risk—it's about knowing your risk.

- It starts by categorizing systems and assessing risks at every tier (organization, business line, assets)
- Then moves to selecting and implementing controls, followed by continuous monitoring

Compliance ensures that you're not just secure, but accountable.

- You monitor the threat landscape and controls
- You self-assess and prepare for audits
- You go through external and internal audits, ensuring adherence to standards and regulations

Recommendations for Organizations (Cont.)

Formalizing Second-Line Responsibilities for Cyber Risk

The second line of defense (e.g., CISO, risk management, compliance teams) oversees and supports the first line in managing cybersecurity risks, integrating them into enterprise risk management (ERM). Formalized responsibilities include:

Develop Frameworks: Create policies and templates (e.g., NIST Cybersecurity Framework, CSRRs) for consistent risk management.

Guide Risk Appetite: Translate enterprise risk appetite (e.g., “low appetite for data breaches”) into operational tolerance (e.g., “5-minute max downtime”).

Monitor First Line: Provide tools, training, and reviews to ensure effective risk identification and mitigation, using KRIs and GRC tools.

Normalize Risks: Aggregate and standardize CSRRs into organizational risk registers for enterprise reporting.

Ensure Compliance: Verify adherence to regulations (e.g., SEC rules) and standards (e.g., NIST SP 800-53).

Facilitate Escalation: Escalate significant risks to the Enterprise Risk Register (ERR) and Profile (ERP), ensuring bidirectional communication.

Recommendations for Organizations (Cont.)

Steps for Effective Audit and Control of Information Systems

Step 1: Clearly define the scope (e.g., access control) and align with compliance goals (e.g., PDPA, SOX).

Step 2: Gather documents to understand current controls and identify gaps.

Step 3: Assess risks using frameworks like COSO ERM, prioritizing high-impact issues.

Step 4: Conduct tests (e.g., sample 100 users for MFA compliance) to validate control effectiveness.

Step 5: Document issues with evidence to support remediation efforts.

Step 6: Provide actionable recommendations with timelines and responsibilities.

Step 7: Tailor reports for stakeholders (e.g., board, executives) to ensure alignment.

Step 8: Re-test and monitor to confirm remediation and track ongoing compliance.

Recommendations for Organizations (Cont.)

Strengthening Cybersecurity with Risk Management

In today's evolving cyber threat landscape, effective cyber risk management is essential. Organizations must adopt comprehensive strategies, such as strengthening internal controls, conducting vulnerability testing, and maintaining reliable backup systems, to mitigate risks and ensure a swift response to cybersecurity incidents.

Internal Controls

- Implement strong access controls with multi-factor authentication and least privilege principles.
- Develop clear cybersecurity policies and conduct regular employee training to raise awareness.
- Use continuous monitoring and audits to detect unusual activities early.

Vulnerability Testing

- Conduct regular vulnerability assessments and penetration tests to identify security gaps.
- Prioritize and promptly fix critical vulnerabilities based on risk level.
- Retest after remediation to ensure issues are resolved.

Backup Systems

- Maintain regular, secure backups stored both onsite and offsite (cloud).
- Protect backups with encryption and access controls to prevent tampering.
- Test backup restoration processes regularly to ensure quick recovery after an incident.
- These measures help organizations proactively detect threats, reduce risks, and recover quickly from cyber incidents.

Recommendations for Organizations (Cont.)

Strengthening Cybersecurity with Enterprise Risk Management

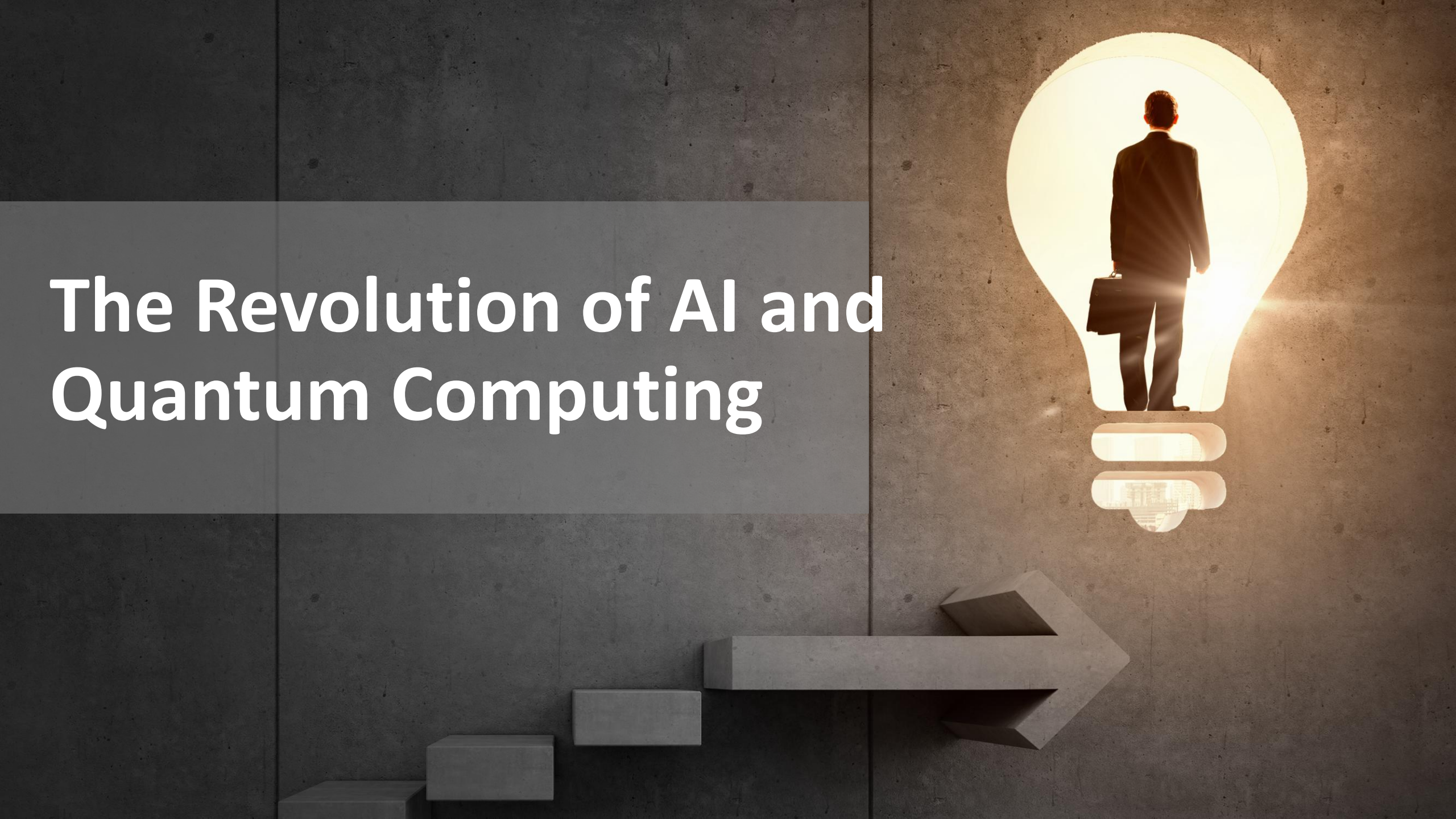
Recommendation	Details	Outcome/Benefit
Elevate Governance & Accountability	Assign CISO/CIO as accountable owner, report to board's risk/audit committee; include cyber risk in ERM agenda with appetite/tolerance; form a Cyber Risk Committee with IT, risk, compliance, and business leaders.	Ensures high-level ownership and cross-functional oversight.
Develop a Unified Risk Framework	Map NIST/ISO 27001 to COSO ERM/ISO 31000; create a common glossary (e.g., "risk appetite"); standardize scales (e.g., 5x5 matrix) and train all departments.	Harmonizes frameworks and terminology for consistent risk integration.
Use Cyber Risk Registers	Implement CSRRs at system/business-unit levels, roll up into ERR; align with enterprise categories and use business impact language as primary communication tool.	Bridges silos with structured, aggregated risk reporting and audit trails.
Align Cyber Risk Analysis	Tie assessments to objectives (Strategic, Operational, Financial, Compliance); estimate business impacts (e.g., downtime) against tolerance, guided by enterprise priorities.	Ensures relevance to enterprise goals and informed risk evaluation.
Integrate Risk Reporting	Include cyber in quarterly ERM updates; set escalation triggers (e.g., breach >10,000 records); align with annual workshops/reports and crisis protocols.	Sustains awareness and enables timely escalation.

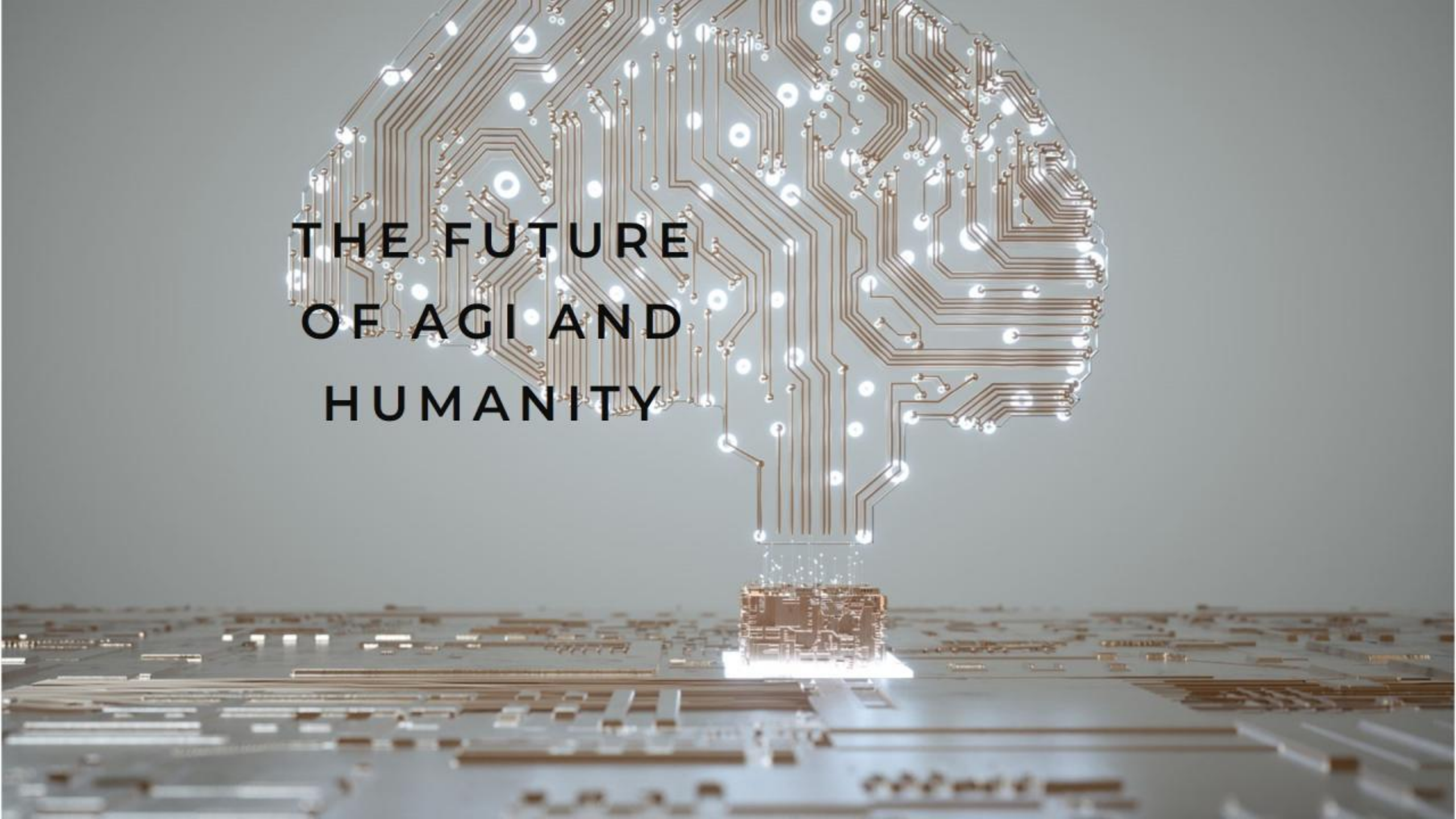
Recommendations for Organizations (Cont.)

Strengthening Cybersecurity with Enterprise Risk Management

Recommendation	Details	Outcome/Benefit
Enhance Cross-Functional Collaboration	Use job rotations, joint training (ERM for IT, cybersecurity for risk staff), and liaison roles (e.g., ERM in IT) to foster understanding.	Improves collaboration and mutual knowledge sharing.
Invest in Risk Analytics & Tooling	Use GRC platforms or spreadsheets for a unified data repository; leverage analytics/dashboards and explore AI/ML for insights; start small (e.g., automate registers).	Enhances risk prioritization and reduces manual errors with scalable tools.
Establish Cyber Risk Appetite	Formulate appetite statements (e.g., low for data loss, moderate for IT disruption <X hours); integrate into project decisions and involve risk in committees.	Embeds cyber risk into strategic decision-making.
Implement Key Risk Indicators (KRIs)	Set thresholds (e.g., “High” risk), automate data collection (e.g., vulnerability stats), report regularly, and refine KRIs over time.	Provides early visibility and aligns IT/risk teams proactively.
Integrate Third-Party Risks	Assess supply chain/third-party risks (e.g., cloud outages) in ERM, track in risk register, and include systemic risks (e.g., malware) in discussions.	Covers ecosystem risks critical to modern operations.
Audit & Continuously Improve	Conduct periodic audits to assess integration (e.g., risk register use, board satisfaction); adapt to new guidance (e.g., NIST CSF 2.0) and address weaknesses.	Ensures ongoing maturity and alignment with evolving threats.

The Revolution of AI and Quantum Computing

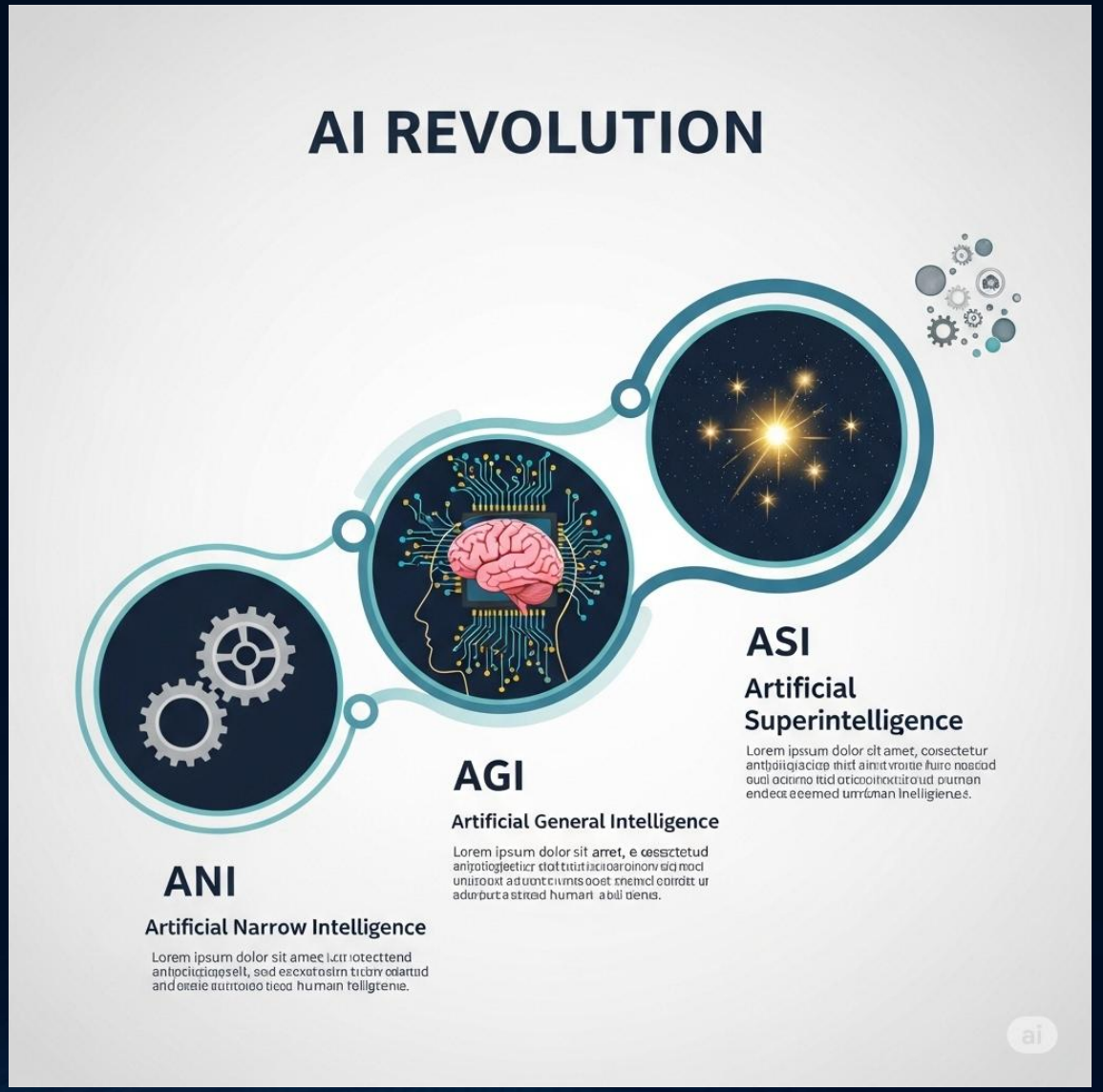



THE FUTURE
OF AGI AND
HUMANITY

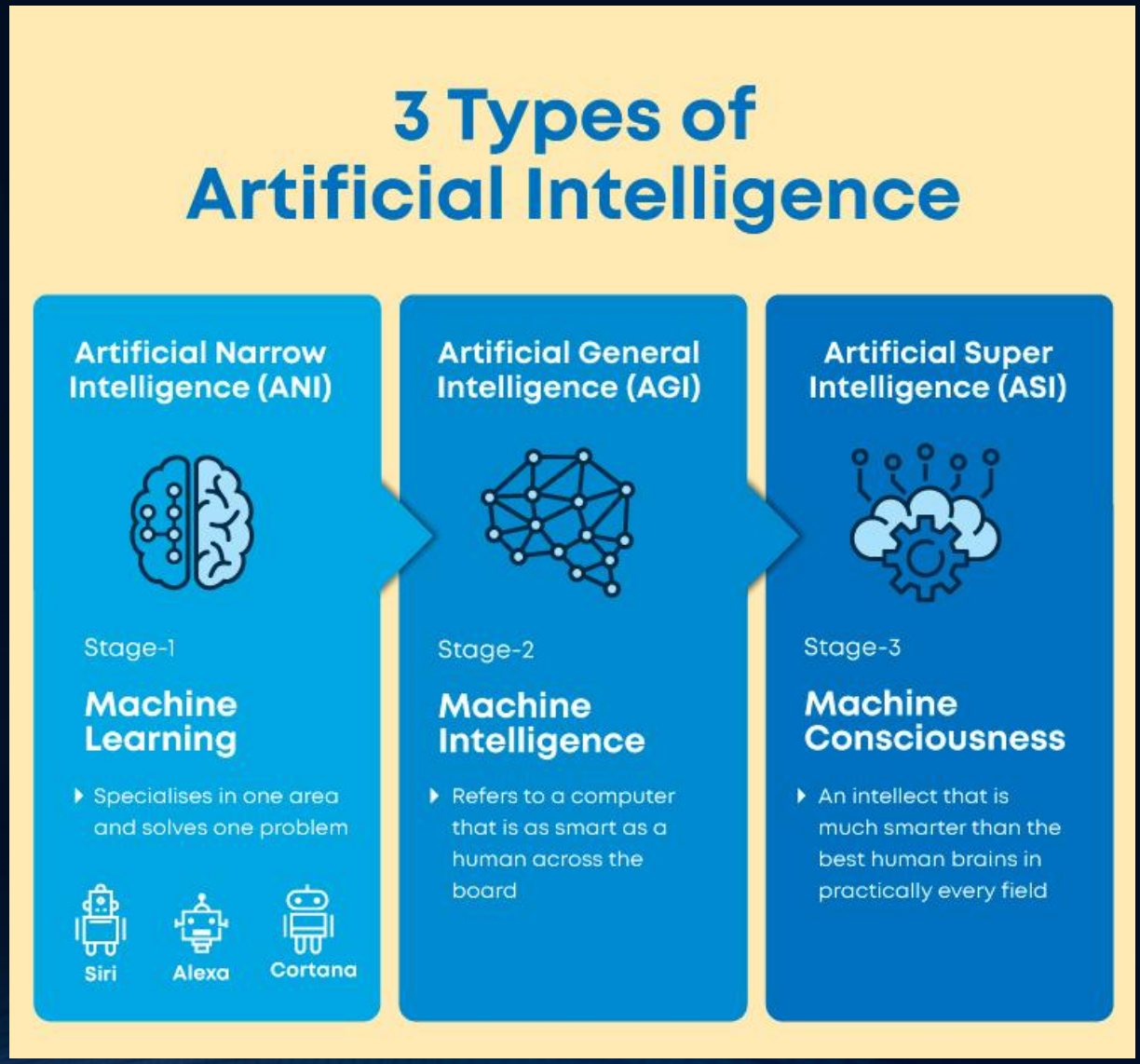
Prediction for AGI 2025-2030

The Road to AGI

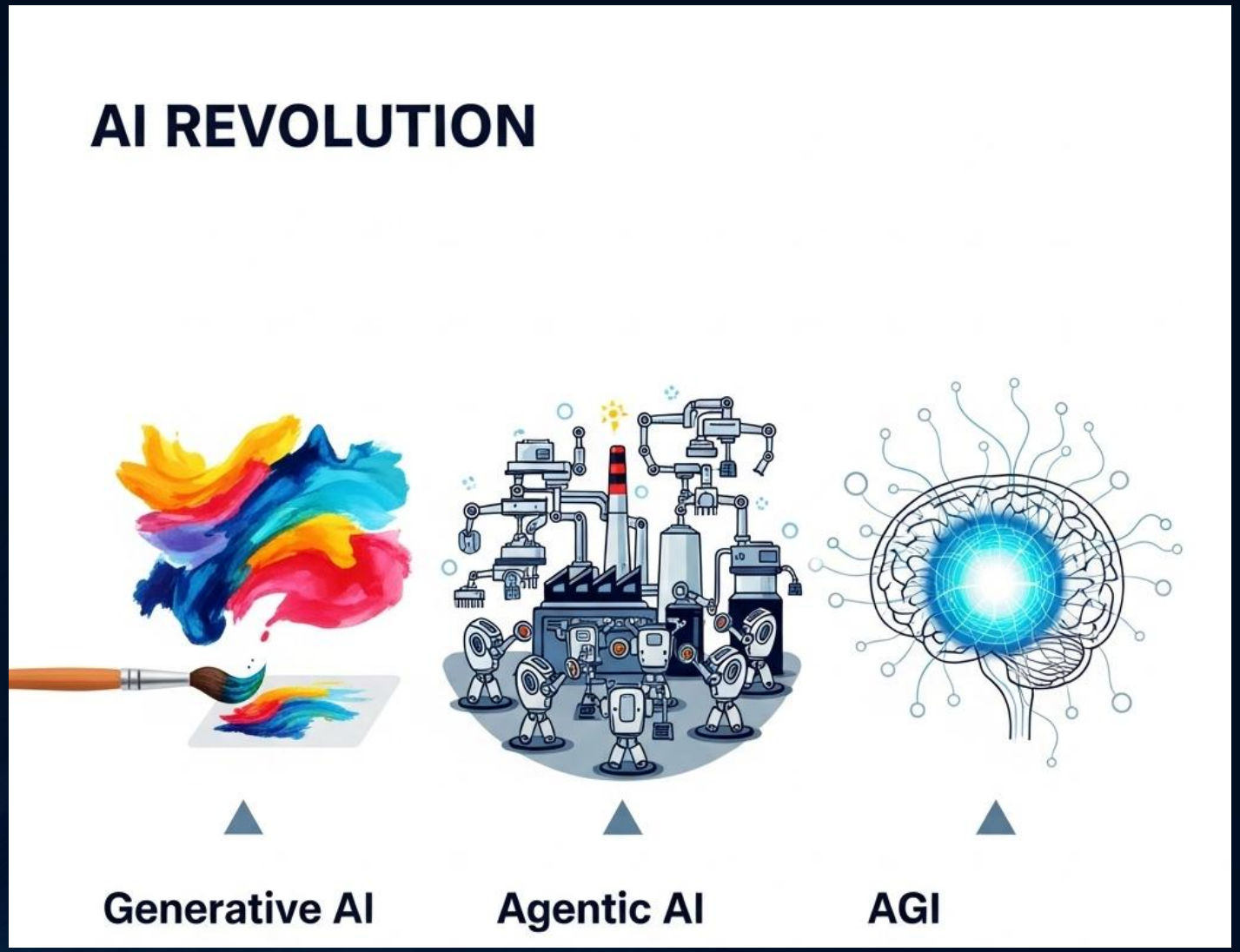
ANI->AGI->ASI



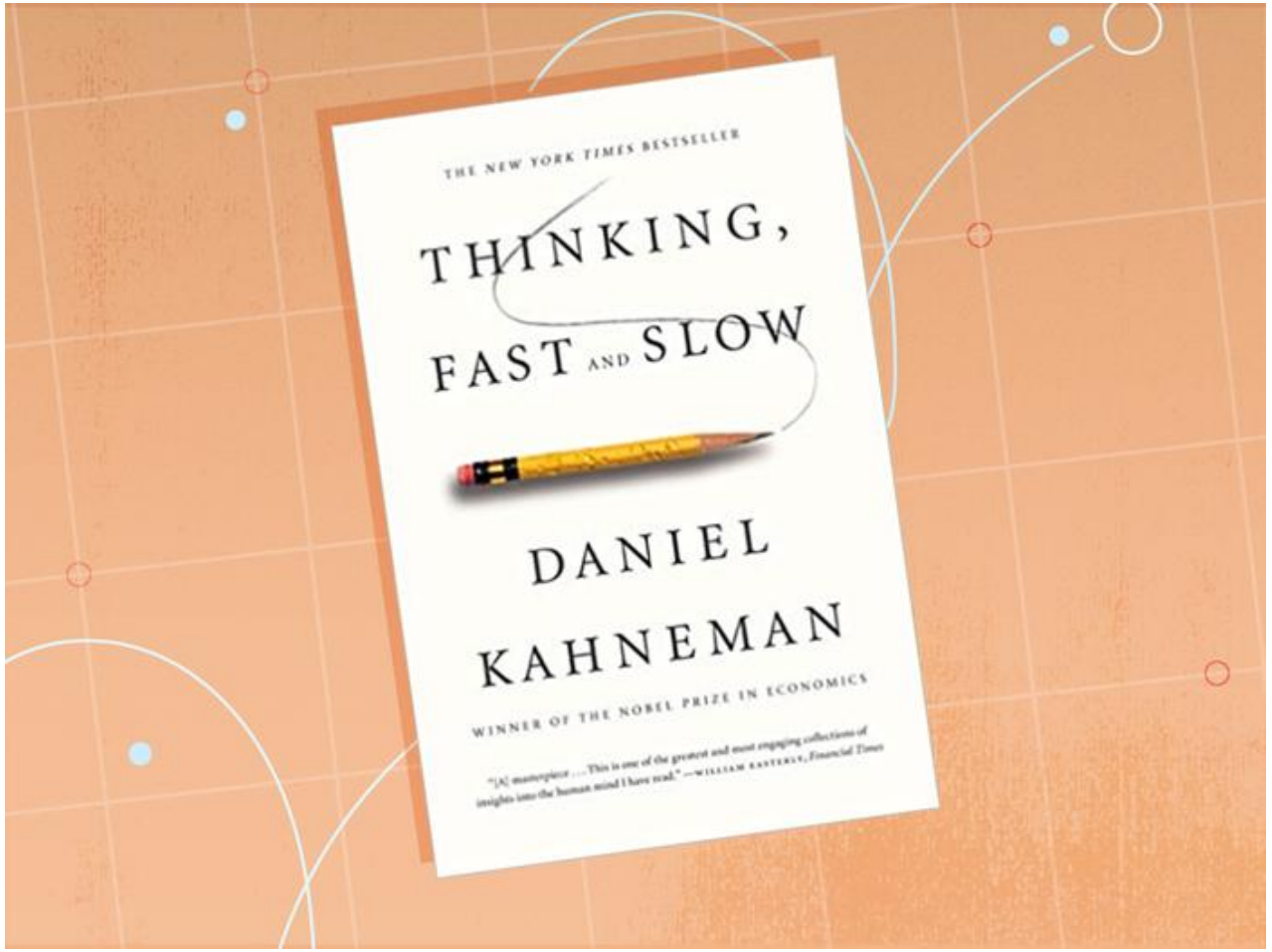
ANI->AGI->ASI



Generative AI -> Agentic AI -> AGI



Human Thinking : System I and System II



SYSTEM 1

Intuiition & instinct

95%

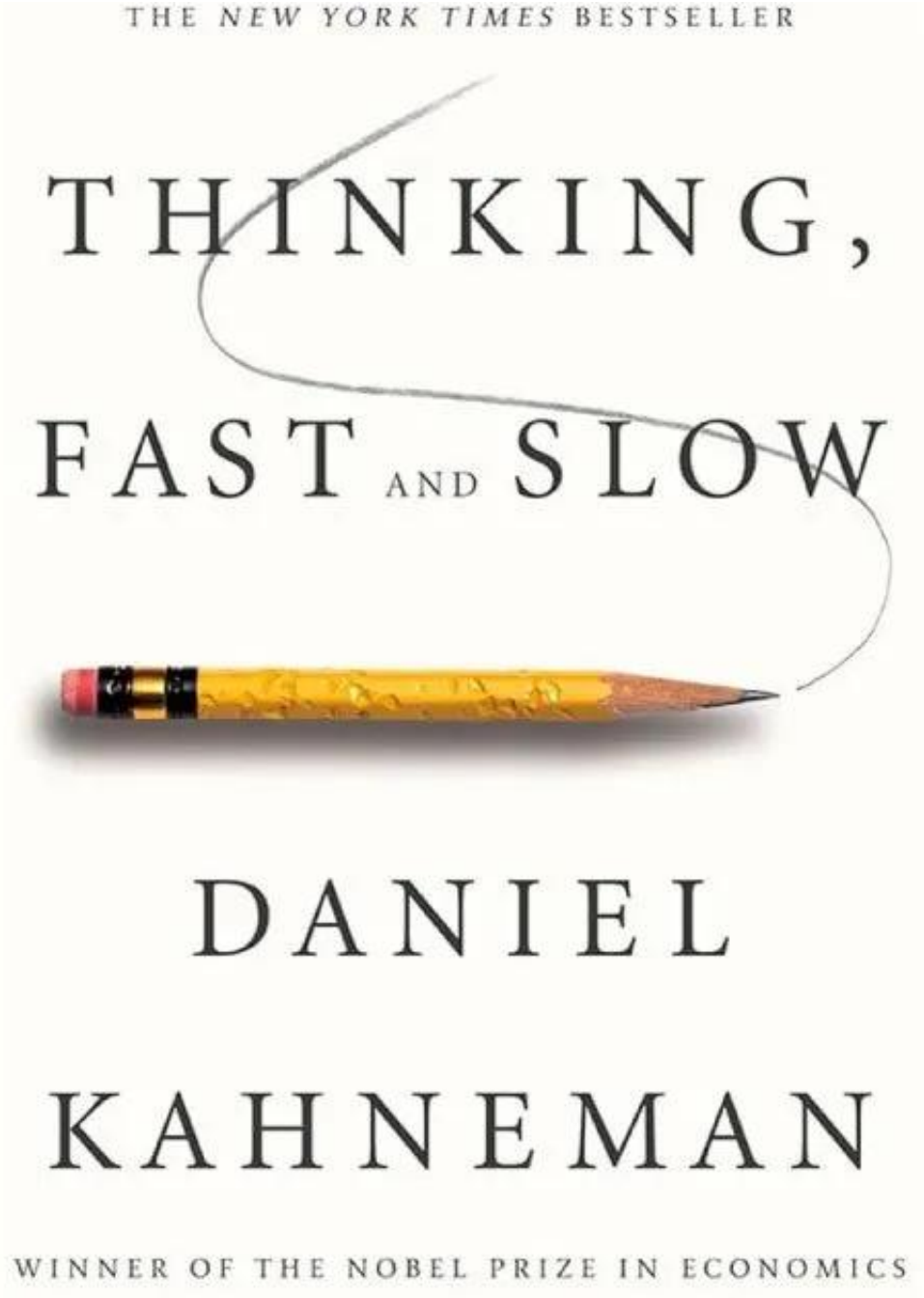
Unconscious
Fast
Associative
Automatic pilot

SYSTEM 2

Rational thinking

5%

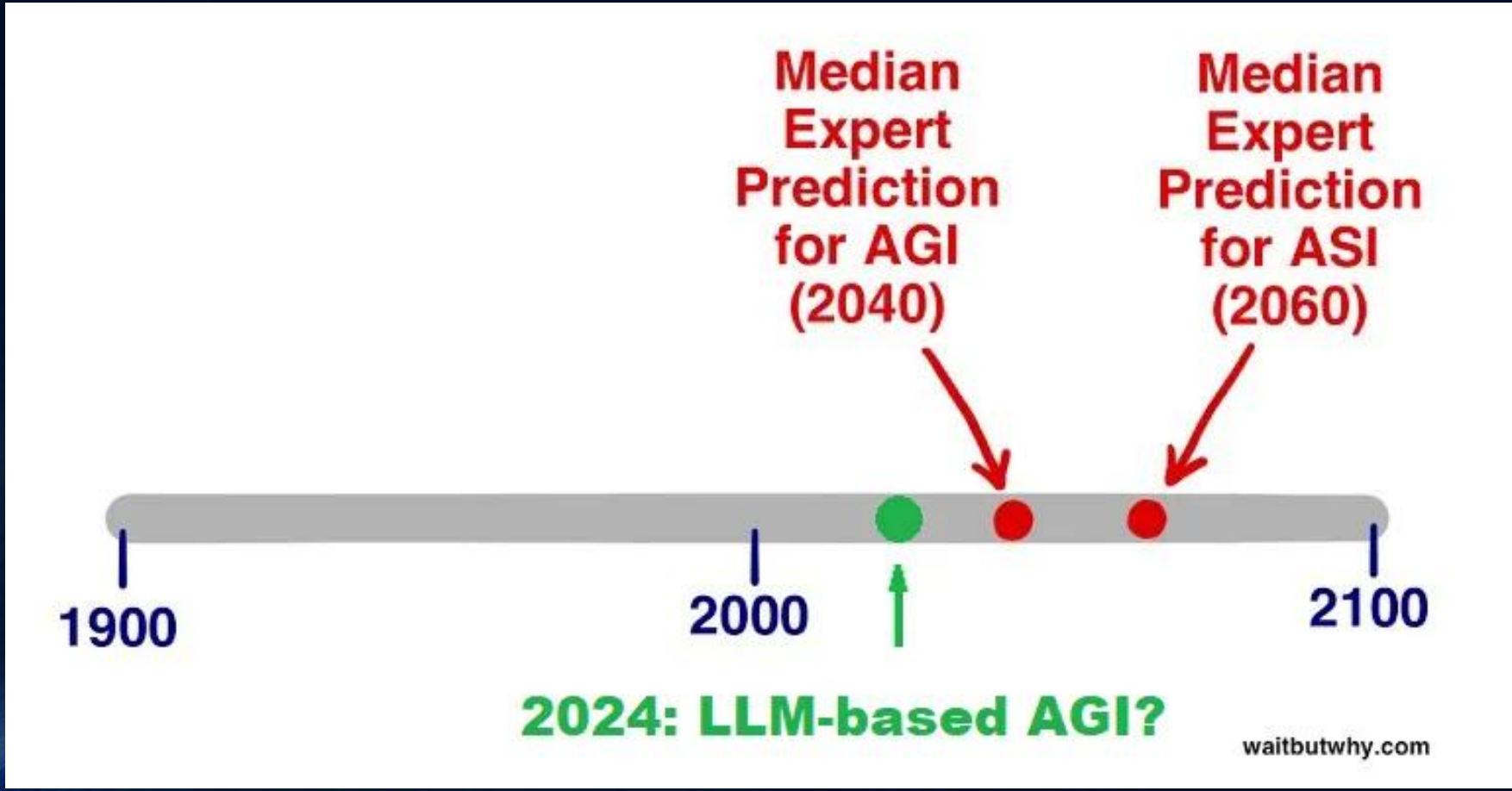
Takes effort
Slow
Logical
Lazy
Indecisive



SYSTEM 1	SYSTEM 2
FAST	SLOW
SUBCONSCIOUS	CONSCIOUS
AUTOMATIC	EFFORTFUL
EVERYDAY DECISIONS	COMPLEX DECISIONS
ERROR PRONE	RELIABLE

Human System II Thinking => AI Reasoning (CoT)

Prediction for AGI 2040-2060



Evolution of the Technology Curve

1

2023-2024

Generative AI

Content creation, summarisation, and coding assistance dominated the landscape

2

2025-2026

Agentic AI & Reasoning

Autonomous task execution and complex problem-solving capabilities emerge

3

2027+

AGI & Embodied

Human-level capability with robotics integration transforms operations

Strategic Risks & Challenges

Navigating the Headwinds

1 Security

Agentic AI increases the attack surface, with prompt injection potentially leading to unauthorised actions across systems

2 Governance

Liability frameworks remain unclear when autonomous agents make mistakes or create unintended consequences

3 Talent

The skill gap shifts from "prompt engineering" to "agent orchestration" and sophisticated model evaluation

4 Cost

"Reasoning" models are computationally expensive, resulting in significantly higher inference costs at scale

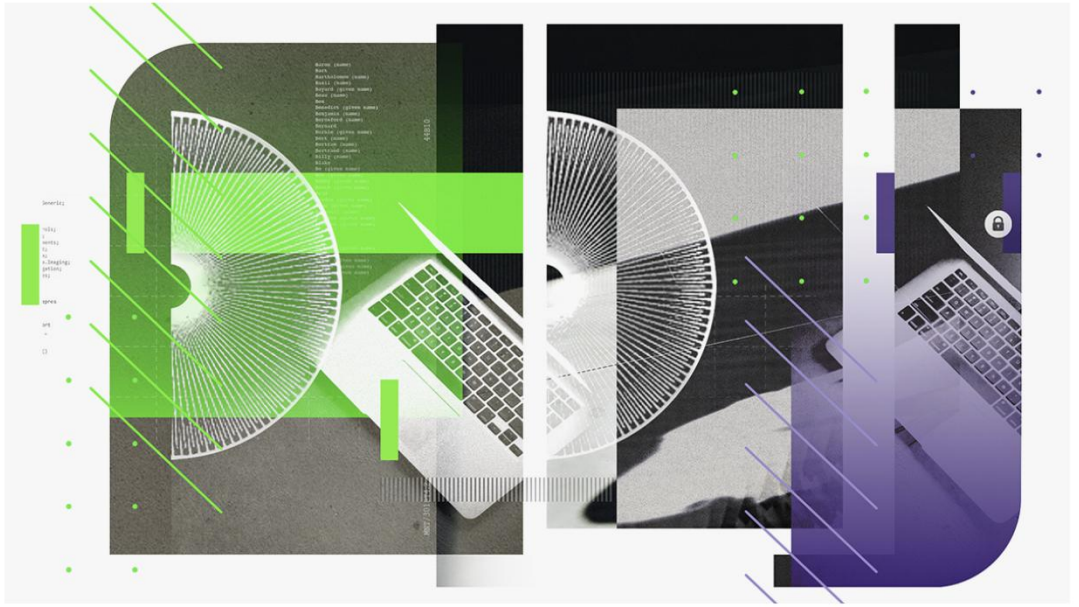
From Shadow IT to Shadow AI

Cybersecurity And Digital Privacy

The New Risks ChatGPT Poses to Cybersecurity

by Jim Chilton

April 21, 2023



Skizzomat

The 2026 AI Horizon: The Four Megatrends to Watch

Strategic Implications of the Shift from Content Generation to Autonomous Action

Megatrend 1: From Gen AI to Agentic AI

Megatrend 2: The Rise of "Reasoning" Models (System II)

Megatrend 3: AI Sovereignty & The Data Wall/Control

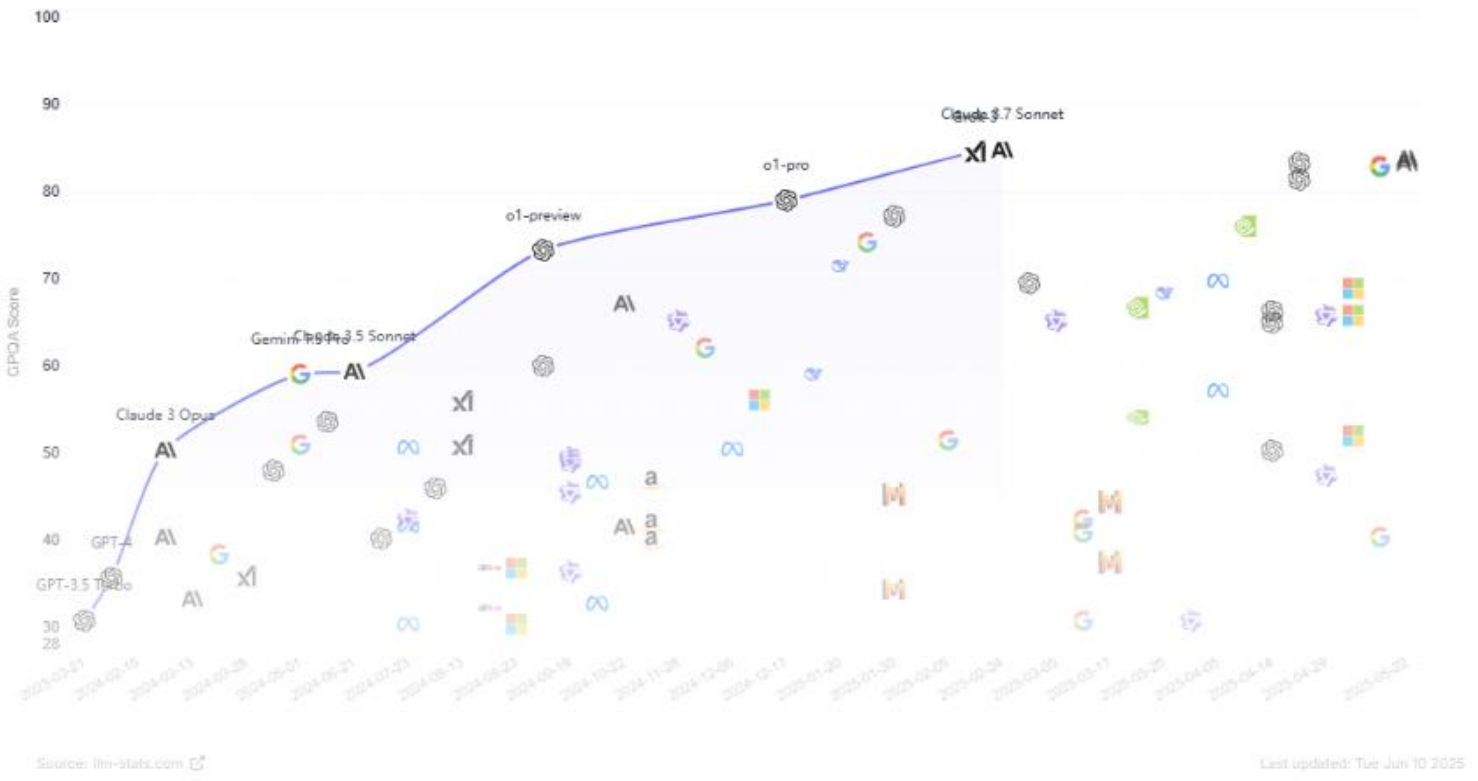
Megatrend 4: The Future of AGI

Issues Regarding AI Usage in An Organization

AI Developers Are Now Relentlessly Competing

Explosion of Generative AI Models

Comparative AI models across benchmarks, pricing, and capabilities.



- Organizations avoid vendor lock-in by using models from multiple providers
- High usage of LLMs leads to soaring costs, especially with enterprise-level subscriptions

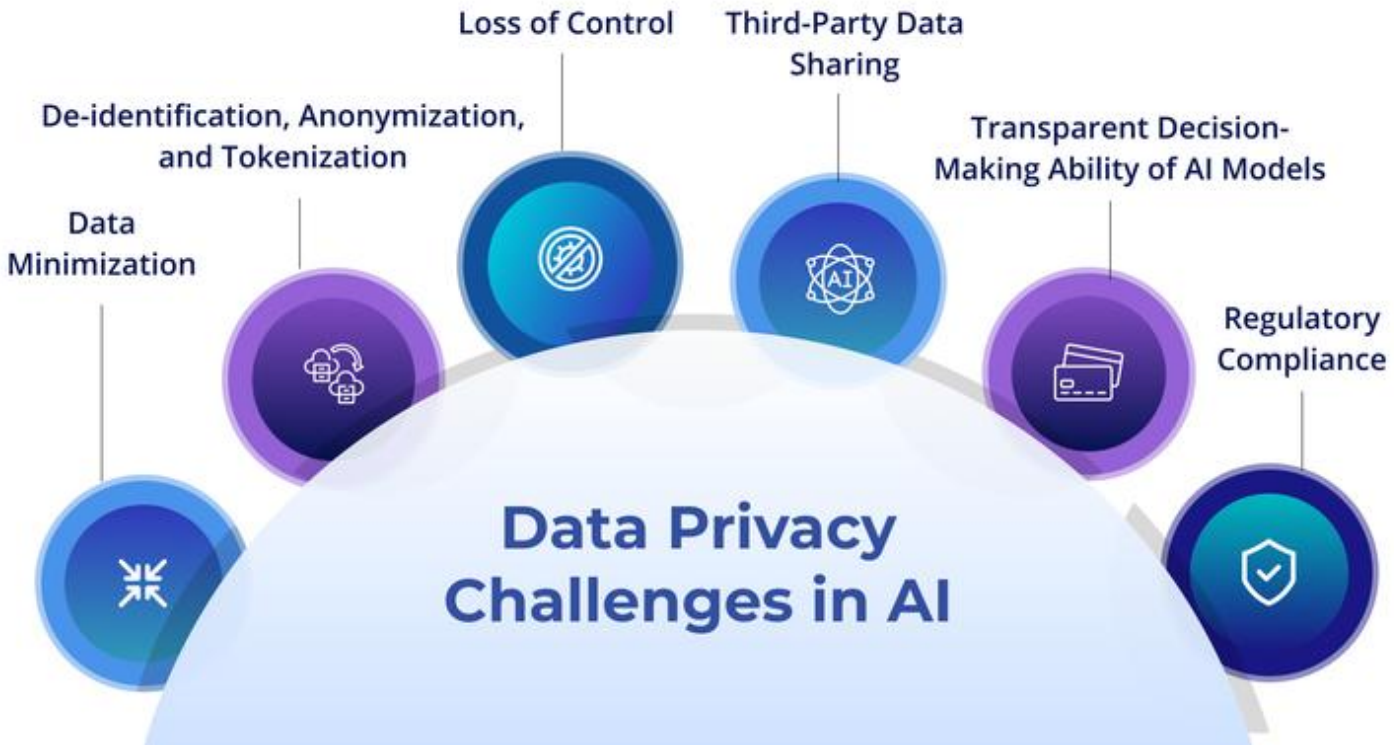
Many organizations start to

Explore optional models
Optimize the cost of GenAi usage

LLM Leaderboard 2025 - Verified AI Rankings

Ethics and Privacy Are Also Concerning

AI technologies frequently gather and process vast amounts of personal data, which raises significant concerns about privacy and security. To address these risks, it is essential to promote robust data protection regulations and enforce secure data management practices.

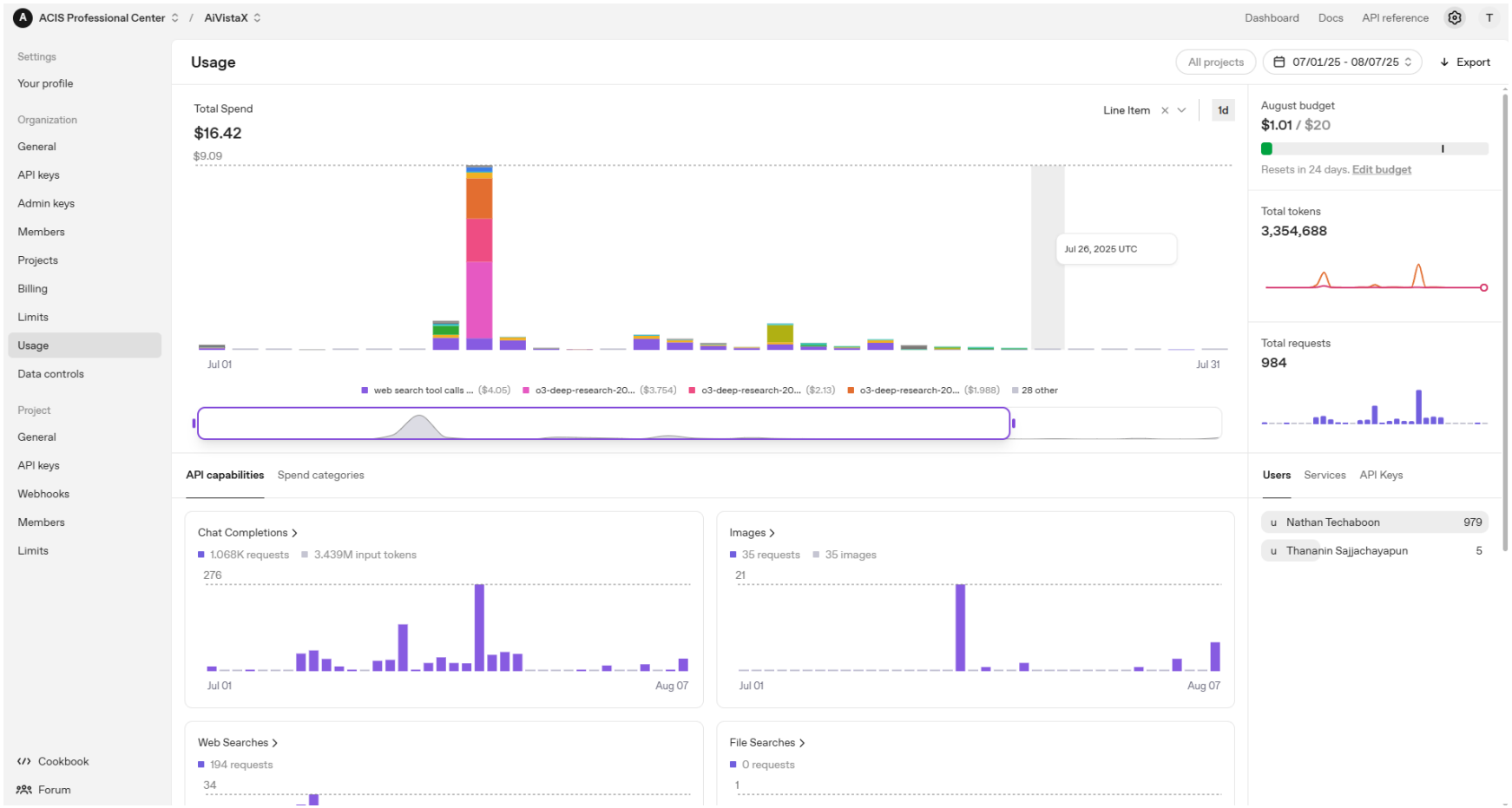


Overcome Data Privacy Challenges | Fortanix

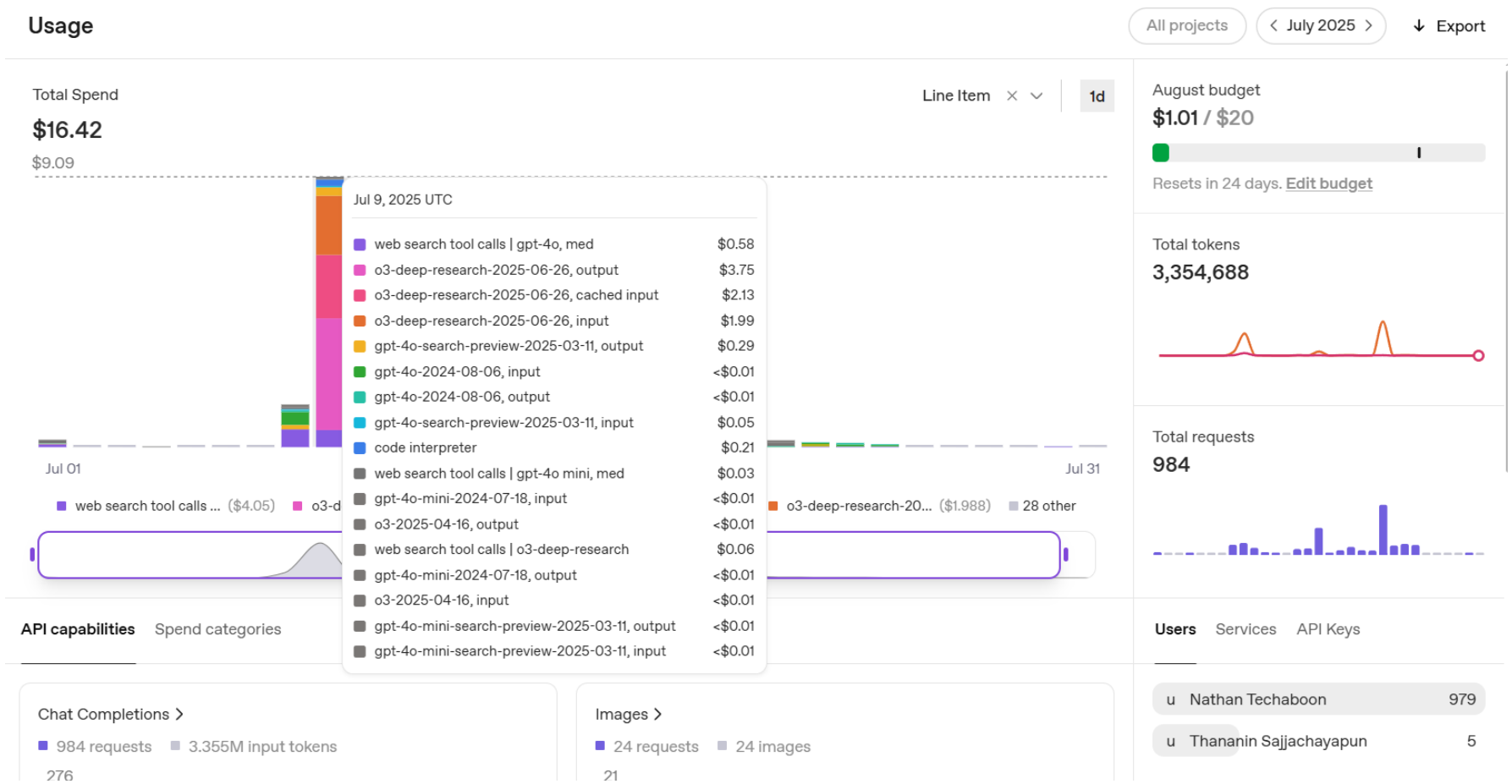
LLM API Dashboard
Usage and Cost Tracking

- OpenAI
- Anthropic
- Grok
- Gemini

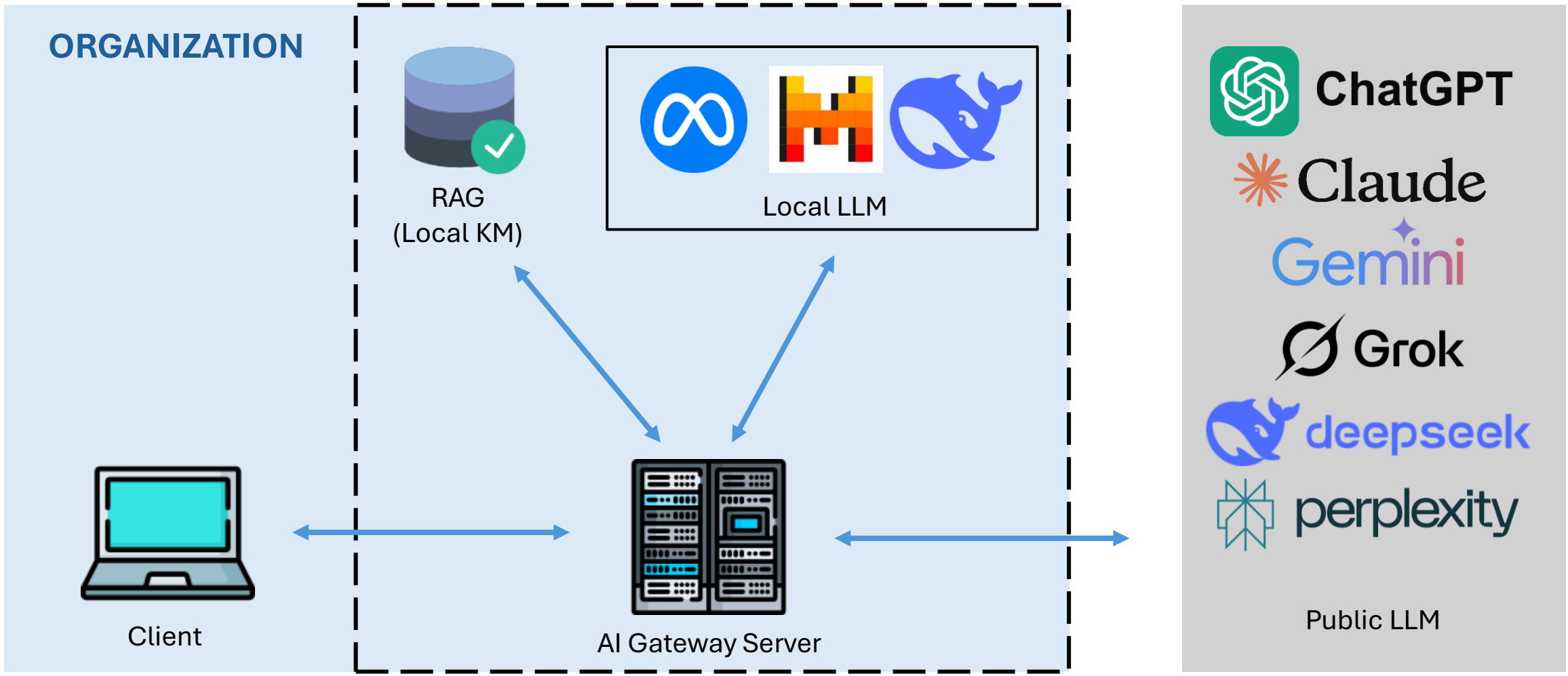
OpenAI Platform



OpenAI Platform



AI Gateway/AI Firewall : Shadow AI Migitation



Responsible AI & AI Governance

Responsible AI and AI Governance

Responsible AI:

This is the **set of principles, ethical considerations, and desired outcomes** for AI systems (fairness, transparency, safety, etc.). It's the *'what'* and *'why'* – what ethical standards should AI meet, and why are these important. It guides the *design and function* of AI.

AI Governance:

This is the **framework of rules, policies, standards, processes, roles, and controls** that an organization or society puts in place to *manage* and *direct* the development and use of AI. It's the *'how'* – how do we ensure AI systems adhere to responsible principles, comply with laws, and manage risks effectively. It provides the *structure and oversight*.

AI Governance

Why AI Governance

AI Governance is now essential

AI is no longer just a technology enabler. It is now recognized as both a **risk amplifier** (misinformation, cyber threats) and a **standalone systemic risk** (adverse outcomes, ethical breakdowns, societal disruption). This underscores the **critical need for AI governance** frameworks that are proactive, globally harmonized, and capable of managing both near-term threats and long-term structural consequences.

Ref. WEF Global Risk Report 2025

List of AI Related frameworks / standards / Laws active globally (as of October 2025)

OECD AI Principles (2019) • Promotes human-centric, fair, and accountable AI • Voluntary • Provides ethical principles baseline	**EU AI Act (2024)** • Regulates AI systems by risk level • Mandatory (EU law) • Sets legal compliance baseline for AI governance	**ISO/IEC 42001:2023 (AIMS)** • Establishes AI Management System (AIMS) • Certifiable (ISO standard) • Provides management system backbone for AI governance
NIST AI Risk Management Framework (2023) • Process to identify, manage, and communicate AI risks • Voluntary • Operationalizes risk-based AI governance	**Thai Personal Data Protection Act (TH-PDPA) - 2022** • Regulates collection and processing of PII • Mandatory law • Forms privacy and data ethics foundation	**Thailand AI Governance Guideline (TH-ETDA)** • National framework for responsible AI implementation • Voluntary guideline • Local adaptation of global AI governance principles
AI Security Guidelines (TH-NCSA) • Comprehensive Framework for AI Security • Focus on Ethical and Responsible Use • Operational Safeguards and Incident Response	**NIST Trustworthy & Responsible AI** • Defines trustworthiness dimensions and metrics • Voluntary • Links trust principles to governance criteria	**PMI Playbook for Data Science & AI** • Project management practices for AI initiatives • Voluntary guide • Integrates governance into AI project lifecycle
AI Data Security (NSA AISC) • Protects AI data/models from cyber threats • Voluntary best practice • Strengthens security and resilience pillar	**ISO/IEC 23894:2023 (AI Risk)** • Guidelines for managing AI-related risks • Voluntary guidance • Supports risk management pillar of AI governance	**Gartner AI Maturity Model** • Measures organizational AI capability maturity • Voluntary tool • Assesses governance and process maturity level
AI Literacy (ETDA) • Builds understanding of AI and its implications • Voluntary educational initiative • Supports awareness and accountability culture	**US Dept. of Energy – Responsible AI** • Responsible AI use in critical infrastructure • Voluntary agency guideline • Sector-specific implementation of AI governance	**ITU AI Governance Framework** • UN-led policy and standardization for AI • Voluntary international standard • Ensures global policy alignment and interoperability
Singapore Model AI Governance Framework • Practical guidance for responsible AI deployment • Voluntary national framework • Operational blueprint for ethical AI governance	**Malaysia Guidelines on AI Governance and Ethics** • Comprehensive Framework for AI Security • Founded on Seven Core Principles • Emphasizes Consumer Rights and Accountability	**UAE National AI Strategy 2031** • Ensure strong governance and effective regulation • Aims to make the UAE a global thought leader in AI governance

Workshop: AI Tools for the Modern Second Line (Cont.)

Key Drivers for AI Governance

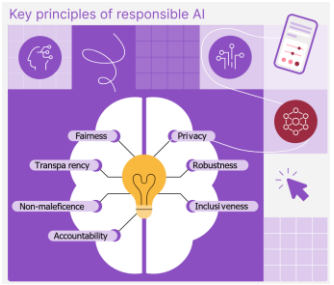
Key Drivers

1) Global Frameworks

1.1) NIST AI Risk Management

Leverage NIST's AI RMF to build a **risk-based governance process**. NIST RMF defines four core functions – **Govern, Map, Measure, Manage** – that will inform our approach

1.2) ISO/IEC 42001:2023

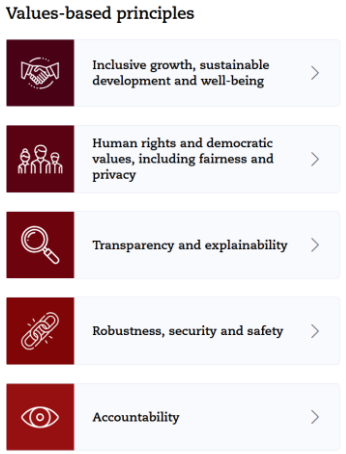


Structure Organization AI governance program as an **AI Management System (AIMS)** consistent with ISO 42001's guidance. This involves leadership commitment, risk-based planning, operational controls, and continuous improvement

1.3) EU AI Act

Draw on sector-specific and other international best practices. For example, the **EU AI Act's risk-based approach** (though not directly applicable yet) inspires our focus on **high-risk use cases**

1.4) OECD's AI principles



Adopt the OECD's **five value-based principles** to ensure **"innovative and trustworthy AI that respects human rights and democratic values."** These principles – 1) inclusive growth, 2) human-centered values (fairness, privacy), 3) transparency & explainability, 4) robustness & safety, and 5) accountability – will be woven into Organization AI policy and guidelines.

AI Governance Implementation

ACIS Professional Center Co., Ltd.

YOUR SATISFACTION IS OUR PRIDE

We have been certified to :

- ISO 22301:2019 "Business Continuity Management System" (BCMS)
- ISO/IEC 27001:2022 "Information Security Management System" (ISMS)
- ISO/IEC 27701:2019 "Privacy Information Management System" (PIMS)

The Imperative for Responsible AI

The Imperative for AI Governance

AI governance is defined as **a system of laws, policies, frameworks, practices, and processes** at international, national, and organizational levels **designed to help stakeholders implement, manage, oversee, and regulate the development, deployment, and use of AI technology.**

It is crucial for managing associated **risks**

To ensure...

- AI alignment with an organization's objectives
- Promotion of responsible and ethical AI usage
- Compliance with legal and regulatory requirements

- Businesses are racing to be the first in the marketplace, but this can result in the release of unethical, unresponsive and potentially malicious AI systems into the world
- We as humans configure these AI models, and our biases, morals and ethical values are mirrored in the AI systems we develop
- Human biases, morals and ethical values instilled in AI systems can affect AI decision-making that can have significant consequences for the data subject

Affected

- **Individuals** (civil rights, economic opportunity, safety)
- **Groups** (discrimination towards subgroups)
- **Society** (democratic process, public trust in governmental institutions, educational access, jobs redistribution)
- **Organizations** (reputational, cultural, economic, acceleration risks)
- **Ecosystems** (natural resources, environment, supply chain)

Key Risks & Attack Scenarios

IT infrastructure supporting AI systems shares the same vulnerabilities as traditional IT systems. AI systems are vulnerable to attacks throughout their lifecycle, from data collecting to inference. Three categories of AI-specific attacks are typically identified:

Poisoning

Altering training data or model parameters **to change AI system's response to all inputs** or to a specifically crafted input

Extraction

Reconstruction or recovery of confidential data such as model parameters, configuration or training data from the AI system or model **after the learning phase**

Evasion

Alteration of input data **to change the expected functioning of the AI system**.

The attacks could result in the malfunctioning of an AI system (availability or integrity risks)

Main risks scenarios involving an AI system

- Compromising AI hosting and management infrastructure
- Supply chain attack
- Lateralization via interconnections between AI systems and other systems
- Human and organisational failures
- Malfunction in AI system responses

Map with Enterprise Risk categories

1) Strategy, 2) Financial, 3) Compliance, 4) Operation

AI Governance Frameworks & Regulations

Grounding AI governance

The "why" and "how" of AI governance

Why	Principles	• OECD AI Principles • FIPs • UNESCO's Recommendation on the Ethics of Artificial Intelligence
How	Frameworks	• ISO (several standards) • NIST AI Risk Management Framework • IEEE 7000-21 • HUDERIA • Other standards specific to jurisdiction/industry

OECD AI Principles

The OECD AI Principles were initially adopted in 2029 and updated in May 2024. The Principles guide AI actors in their efforts to develop trustworthy AI and provide policymakers with recommendations for effective AI policies.

Values-based principles

Inclusive growth, sustainable development and well-being

This Principle highlights the potential for trustworthy AI to contribute to overall growth and prosperity for all – individuals, society, and planet – and advance global development objectives.

Human rights and democratic values, including fairness and privacy

Respect for the rule of law, human rights and democratic values, including fairness and privacy. AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and should include appropriate safeguards to ensure a fair and just society.

Transparency and explainability

This principle is about transparency and responsible disclosure around AI systems to ensure that people understand when they are engaging with them and can challenge outcomes.

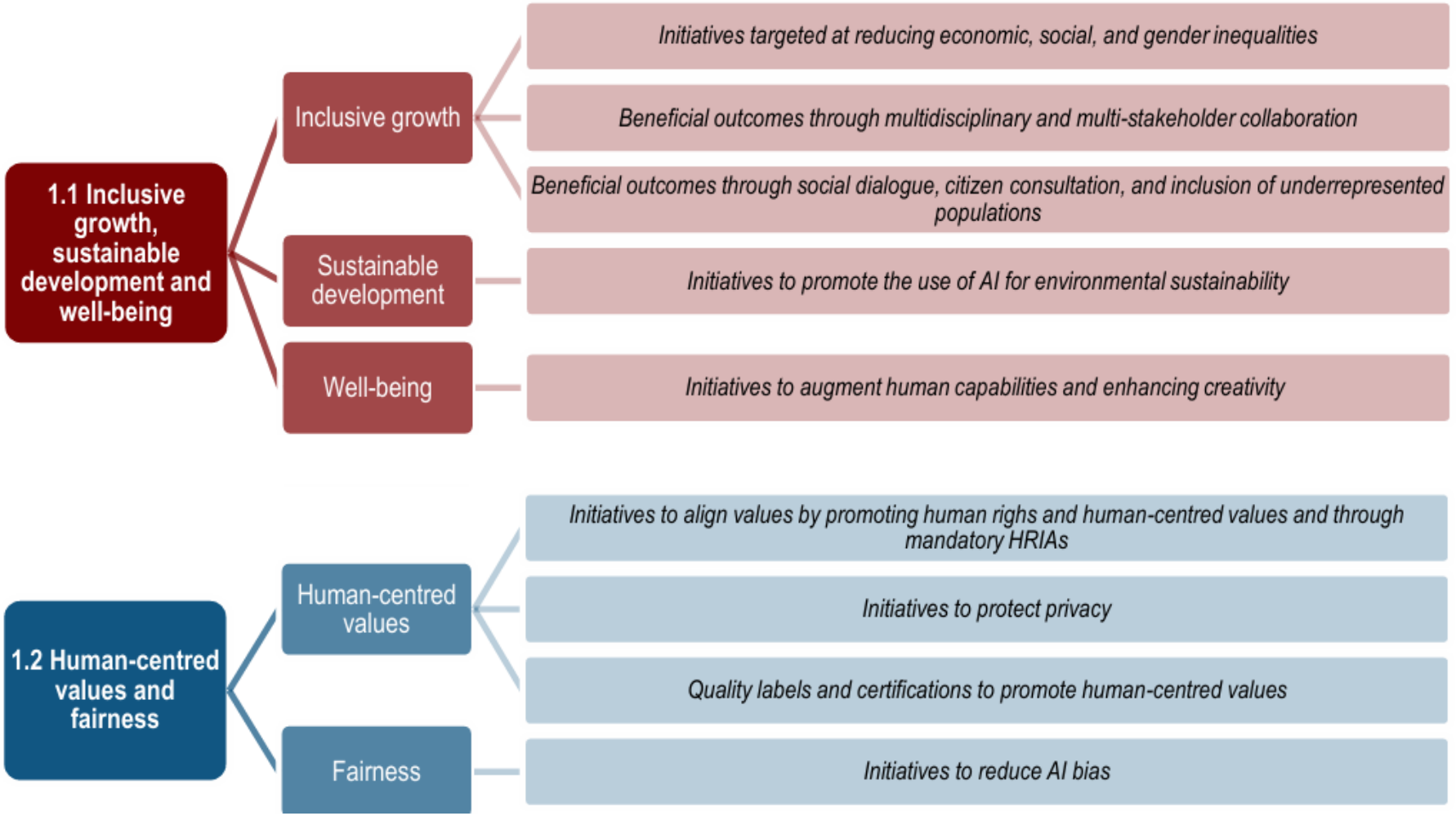
Robustness, security and safety

AI systems must function in a robust, secure and safe way throughout their lifetimes, and potential risks should be continually assessed and managed.

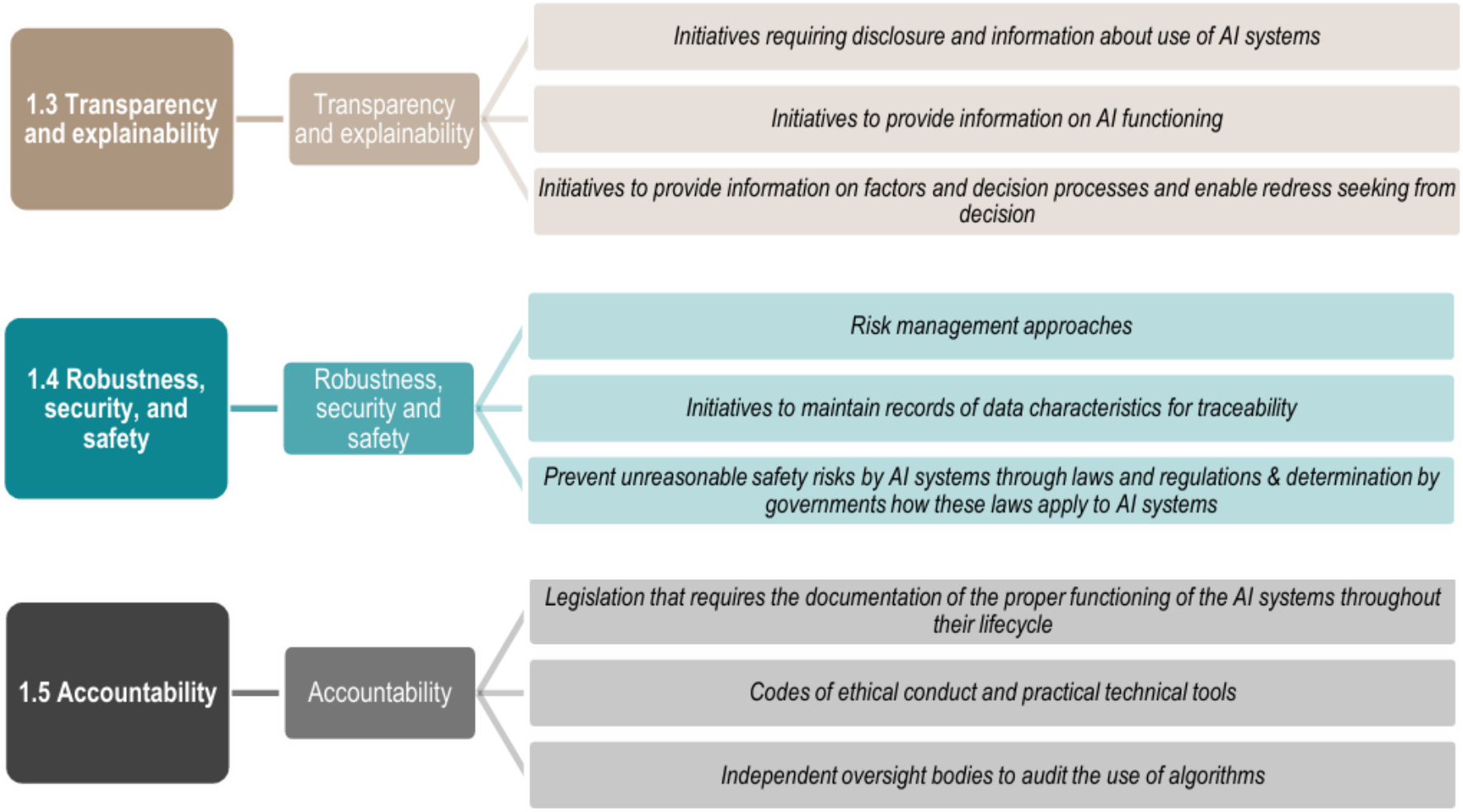
Accountability

Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the OECD's values-based principles for AI

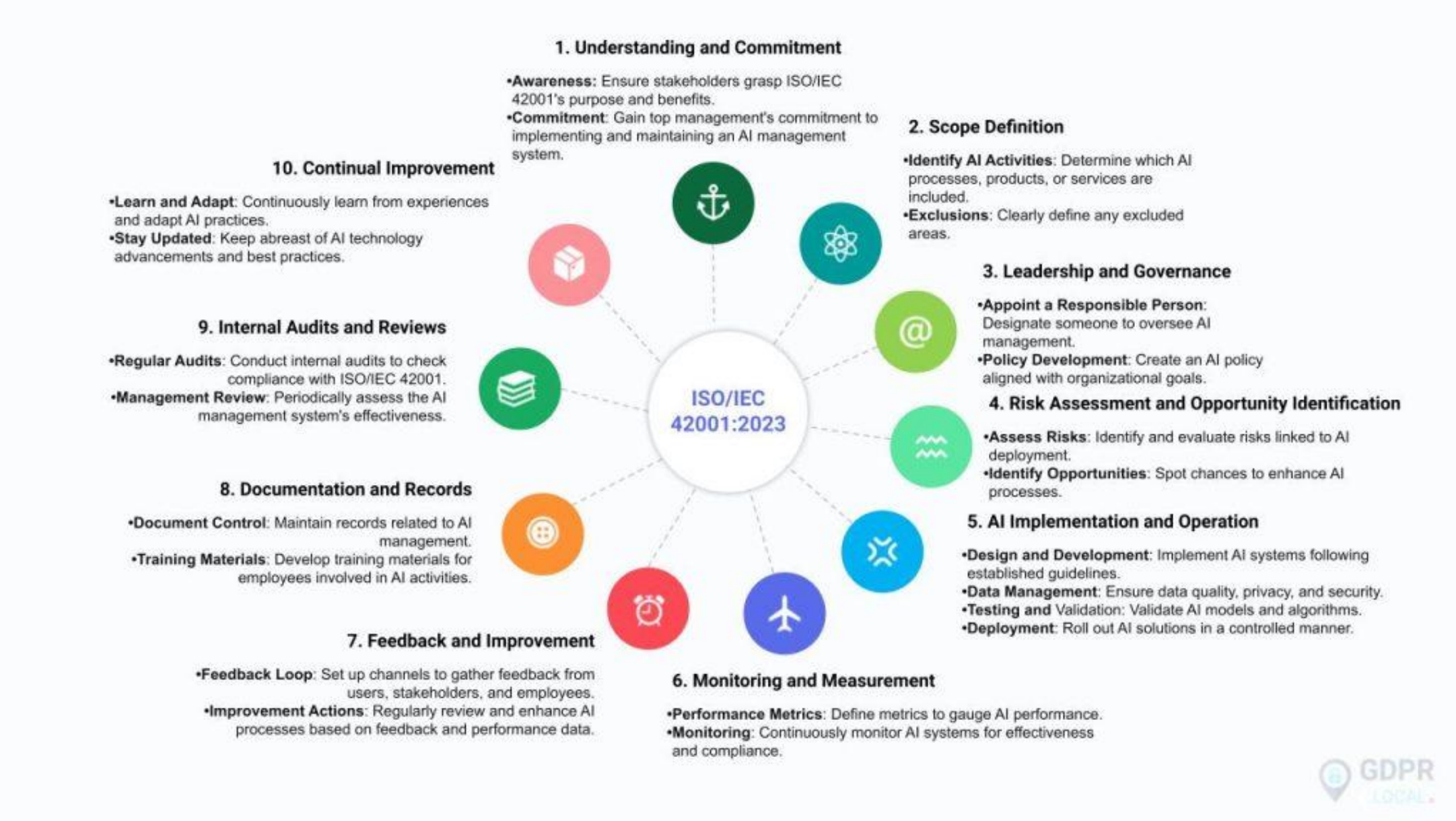
Overview OECD AI Principle



Overview OECD AI Principle



Overview ISO/IEC 42001:2023



ISO/IEC 42001:2023

ISO/IEC 42001

ISO/IEC 42001:2023

AI Management System

IT — Artificial intelligence — Management system

(Edition 1, 2023)

https://www.iso.org/standard/81230.html

Accredited certification

ISO/IEC 38507

ISO/IEC 38507:2022

AI Governance

Governance of IT — Governance implications of the use of artificial intelligence by organizations

(Edition 1, 2022)

https://www.iso.org/standard/56641.html

ISO/IEC 5259-1:2024
Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology, and examples

ISO/IEC 5259-2:2024
Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures

ISO/IEC 5259-3:2024
Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines

ISO/IEC 5259-4:2024
Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 4: Data quality process framework

ISO/IEC 5338:2023
Information technology — Artificial intelligence — AI system life cycle processes

ISO/IEC 8183:2023
Information technology — **Artificial intelligence** — Data life cycle framework

ISO/IEC 23053:2022
Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)

ISO/IEC TR 24029-1:2021
Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview

ISO/IEC CD 27090
Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems

ISO/IEC 22989

ISO/IEC 22989:2022

AI Concepts

IT — Artificial intelligence concepts and terminology

(Edition 1, 2022)

https://www.iso.org/standard/74296.html

ISO/IEC 23894

ISO/IEC 23894:2023

AI Risk Management

IT — AI — Guidance on risk management

(Edition 1, 2023)

https://www.iso.org/standard/77304.html

ISO/IEC TR 24368

ISO/IEC TR 24368:2022

AI Guides

IT — AI — Overview of ethical and societal concerns

(Edition 1, 2022)

https://www.iso.org/standard/78507.html

ISO/IEC FDIS 42005

ISO/IEC FDIS 42005

AI Impact Assessment

IT — AI — AI system impact assessment

(FDIS, 2024)

https://www.iso.org/standard/44545.html

ISO/IEC 42001:2023

Clause 4
Context of the Organization
บริบทองค์กร

- 4.1 Understanding the organization and its context
  - ความเข้าใจองค์กรและบริบทขององค์กร
- 4.2 Understanding the needs and expectations of interested parties
  - ความเข้าใจข้อกำหนดและความคาดหวังของผู้มีส่วนได้เสีย
- 4.3 Determining the scope of the AI management system
  - การกำหนดขอบเขตระบบบริหารจัดการAI
- 4.4 AI management system
  - ระบบบริหารจัดการ AI

Clause 5
Leadership
ภาวะผู้นำ

- 5.1 Leadership and commitment
  - ภาวะผู้นำและพันธสัญญา
- 5.2 AI Policy
  - นโยบาย AI
- 5.3 Roles, responsibilities and authorities
  - บทบาท ความรับผิดชอบ และอำนาจหน้าที่

Clause 6
Planning
การวางแผน

- 6.1 Actions to address risks and opportunities
  - การพิจารณาความเสี่ยงและโอกาส
- 6.1.1 General [risk methodology]
  - บททั่วไป
- 6.1.2 AI risk assessment
  - การประเมินความเสี่ยงของ AI
- 6.1.3 AI risk treatment
  - การจัดการความเสี่ยงจาก AI
- 6.2 AI objectives and planning to achieve them
  - วัตถุประสงค์ของ AI และการวางแผนเพื่อให้บรรลุผลดังกล่าว
- 6.3 Planning of changes
  - การวางแผนเปลี่ยนแปลง

Clause 7
Support
การสนับสนุน

- 7.1 Resources
  - ทรัพยากร
- 7.2 Competence
  - ความสามารถ
- 7.3 Awareness
  - การสร้างความตระหนัก
- 7.4 Communication
  - การสื่อสาร
- 7.5 Documented Information
  - เอกสารสารสนเทศ
- 7.5.1 General
  - บททั่วไป
- 7.5.2 Creating and updating documented information
  - การจัดสร้างและการปรับปรุงข้อมูลเอกสารให้เป็นปัจจุบัน
- 7.5.3 Control of documented information
  - การควบคุมเอกสารสารสนเทศ

Clause 8
Operation
การดำเนินการ

- 8.1 Operational planning and control
  - การวางแผนและการควบคุมการดำเนินการ
- 8.2 AI risk assessment
  - การประเมินความเสี่ยงของ AI
- 8.3 AI risk treatment
  - การจัดการความเสี่ยงจาก AI

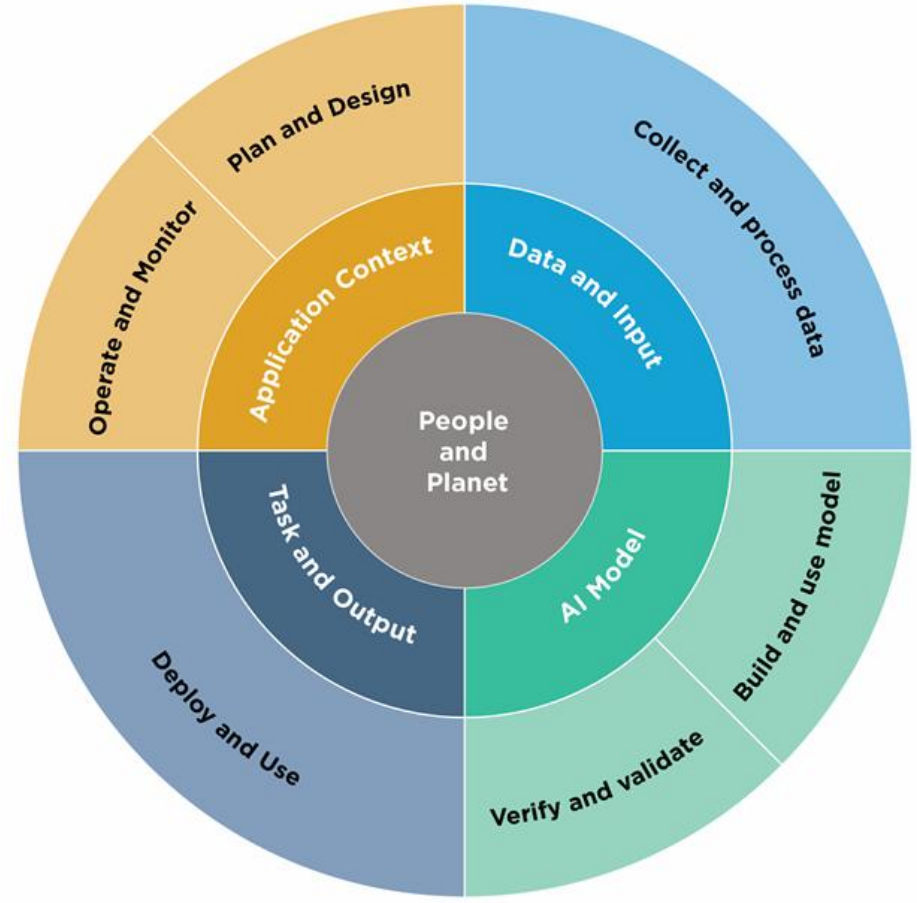
Clause 9
Performance Evaluation
การประเมินผล

- 9.1 Monitoring, measurement, analysis and evaluation
  - การติดตามผล วัดผล วิเคราะห์ผล และประเมินผล
- 9.2 Internal audit
  - การตรวจสอบภายใน
- 9.2.1 General
  - บททั่วไป
- 9.2.2 Internal audit programme
  - แผนตรวจสอบภายใน
- 9.3 Management review
  - การทบทวนโดยฝ่ายบริหาร
- 9.3.1 General
  - บททั่วไป
- 9.3.2 Management review inputs
  - ข้อมูลปัจจัยนำเข้าสำหรับการทบทวนโดยฝ่ายบริหาร
- 9.3.3 Management review results
  - ผลของการทบทวนโดยฝ่ายบริหาร

Clause 10
Improvement
การปรับปรุง

- 10.1 Continual improvement
  - การปรับปรุงอย่างต่อเนื่อง
- 10.2 Nonconformity and corrective action
  - ความไม่สอดคล้องและการปรับปรุงแก้ไข

Overview NIST AI Risk Management Framework



Lifecycle and Key Dimensions of an AI System

AI risk management offers a path to *minimize potential negative impacts of AI systems*, such as threats to civil liberties and rights, while also providing opportunities to *maximize positive impacts*. Addressing, documenting, and managing **AI risks** and potential negative impacts effectively can lead to more trustworthy AI systems.

NIST AI RMF: Characteristics of trustworthy AI systems

Creating **trustworthy AI** requires balancing each of these characteristics based on the AI system's context of use.

Addressing AI trustworthiness characteristics individually will not ensure AI system trustworthiness; trade-offs are usually involved, rarely do all characteristics apply in every setting, and some will be more or less important in any given situation.

NIST AI Risk Management

AI risk management offers a path to minimize potential negative impacts of AI systems, such as threats to civil liberties and rights, while also providing opportunities to maximize positive impacts. Addressing, documenting, and managing AI risks and potential negative impacts effectively can lead to more trustworthy AI systems.

The AI RMF Core provides outcomes and actions that enable dialogue, understanding, and activities to manage AI risks and responsibly develop trustworthy AI systems. The Core is composed of four functions: GOVERN, MAP, MEASURE, and MANAGE. Each of these high-level functions is broken down into categories and sub-categories.

Effectiveness of the AI RMF

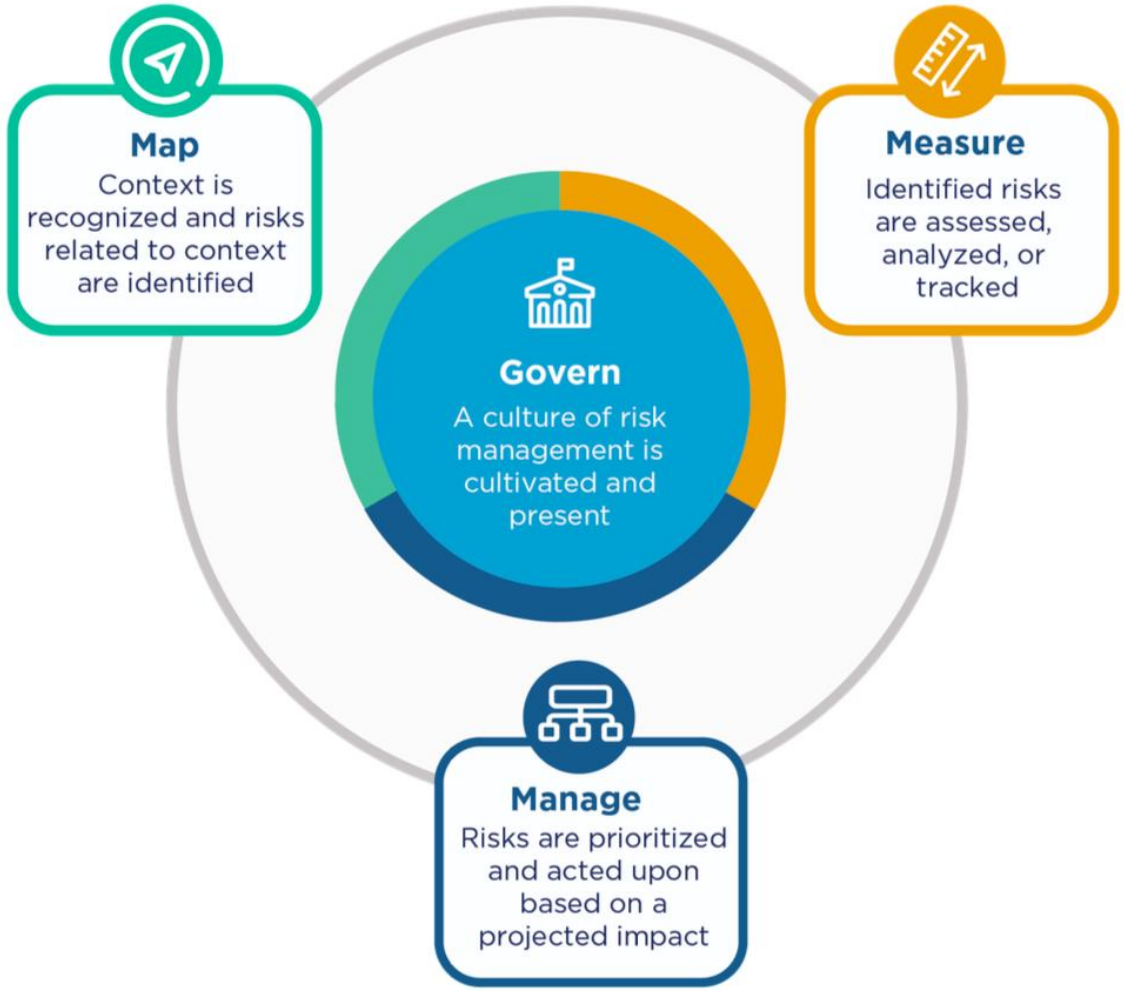
- Enhanced processes for governing, mapping, measuring, and managing AI risk, and clearly documenting outcomes
- Improved awareness of the relationships and tradeoffs among trustworthiness characteristics, socio-technical approaches, and AI risks
- Explicit processes for making go/no-go system commissioning and deployment decisions;
- Established policies, processes, practices, and procedures for improving organizational accountability efforts related to AI system risks
- Enhanced organizational culture which prioritizes the identification and management of AI system risks and potential impacts to individuals, communities, organizations, and society;
- Better information sharing within and across organizations about risks, decision-making processes, responsibilities, common pitfalls, TEVV practices, and approaches for continuous improvement
- Greater contextual knowledge for increased awareness of downstream risks
- Strengthened engagement with interested parties and relevant AI actors
- Augmented capacity for TEVV of AI systems and associated risks

Overview NIST AI Risk Management Framework

The **AI RMF Core** provides outcomes and actions that enable dialogue, understanding, and activities to manage AI risks and responsibly develop trustworthy AI systems.

The Core is composed of four functions: **GOVERN, MAP, MEASURE,** and **MANAGE**.

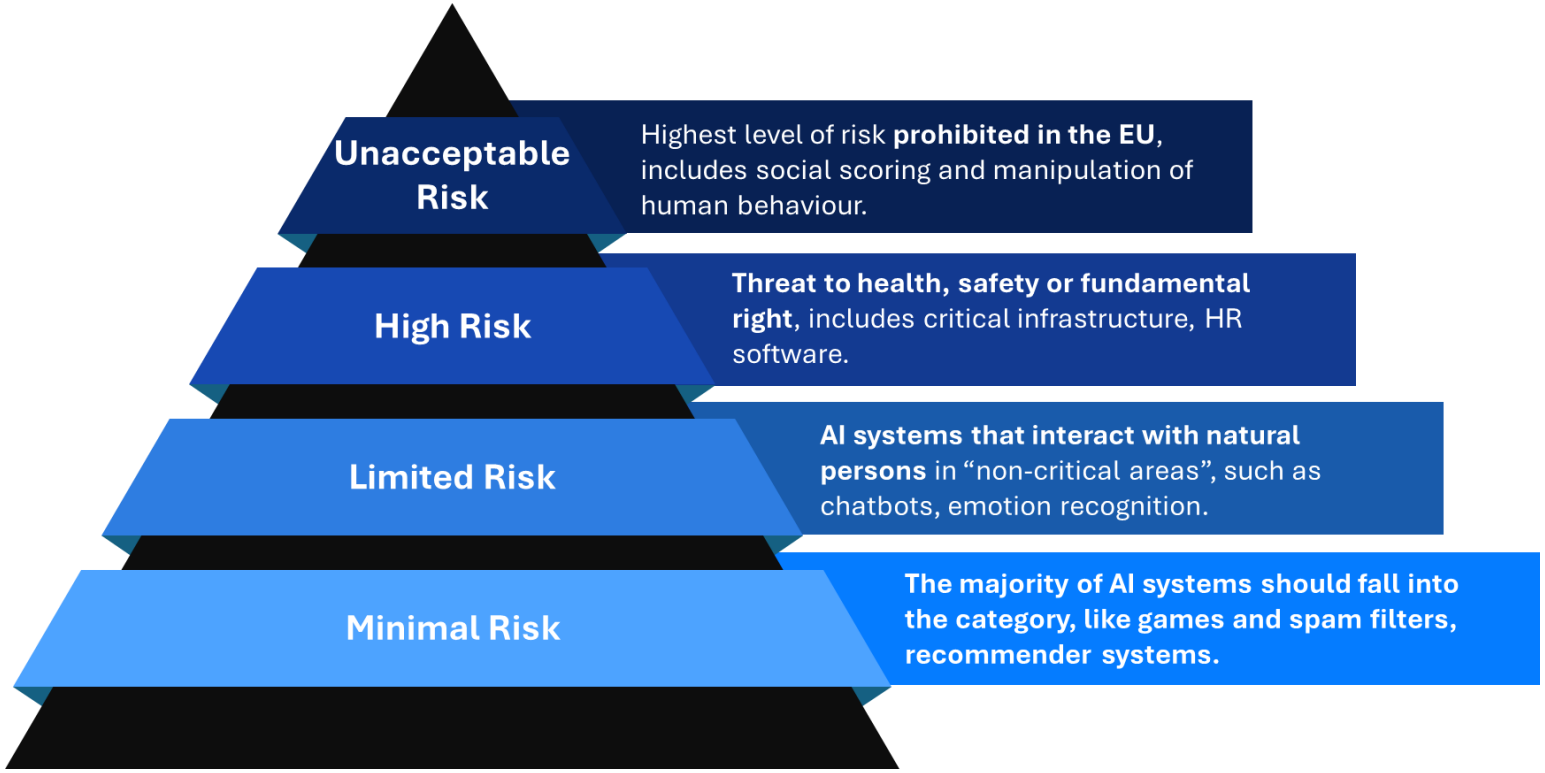
Govern: establishing clear oversight, accountability, and ethical policies
Map: Contextualizing risks and benefits
Measure: Tracking, testing, and assessing risks
Manage: Prioritizing and acting on identified risks



Overview EU AI Act

Under the AI Act, the **European Artificial Intelligence Board** (comprising member state and Commission representatives) supervises AI use. It **monitors, advises on, and can regulate** AI applications to ensure consistent enforcement and uphold human rights throughout the EU

Under the AI Act, AI systems are categorized into **four risk levels**, with corresponding regulatory requirements tailored to each level of risk.



Penalties:

- **Prohibited AI Practices**: Utilizing or placing on the market AI systems that are banned under the Act can result in fines up to €35 million or 7% of the company's total worldwide annual turnover, whichever is higher.
- **Other AI Practices**: Failing to meet obligations related to high-risk AI systems may lead to fines up to €15 million or 3% of the total worldwide annual turnover, whichever is higher.
- **Other Non-Compliance**: Providing incorrect information or other forms of non-compliance can incur fines up to €7.5 million or 1.5% of the total worldwide annual turnover, whichever is higher.

EU AI Act

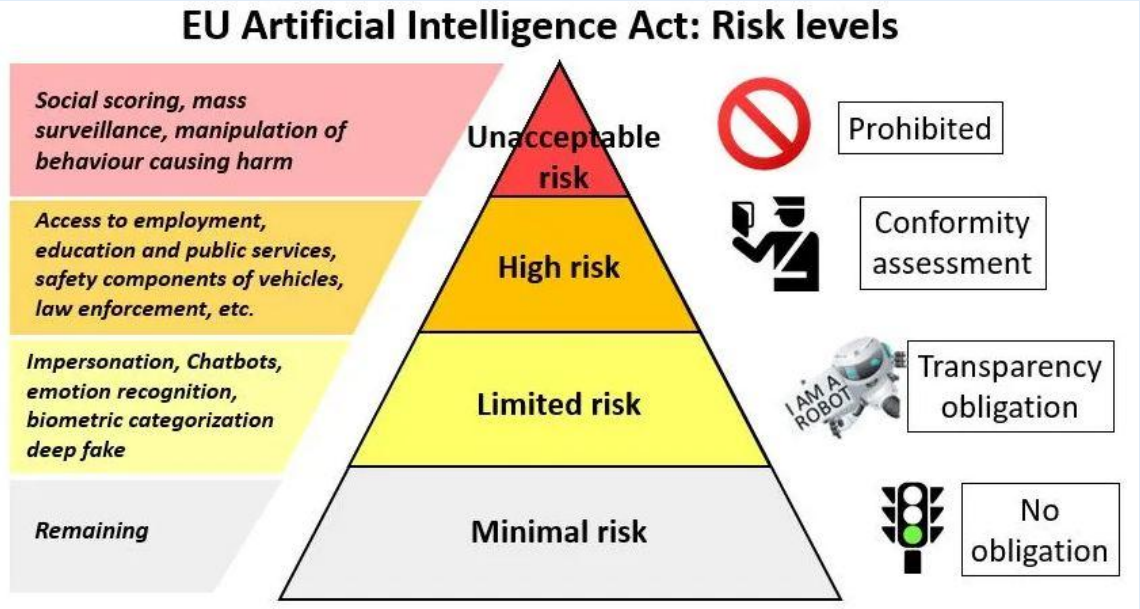
AI Act ให้อำนาจการกำกับดูแลการใช้งาน AI แก่คณะกรรมการ European Artificial Intelligence Board ซึ่งประกอบด้วยตัวแทนจากประเทศสมาชิกสหภาพยุโรปและคณะกรรมาธิการยุโรป ทำหน้าที่ตรวจสอบและให้คำแนะนำเกี่ยวกับการใช้งาน AI รวมถึงให้อำนาจในการกำหนดข้อบังคับและมาตรการควบคุมสำหรับ AI เพื่อให้การใช้บังคับ AI Act เป็นไปอย่างมีประสิทธิภาพในทุกประเทศสมาชิก และไม่ละเมิดสิทธิมนุษยชนของประชาชน

Penalties

- **Prohibited AI Practices**: Utilizing or placing on the market AI systems that are banned under the Act can result in fines up to €35 million or 7% of the company's total worldwide annual turnover, whichever is higher.
- **Other AI Practices**: Failing to meet obligations related to high-risk AI systems may lead to fines up to €15 million or 3% of the total worldwide annual turnover, whichever is higher.
- **Other Non-Compliance**: Providing incorrect information or other forms of non-compliance can incur fines up to €7.5 million or 1.5% of the total worldwide annual turnover, whichever is higher.

ภายใต้ AI Act มีการแบ่งประเภท AI ตามระดับความเสี่ยงและกำหนดข้อบังคับที่เหมาะสมสำหรับแต่ละระดับความเสี่ยง 4 ระดับ ได้แก่

1) AI ที่มีความเสี่ยงระดับที่ยอมรับไม่ได้ (Unacceptable risk)
2) AI ที่มีความเสี่ยงสูง (High risk)
3) AI ที่มีความเสี่ยงจำกัด (Limited risk)
4) AI ที่มีความเสี่ยงน้อยที่สุด (Minimal risk)



Draft Thailand's AI Act

As of 2025, **two** draft legislations have been introduced in Thailand.

1. The Draft Royal Decree on Business Operations that Use Artificial Intelligence System ("Draft Decree") – พระราชกฤษฎีกา (พรฎ)

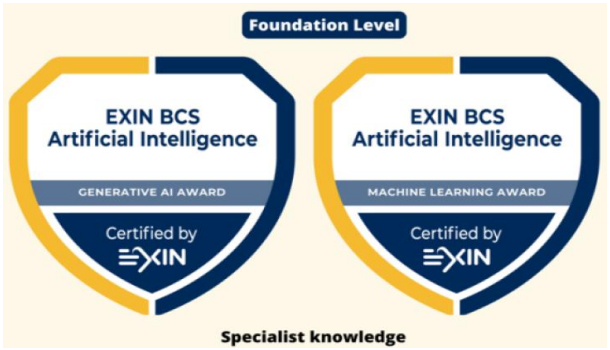
- In October 2022, **the Office of the National Digital Economy and Society Commission (ONDE)** สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) introduced the Draft Decree.
- It will be enacted by virtue of the Electronic Transaction Act B.E. 2544 (2001) ("ETA")
- It was created on a risk-based approach like the EU Proposal on AI Act. The **obligations for providing AI systems** will be stricter as the risk increases.
- The Draft Decree **only regulates AI systems within the reach of the general consumer** and does not extend to those undergoing research and development.
- The Draft Decree also contains **extraterritorial applicability** to service providers located outside of Thailand, which requires service registration with the regulator and the appointment of a local point of contact.
- Liabilities include an administrative order and criminal punishment.

2. The Draft Act on the Promotion and Support of AI Innovations in Thailand ("Draft Act") – พระราชบัญญัติ (พรบ)

- The Draft Act was first introduced by **the Electronic Transactions Development Committee of the Electronic Transactions Development Agency (ETDA)** in March 2023.
- It provides mechanisms and legal instruments to **help the development of AI in the country**, along with provisions **to protect consumers** from AI services.
- Enacted as a separate piece of legislation and would not be based on the ETA.
- There is currently no specific sanction outlined in this Draft Act, except when an AI service provider does not act according to its advertisement relating to the quality of service (consumer protection).

Related certifications related to AI Governance Services

AI Governance Training and Certification Courses



AI Governance in the Real World

AI Governance: Monitoring & Observability

- Gain full visibility into AI service usage and performance.
- Ensuring that AI services are reliable, efficient, secure, and cost-effective.

Request & Response Logging	Track all prompts, responses, and user activity for auditing and debugging.
Performance Monitoring	Measure latency, throughput, and error rates of AI model calls.
Cost & Token Usage Tracking	Monitor token consumption and associated costs per model, user, or app.
End-to-End Tracing (e.g., RAG Workflows)	Visualize the full path of complex AI operations across multiple services.
Anomaly Detection & Alerts	Trigger notifications for unusual activity, errors, or cost spikes.
Governance & Compliance Reporting	Provide logs and metrics for audits, security reviews, or policy enforcement.
Usage Dashboards & Visualization	Present historical trends for performance and usage.

AI Governance in the Real World

Role-Based Access Control and User management

To ensure secure, policy-aligned usage of AI services by managing who can access which models, features, or data based on user roles and permissions.

Roles	Description	Model Access	Permissions
Admin	Manages the AI Gateway and user access	All public & private models	• Manage users & roles • Configure routing & policies • View all logs- Set usage limits
Team Lead	Oversees team-level AI usage	Approved LLMs (public/private)	• Approve user access • Set team quotas • View team usage reports
Developer	Builds applications using AI APIs	Public models + sandboxed local	• Call APIs • Access dev tools • View logs for debugging
Data Analyst	Uses AI to query reports or documents	Approved LLMs with local data	• Submit prompts • View results • Limited editing of prompt templates

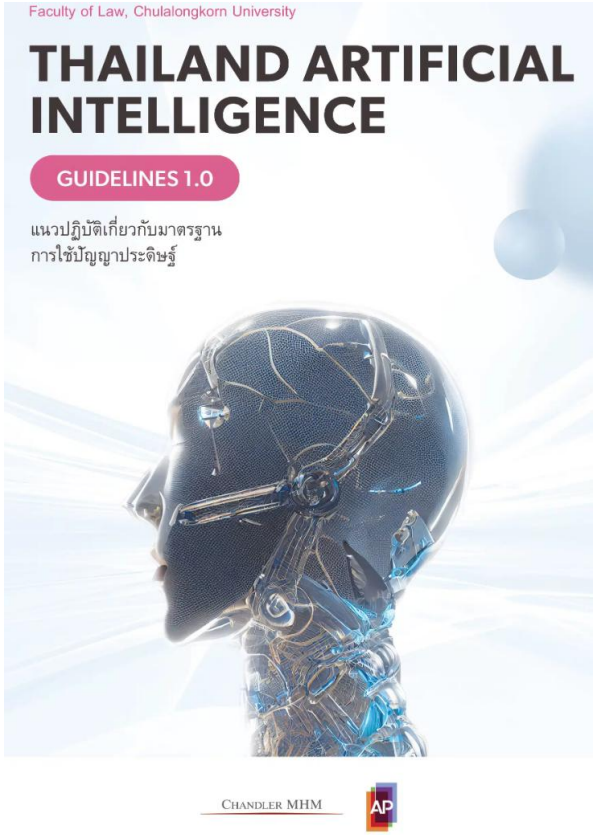
Establishing AI Governance

AI Governance Frameworks & Regulations

2) Thai Regulatory Context

2.1) Thai Personal Data Protection Act (PDPA)
2.2) Thailand AI ethics guidelines (ETDA & TAIG)
2.3) Thailand Artificial Intelligence Guideline 1.0

} Align with any emerging Thai guidelines (such as the NCSA's forthcoming AI security guidelines focusing on AI alignment with cybersecurity and PDPA).



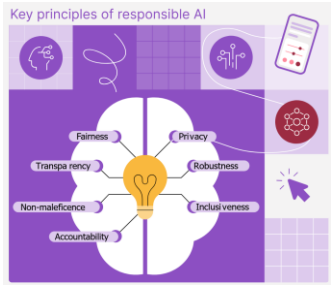
AI Governance Frameworks & Regulations

1) Global Frameworks

1.1) NIST AI risk management

Leverage NIST's AI RMF to build a **risk-based governance process**. NIST RMF defines four core functions – **Govern, Map, Measure, Manage** – that will inform our approach

1.2) ISO/IEC 42001:2023

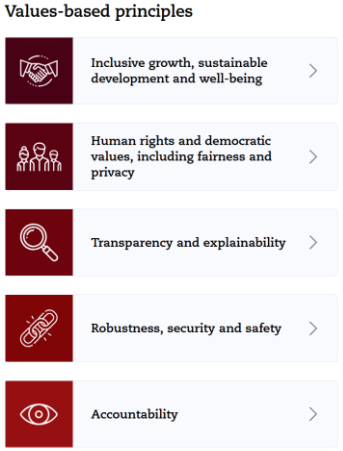


Structure AI governance program as an **AI Management System (AIMS)** consistent with ISO 42001's guidance. This involves leadership commitment, risk-based planning, operational controls, and continuous improvement

1.3) EU AI Act

Draw on sector-specific and other international best practices. For example, the **EU AI Act's risk-based approach** (though not directly applicable yet) inspires our focus on **high-risk use cases**

1.4) OECD's AI principles



Adopt the OECD's **five value-based principles** to ensure **"innovative and trustworthy AI that respects human rights and democratic values."** These principles – 1) inclusive growth, 2) human-centered values (fairness, privacy), 3) transparency & explainability, 4) robustness & safety, and 5) accountability – will be woven into Enterprise AI policy and guidelines.

22 Key Elements/Contents in AI Governance implementation

1. Trustworthy and responsible AI awareness for top management
2. Trustworthy and responsible AI awareness for user
3. AIMS Context of the organization
4. AIMS objectives
5. AI governance committee & charter
6. AI related roles and responsibility
7. Trustworthy and responsible AI policy
8. Acceptable use of AI policy
9. AI risk management procedure
10. AI system/project impact assessment procedure
11. Effectiveness and efficiency measurement procedure
12. Information for interested parties of AI systems management procedure
13. Resources for AI systems/projects management procedure
14. AI system third-party and customer relationships management procedure
15. AI system development lifecycle management procedure
16. AI data governance procedure
17. Compliance metrics and monitoring checklist
18. AI risk assessment report
19. AI risk treatment plan
20. AI project compliance check & impact assessment report
21. AIMS Internal Audit Report *(Option for AIMS: ISO/IEC 42001 Certification)*
22. AIMS Management Review Presentations *(Optional for AIMS: ISO/IEC 42001 Certification)*

ISO/IEC 42001:2023
AI Management System (AIMS)

Date: 27 January 2026

ACIS Professional Center Co., Ltd.

YOUR SATISFACTION IS OUR PRIDE

We have been certified to :

ISO 22301:2019	“Business Continuity Management System” (BCMS)
ISO/IEC 27001:2022	“Information Security Management System” (ISMS)
ISO/IEC 27701:2019	“Privacy Information Management System” (PIMS)
ISO/IEC 42001:2023	“Artificial Intelligence Management System” (AIMS)

AI Governance Frameworks

AI Governance References

Frameworks	Standards/Management Systems	Regulations	Guidelines/Playbooks
OECD's AI Principles Provide a global ethical standard for designing and operating trustworthy AI systems that are human-centric, fair, and accountable	**ISO/IEC 42001:2023 (AI Management System-AIMS)** Provides a certifiable framework for organizations to establish, implement, and continually improve a structured AI Management System	**Thai Personal Data Protection Act 2019** Governs the collection, use, and disclosure of personal data, setting rules for data controllers and processors to protect individuals' privacy rights	**Thailand AI Governance Guideline (ETDA)** Provides a framework and recommendations for organizations to implement responsible and ethical AI governance
NIST Trustworthy and Responsible AI Defines the key characteristics of trustworthy AI, such as accuracy, reliability, fairness, and transparency, to guide its responsible development	**ISO/IEC 38507:2022 (IT Governance – Implication of AI Usage)** A board-level AI governance standard. It defines what governing bodies should oversee and decide about AI	**EU AI Act** A comprehensive regulatory framework for AI, categorizing and governing systems based on their potential risk to health, safety, and fundamental rights	**AI Security Guidelines (NCSA)** Provide practical guidance for securely and responsibly designing, deploying, and governing AI systems across their lifecycle, aligned with international standards and Thai cybersecurity and data protection laws
NIST AI Risk Management Framework (AI RMF) Provides a structured, four-step process for organizations to better understand, manage, and communicate AI risks	**ISO/IEC FDIS 42005 (AI Impact Assessment)** A practical, risk-based guidance for AI impact assessment. It provides the risk and impact intelligence that boards, executives, and regulators expect before AI systems are approved or scaled		**Playbook for Project Management in Data Science and AI Projects (Project Management Institute-PMI)** Offers practical guidance and a structured framework tailored to the unique challenges of managing AI and data science projects
Gartner AI Maturity Model Helps organizations assess their current AI capabilities and provides a roadmap to advance through different stages of AI maturity	**ISO/IEC 23894:2023 (AI Risk Management)** Offers specific guidance on the principles and processes for managing risks associated with artificial intelligence systems		

ACIS AI Governance Frameworks

AI Governance Framework

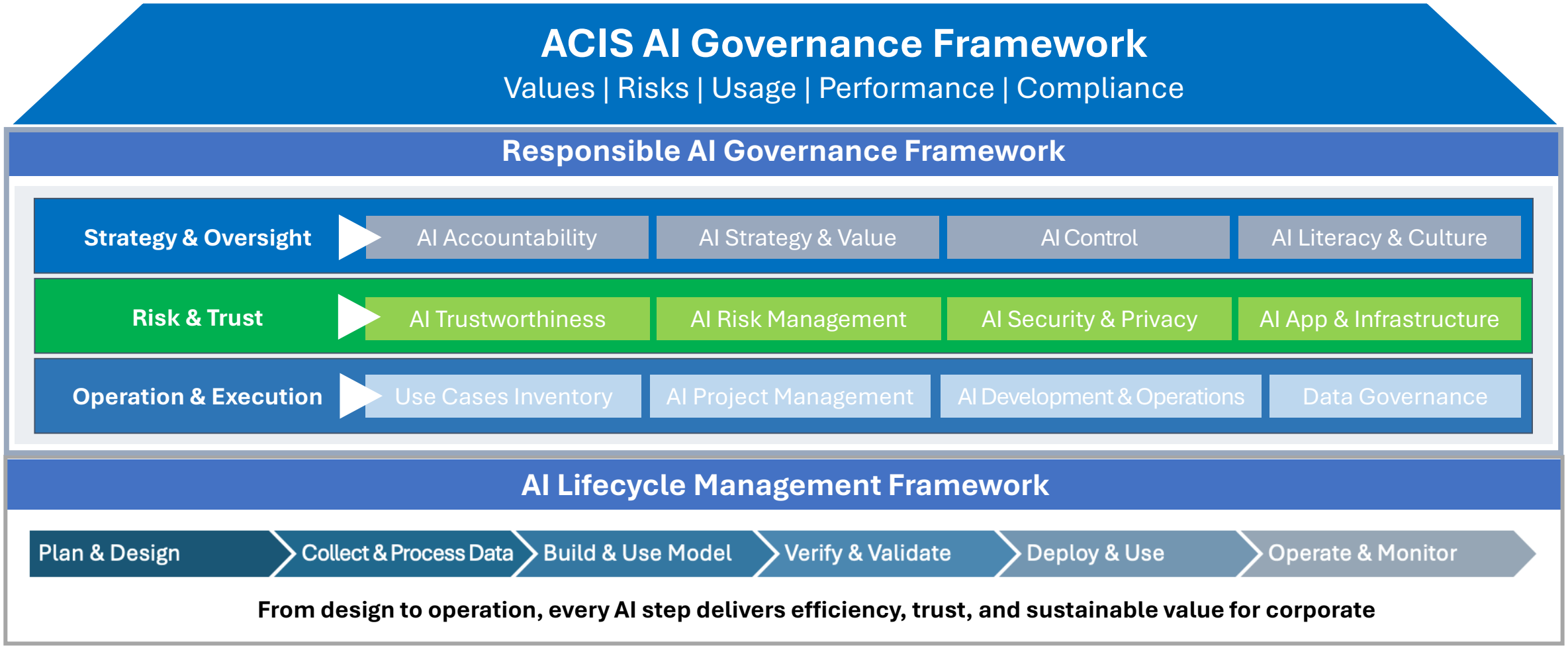
Oversight			
1) Accountability	2) AI Value	3) AI Control	4) AI Literacy & Culture
Risk Management			
5) AI Trustworthiness	6) AI Risk & Impact	7) AI Security & Privacy	8) Data Governance
Operations			
9) AI Project Management	10) Use Cases Inventory	11) AI Development & Use	12) AI App & Infrastructure

AI Lifecycle Management Framework

Plan & Design	Collect & Process Data	Build & Use Model	Verify & Validate	Deploy & Use	Operate & Monitor
• Define business problem • Gather requirements • Assess technical and data • Define success metrics • Design the high-level system architecture • Plan project resources	• Identify data source • Ingest and aggregate raw data • Cleanse & normalize data • Label or annotate data • Split the data into training, validation, and test sets	• Select algorithms and model • Write the code for model training • Train the model • Tune model to optimize performance	• Evaluate model performance against the validation and test datasets • Test for and mitigate bias • Assess the model's robustness and security • Validate that the model's outputs meet the business requirements	• Package the model for production • Set up and configure infrastructure • Integrate the model into the target application or workflow • Perform final integration testing in a staging environment • Release the model into production	• Continuously monitor model performance, latency, and resource usage • Track for data drift or concept drift • Log for analysis and auditing • Set up automated alerts for anomalies • Retrain to keep the model current • Collect user feedback for improvements • Retirement

ACIS AI Governance Framework

Covers all AI usage and development



ISO/IEC 42001:2023

ISO/IEC 42001:2023 (AIMS)

What it is:

- ✓ An international management system standard specifically designed for AI
- ✓ A framework for establishing policies, processes, and controls for AI governance
- ✓ A risk-based approach that scales with your AI maturity and use cases
- ✓ Compatible with existing management systems (e.g., ISO 27001)
- ✓ A foundation for legal compliance and regulatory readiness

What it isn't:

- X A technical specification for building AI models
- X A one-size-fits-all checklist
- X A guarantee against all AI-related risks
- X A replacement for domain expertise, legal judgment, or ethical reasoning

ISO/IEC 42001:2023 (AIMS)


INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

ISO IEC

Reference number
ISO/IEC 42001:2023(E)

© ISO/IEC 2023

Management System Series

Year Published

ISO/IEC 42001:2023

Information Technology Artificial intelligence — Management System

First Edition, Dec. 2023

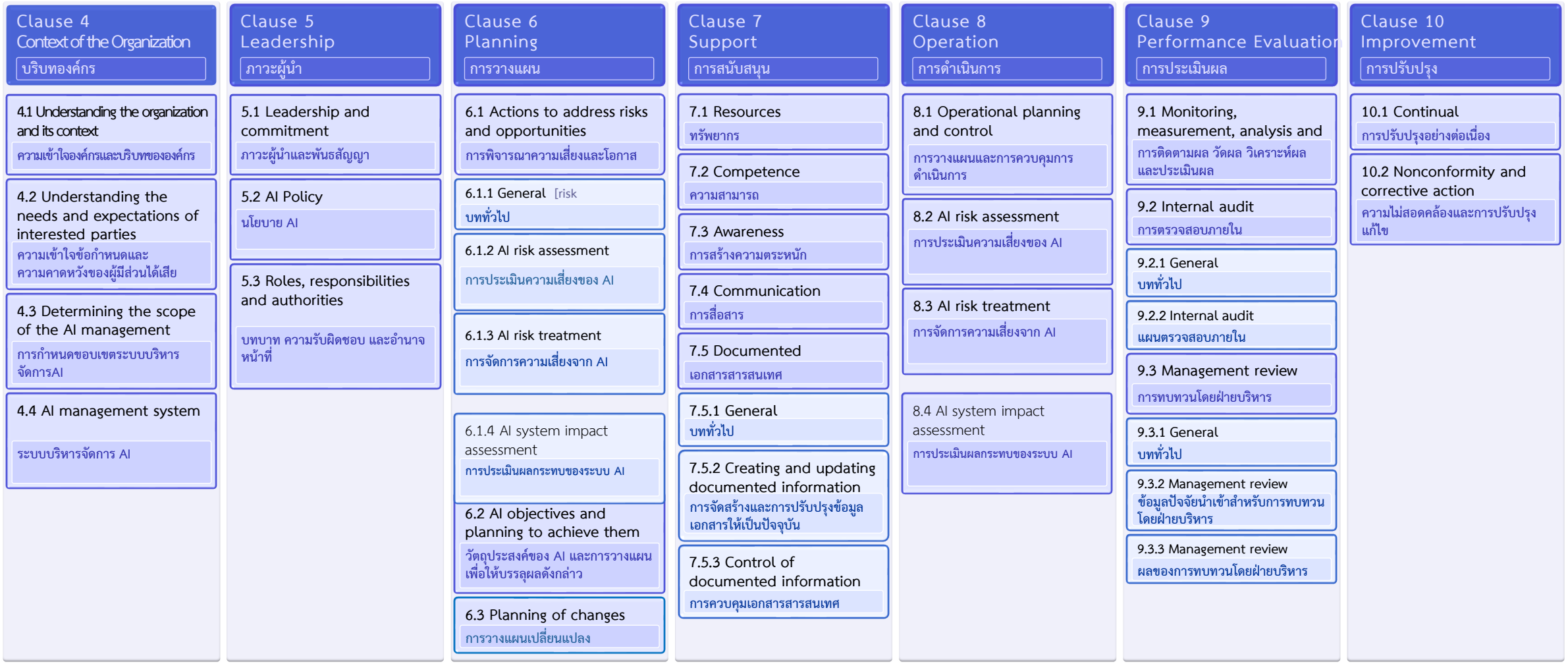
มาตรฐานการจัดการปัญญาประดิษฐ์ (AI)

General Information https://www.iso.org/standard/81230.html

Preview : https://www.iso.org/obp/ui/en/#iso:std:iso-iec:42001:ed-1:v1:en

ISO/IEC 42001:2023 (AIMS) เวอร์ชั่นแรก ประกาศ ณ เดือนธันวาคม 2566 (2023-12)

ISO/IEC 42001:2023 (AIMS)



ISO/IEC 42001:2023 (AIMS)

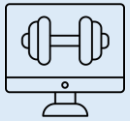
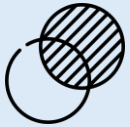
Appendix A: Reference Control Objectives and Controls

The controls provide the organization with a reference for meeting organizational objectives and addressing risks related to the design and operation of AI systems. Not all the control objectives and controls listed in the Appendix A are required, and the organization can design and implement their own controls.

A.1	General บททั่วไป
A.2	Policies Related to AI นโยบายที่เกี่ยวข้องกับ AI
A.3	Internal Organization ภายในองค์กร
A.4	Resources for AI Systems ทรัพยากรสำหรับระบบ AI
A.5	Assessing Impacts of AI Systems การประเมินผลกระทบของระบบ AI
A.6	AI System lifecycle วงจรชีวิตของระบบ AI
A.7	Data for AI system ข้อมูลสำหรับระบบ AI
A.8	Information for interested parties of AI systems ข้อมูลสำหรับผู้ที่สนใจเกี่ยวกับระบบ AI
A.9	Use of AI Systems การใช้ระบบ AI
A.10	Third –party and customer relationships ความสัมพันธ์ระหว่างบุคคลที่สามและลูกค้า

ISO/IEC 42001:2023 (AIMS)

When identifying risks of AI systems, various **AI-related objectives** should be taken into account, depending on the nature of the system under consideration and its application context. AI-related objectives to consider include but are not limited to the objectives described

 **Accountability**	 **AI Expertise**	 **Availability and Quality of Training & Test Data**
 **Environmental Impact**	 **Fairness**	 **Maintainability**
 **Privacy**	 **Robustness**	 **Safety**
 **Security**	 **Transparency and Explainability**	

The Implementation Overview

ISO 42001 follows the Plan-Do-Check-Act cycle

The Core Cycle

Plan (Steps 1-12) • Do (13-15)
Check (16-18) • Act (19-22)

Expected Outcomes

- ✔ Robust AI governance structures
- ✔ Ethical & transparent operations
- ✔ Increased stakeholder trust
- ✔ Proactive AI risk management
- ✔ Regulatory compliance (e.g., EU AI Act)
- ✔ Operational excellence in AI

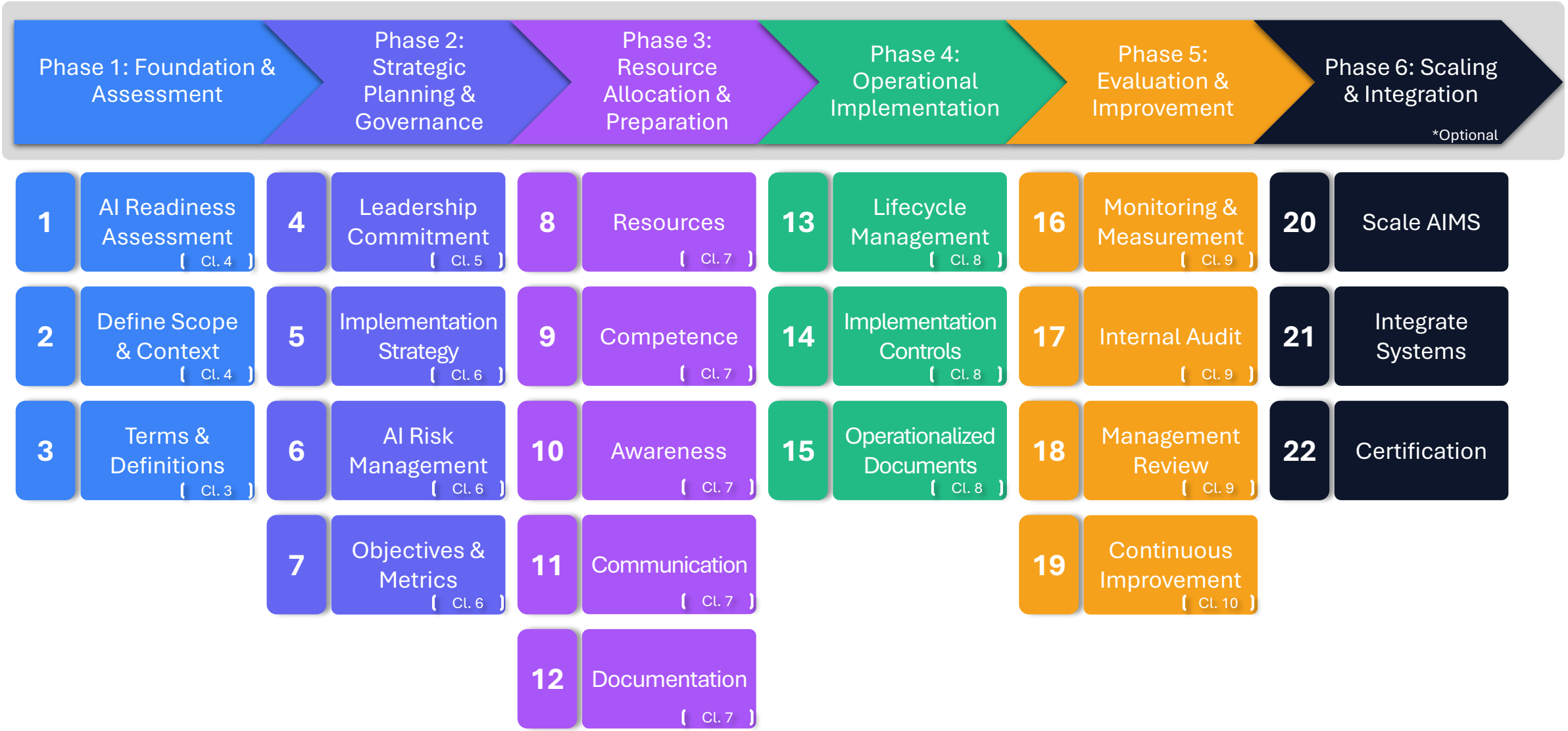
PLAN: Define objectives, identify risks, establish governance

DO: Implement AI systems with controls and documentation

CHECK: Monitor performance, conduct audits, evaluate compliance

ACT: Implement improvements and corrective actions

The Implementation Overview



The Implementation Overview

1

PHASE 1

Foundation & Assessment

Understand Context

1 AI READINESS

- *Conduct AI maturity assessment*
- Inventory existing AI systems
- Perform Clause 4-10 gap analysis

2 SCOPE & CONTEXT

- *Define AIMS boundaries*
- Analyze internal/external context
- Perform stakeholder mapping

3 TERMINOLOGY

- *Create AI terminology glossary*
- Standardize vocab across org
- Define industry-specific terms

2

PHASE 2

Strategic Planning & Governance

Set Direction

4 LEADERSHIP

- *Develop AI Governance Policy*
- Assign RACI responsibilities
- Charter Governance Committee

5 STRATEGY

- *Define rollout approach*
- Create implementation roadmap
- Prioritize pilot AI systems

6 RISK PLANNING

- *Establish Risk Framework*
- Identify AI-specific risks
- Develop Risk Register & Matrix

7 OBJECTIVES

- *Set SMART AIMS objectives*
- Define AI Performance KPIs
- Create measurement framework

3

PHASE 3

Resource Allocation & Preparation

Build Support

8. RESOURCES

- *Budget approval*
- Tech/Tool audit
- Procurement plan

9. COMPETENCE

- *Identify skill gaps*
- Role-based training
- Competence matrix

10. AWARENESS

- *Campaign delivery*
- Onboarding content
- Ethics posters

11. COMM.

- *Internal/Ext plan*
- Feedback loops
- Incident protocols

12. DOC.

- *Setup DMS system*
- Version controls
- Policy hierarchy

The Implementation Overview

4

PHASE 4

Operational Implementation

CORE "DO" PHASE

13 Lifecycle Management

- *Define entry/exit criteria per stage*
- Document design & data choices
- Implement validation gates

14 Control Implementation

- *Deploy bias & fairness testing*
- Setup Human-in-the-Loop oversight
- Apply adversarial robust security

15 AI System Documentation

- *Publish AI Model Cards / Fact Sheets*
- Map data provenance & lineage
- Establish system transparency docs

5

PHASE 5

Performance & Improvement

Verify & Refine

16 MONITORING

- *Deploy monitoring dashboards*
- Track model drift & performance
- Real-time bias alerting

17 INTERNAL AUDIT

- *Charter audit program*
- Conduct conformity assessments
- Manage findings register

18 MGMT REVIEW

- *Conduct leadership reviews*
- Analyze context changes
- Strategic action planning

19 IMPROVEMENT

- *Address non-conformities*
- Perform root-cause analysis
- Share lessons learned

6

PHASE 6

Scaling & Integration

Go Global

20. Scale AIMS

- *Evaluate pilot success*
- Plan organization-wide rollout
- Embed AI ethics in culture

21. Integration

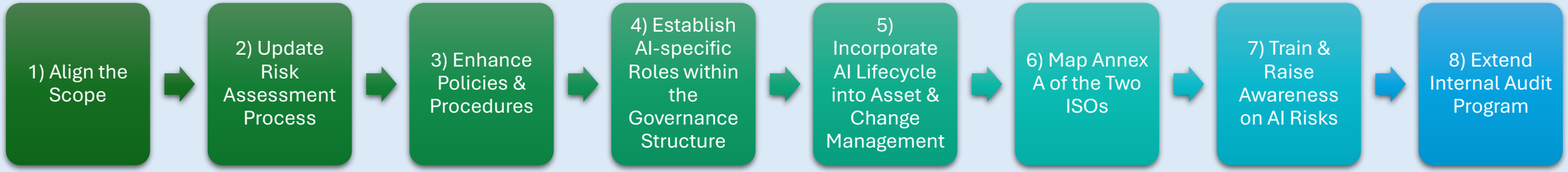
- *Align with ISO 9001/27001*
- Unified management reviews
- Streamline shared controls

22. Certification

- *Conduct pre-assessment audit*
- Select accredited registrar
- Undergo certification audit

Integrating ISO 42001 into Existing ISO 27001

The Integration Steps



1. Identify AI systems in use
   - Define roles, teams, and departments using or building AI
   - Map how these systems interact with existing ISMS assets
2. Include AI-specific risks in ISMS risk register, e.g., bias & discrimination in AI outputs and data leakage/breach
3. Integrate AI governance into existing security & privacy policies
4. Extend the committee/council to include data scientist, AI/ML engineers, legal, risk & compliance
5. Treat AI models as assets and track their lifecycle
6. Looks for overlaps in controls to avoid duplication
7. Make AI a part of regular security awareness training
8. Schedule AI-specific audits as a part of ISMS internal audits

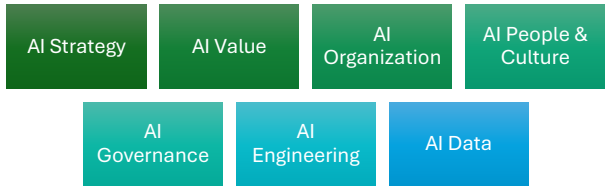
Our Approach for Implementation

The Approach Overview

STEP 1-7 **Assess the current practices and plan for success (2-month)**

STEP 8-22 **Implementations (6-month)** *Excluding CB audit

- Assess current AI-Related practices of an organization in 7 holistical domains



- Identify gaps and mitigations
- Understand current environment & management systems and identify & analyze stakeholders
- Prepare a strategic roadmap for implementation aligning with existing management framework (e.g., ISO 27001)
- Select an AI solution for certification (Scoping)
- Identify objtectives and working team

- Identify resource needed for the selected AI solution (human, model, data, and infrastructure)
- Establish AI governance structure (Operating model), integrating with exsiting structure
- Develop/enhance management system documents (policy & procedures) aligning with ISO 42001 and other relevant standards, e.g., NIST AI RMF, EU AI Act, ETDA AI Governance Guideline
- Conduct AI impact and risk assessments
- Conduct internal audit (IA) / integrate AI audit into existing internal audit plan and program
- Prepare for certification (CB Audit)

Documents Required by ISO 42001 (Not Exhaustive)

- AIMS scope and boundaries
- **Policies and procedures**
- Objectives and plans to achieve them
- Impact & risk assessments and risk register
- Competence evidence
- Communication plans
- Control documents
- Monitoring and measurement records
- Feedback, change and incident records
- Audit programs, plan, and results
- Management review records
- Nonconformity and corrective action records
- AI system documentation
- Training materials and records
- Stakeholder communications
- Evidence of control effectiveness
- Improvement initiatives

Examples of Policies

- AI Acceptable Use Policy
- Data Governance Policy
- Risk Management Policy
- Bias and Fairness Policy
- Privacy and Security Policy
- Human Oversight Policy

Examples of Procedures

- AI System Lifecycle Procedure
- Risk Assessment and Treatment Procedure
- Bias Detection and Mitigation Procedure
- Model Validation and Testing Procedure
- Human Oversight Procedure
- Incident Response Procedure
- Audit and Review Procedure
- Training and Competence Procedure
- Change Management Procedure
- Document Control Procedure

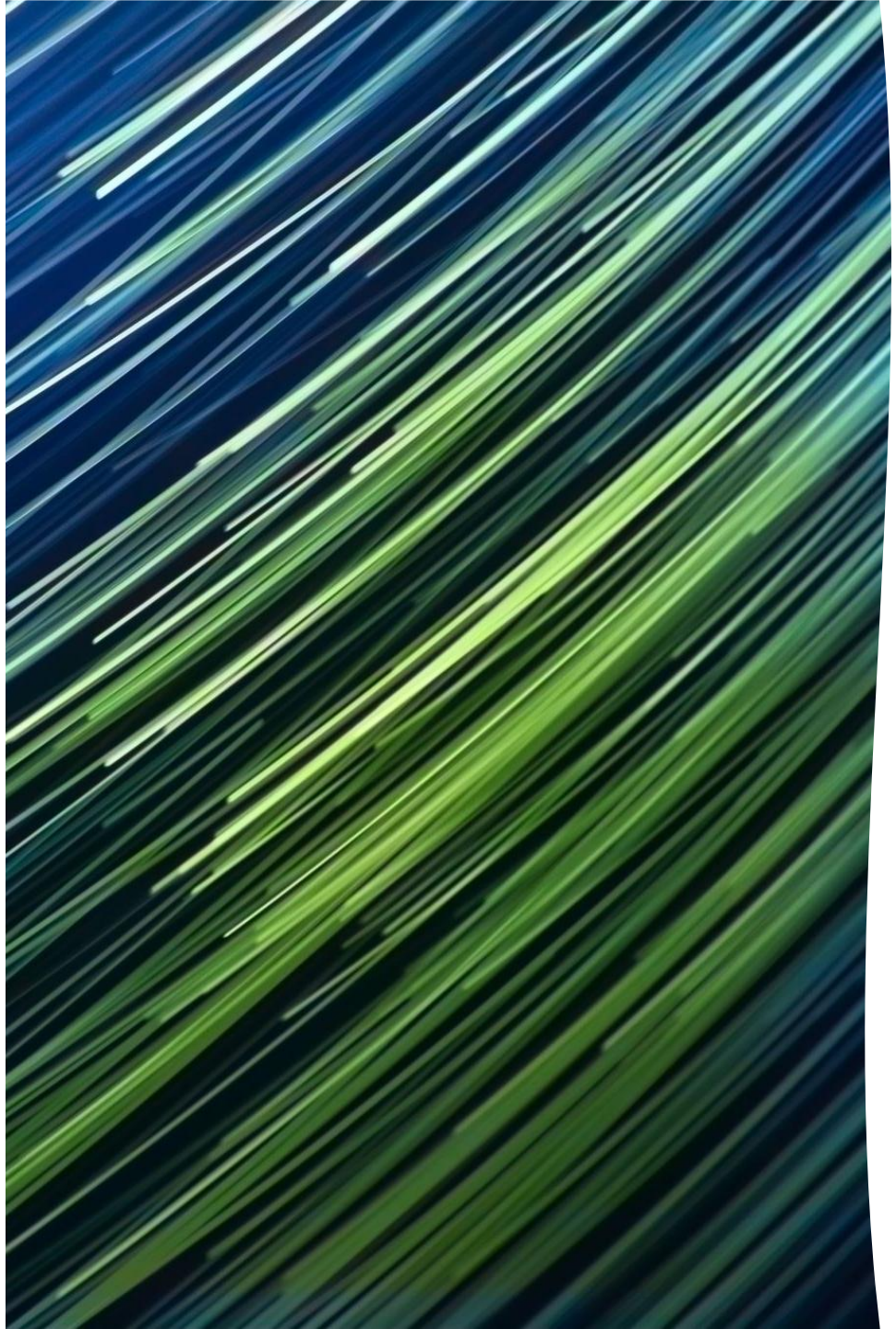
Post-Quantum Cryptography (PQC)

Preparing for a Quantum-Resistant Future

What is PQC?

Post-Quantum Cryptography (PQC) includes cryptographic algorithms designed to resist quantum computer attacks.

Unlike RSA or ECC, PQC is secure against quantum algorithms like Shor’s and Grover’s.



Why Do We Need PQC?

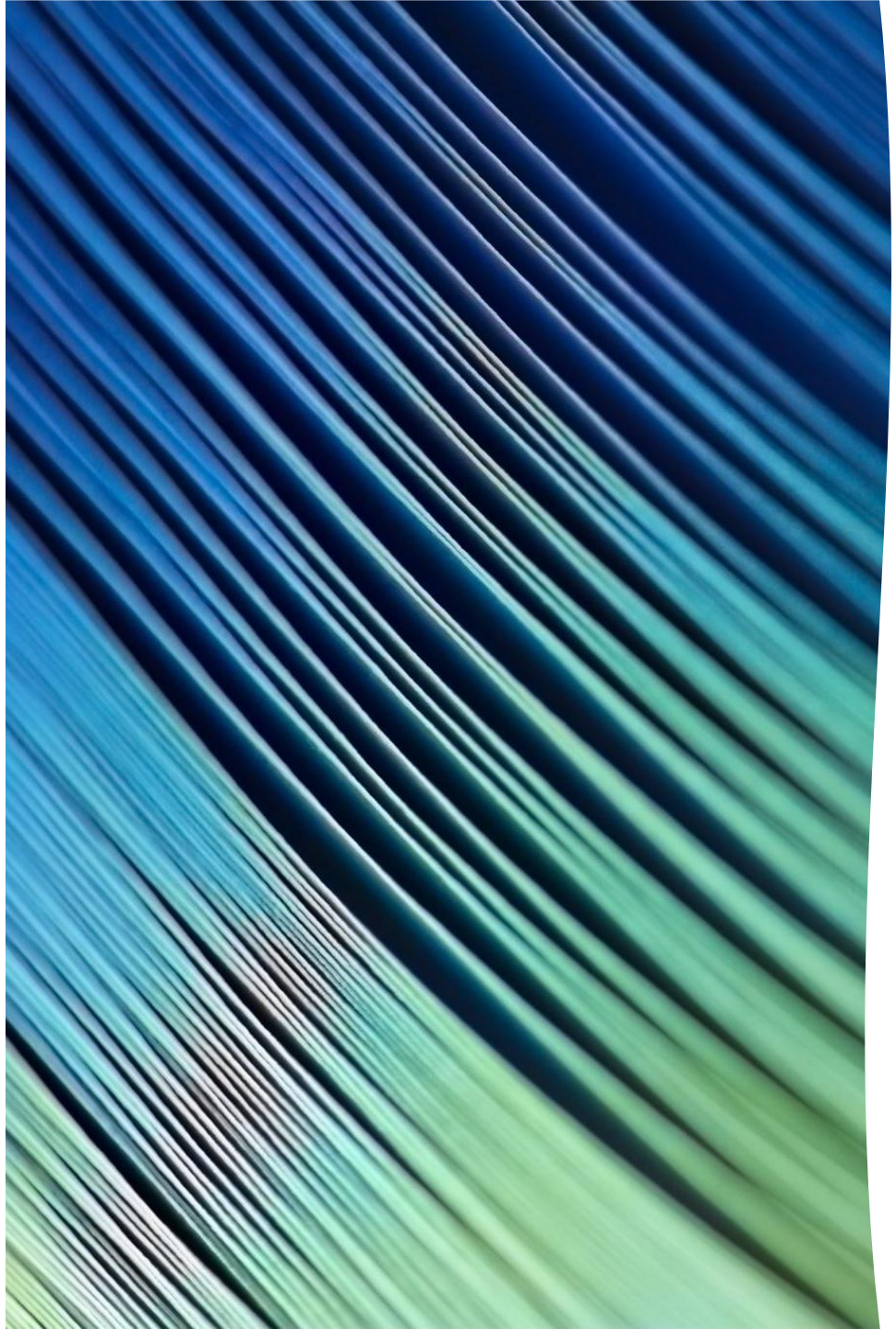
Quantum computers will break RSA and ECC.

'Harvest now, decrypt later' means encrypted data today can be decrypted in the future.

AES-256 is reduced to AES-128 security level under quantum attacks.

Key Characteristics of PQC

- Quantum-resistant: secure against quantum & classical threats
- Classical-compatible: runs on today’s hardware
- Requires longer keys than RSA/ECC
- Under evaluation by NIST for global standards



NIST PQC Standardization

Selected algorithms:

- CRYSTALS-Kyber (Encryption)
- CRYSTALS-Dilithium (Signature)
- FALCON (Signature)
- SPHINCS+ (Signature)

What Should Organizations Do Now?

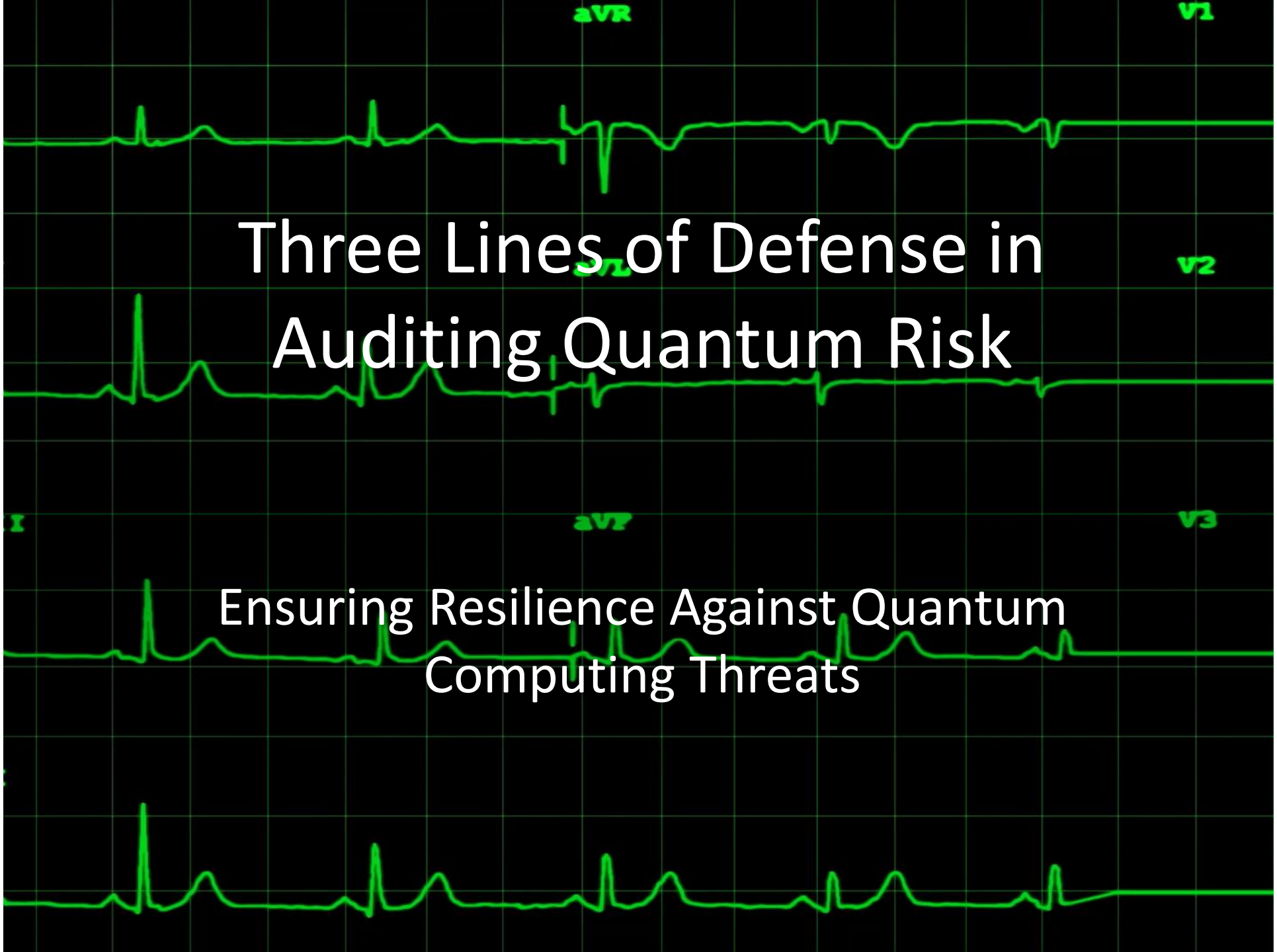
- Inventory cryptographic usage (RSA/ECC)

- Assess long-term data exposure risk

- Plan for crypto-agility and upgrades

- Require PQC-readiness in vendor contracts

- Monitor NIST PQC standard rollout

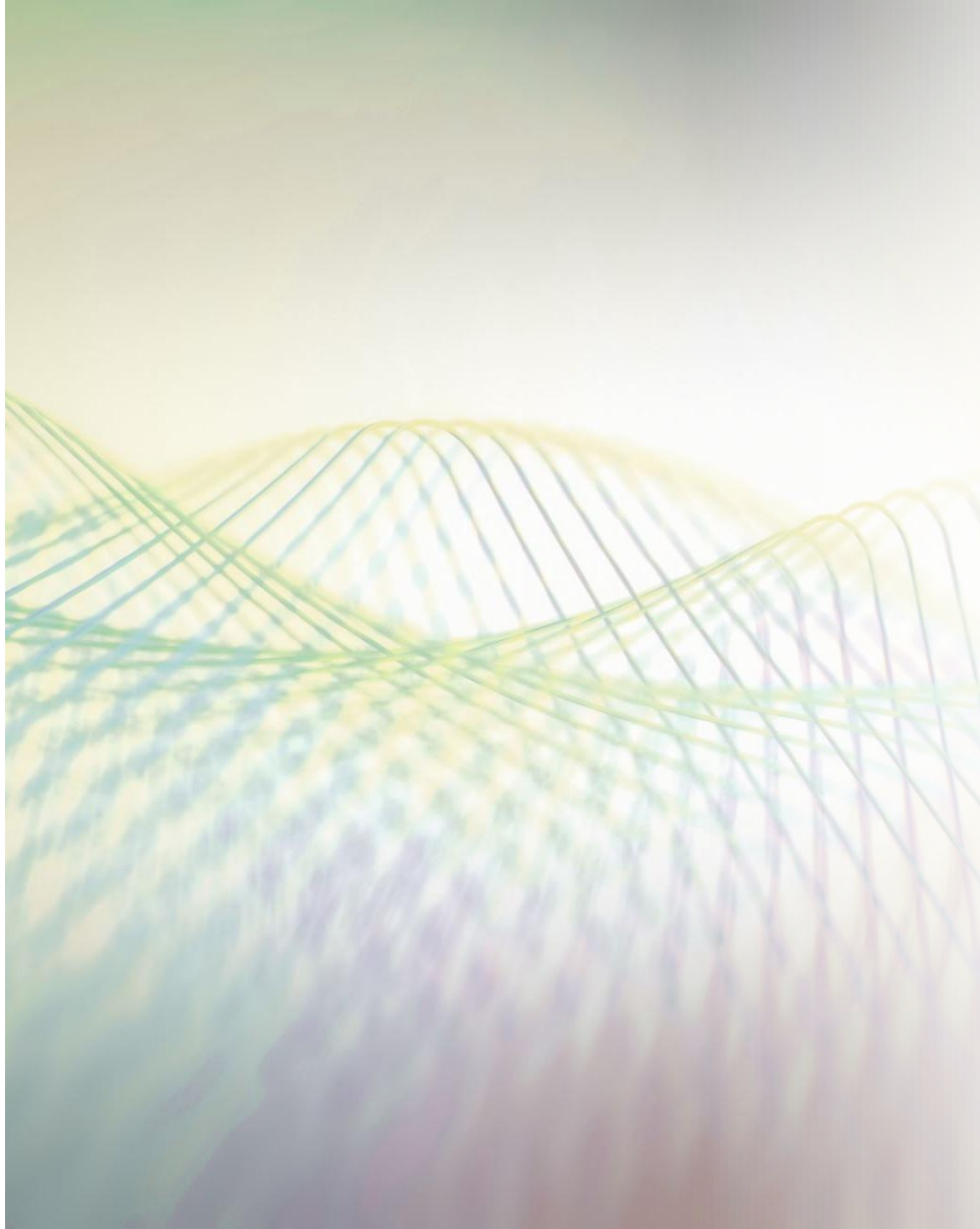


Three Lines of Defense in Auditing Quantum Risk

Ensuring Resilience Against Quantum Computing Threats

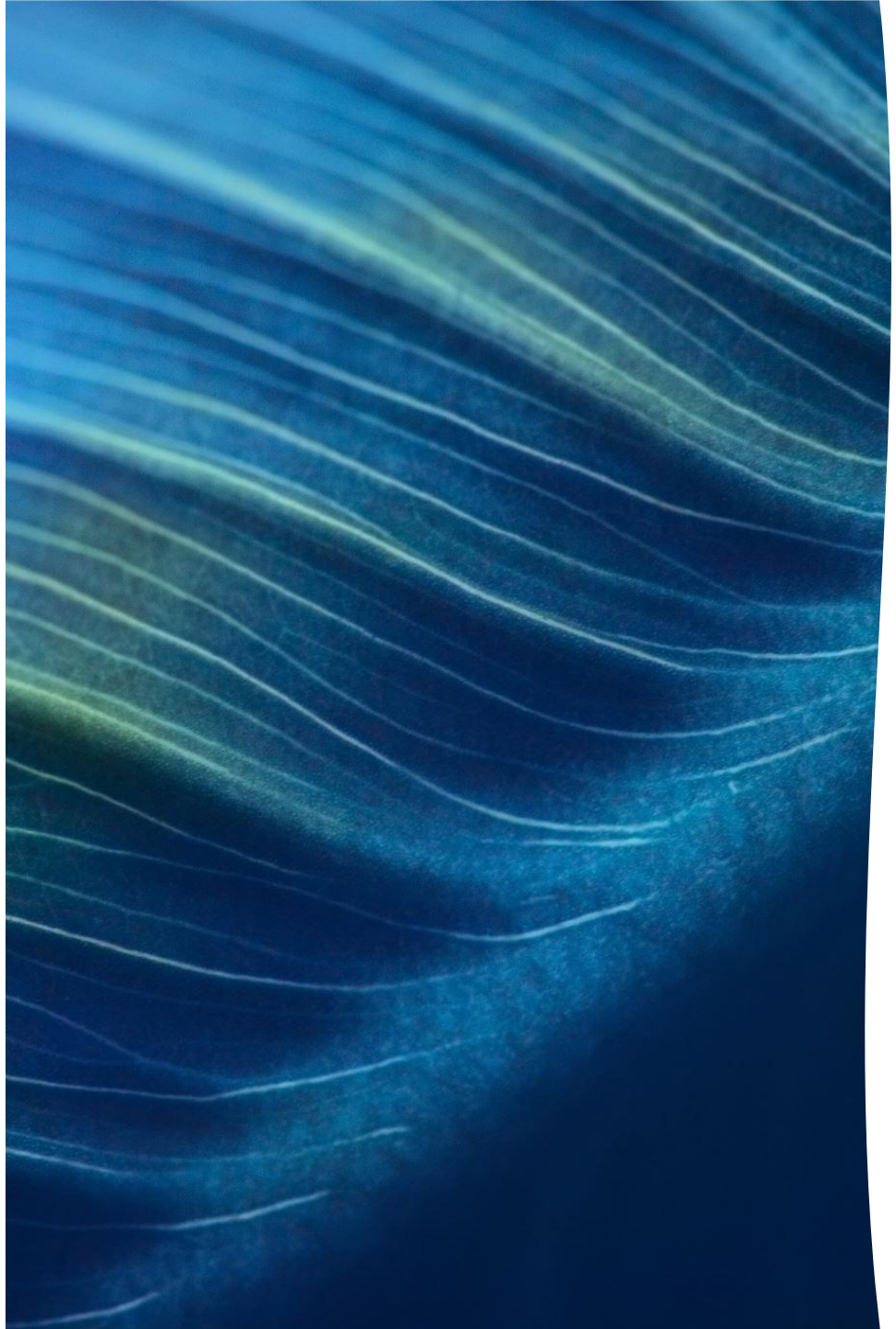
First Line: IT, Security & Crypto Owners

- - Manage and operate cryptographic systems
- - Inventory RSA/ECC assets and assess crypto exposure
- - Identify long-term data confidentiality needs
- - Pilot Post-Quantum Cryptography (PQC)
- - Maintain crypto-agility in applications



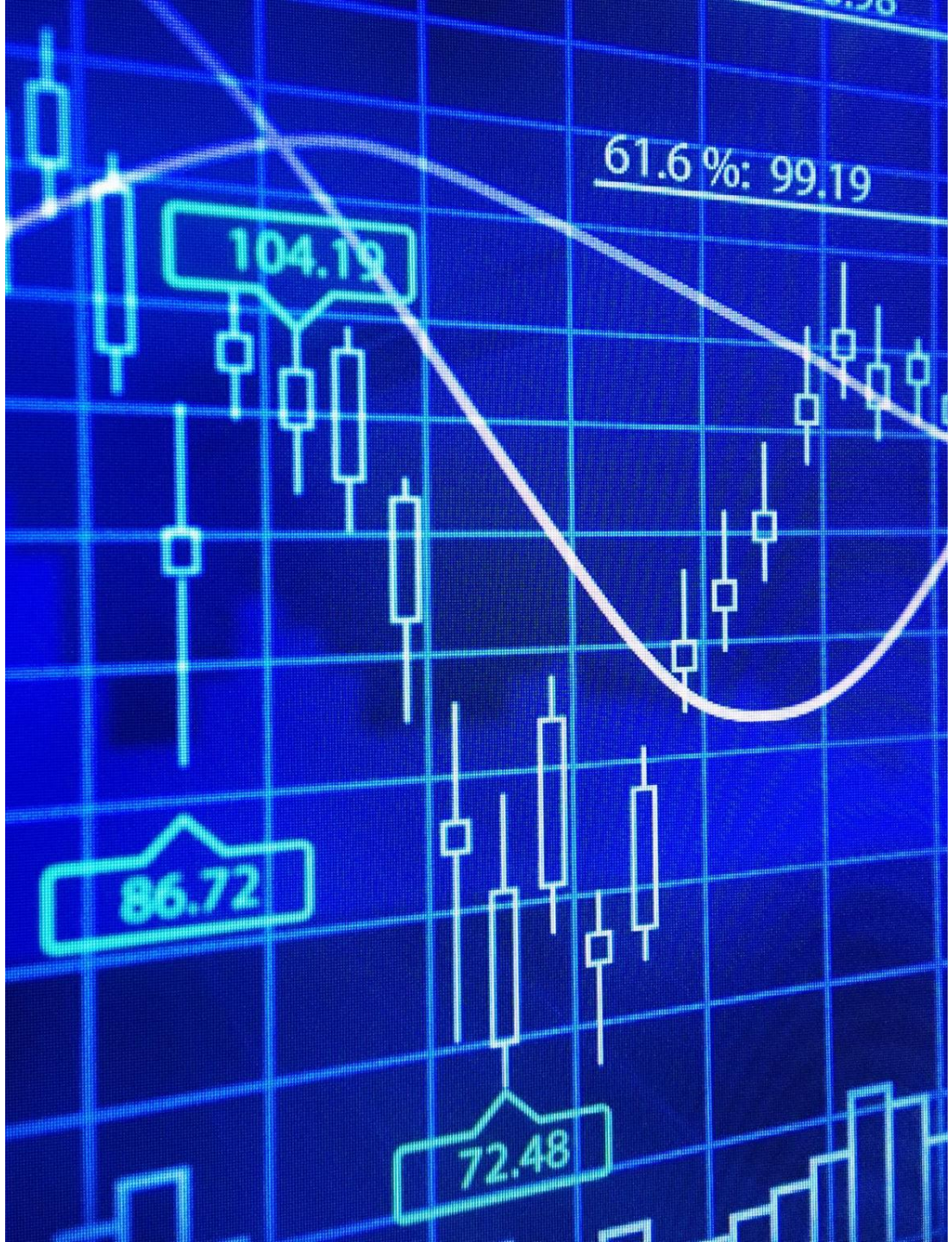
Second Line: Risk, Compliance & Governance

- - Define crypto-agility and PQC standards
- - Align policies with NIST, ETSI, ISO
- - Validate vendor quantum-resilience
- - Include quantum risk in ERM registers
- - Oversee quantum-readiness roadmap



Third Line: Internal Audit / Independent Assurance

Audit	- Audit cryptographic inventory and lifecycle controls
Evaluate	- Evaluate PQC transition maturity
Review	- Review governance over key management
Benchmark	- Benchmark against industry best practices
Report	- Report audit findings to senior management



Board & Executive Oversight

- - Approve crypto-resilience strategy and roadmap
- - Allocate budget for PQC and crypto upgrade
- - Oversee high-value third-party risks
- - Monitor compliance with global crypto standards

Country Level Risk about the future of Thailand AI Sovereignty

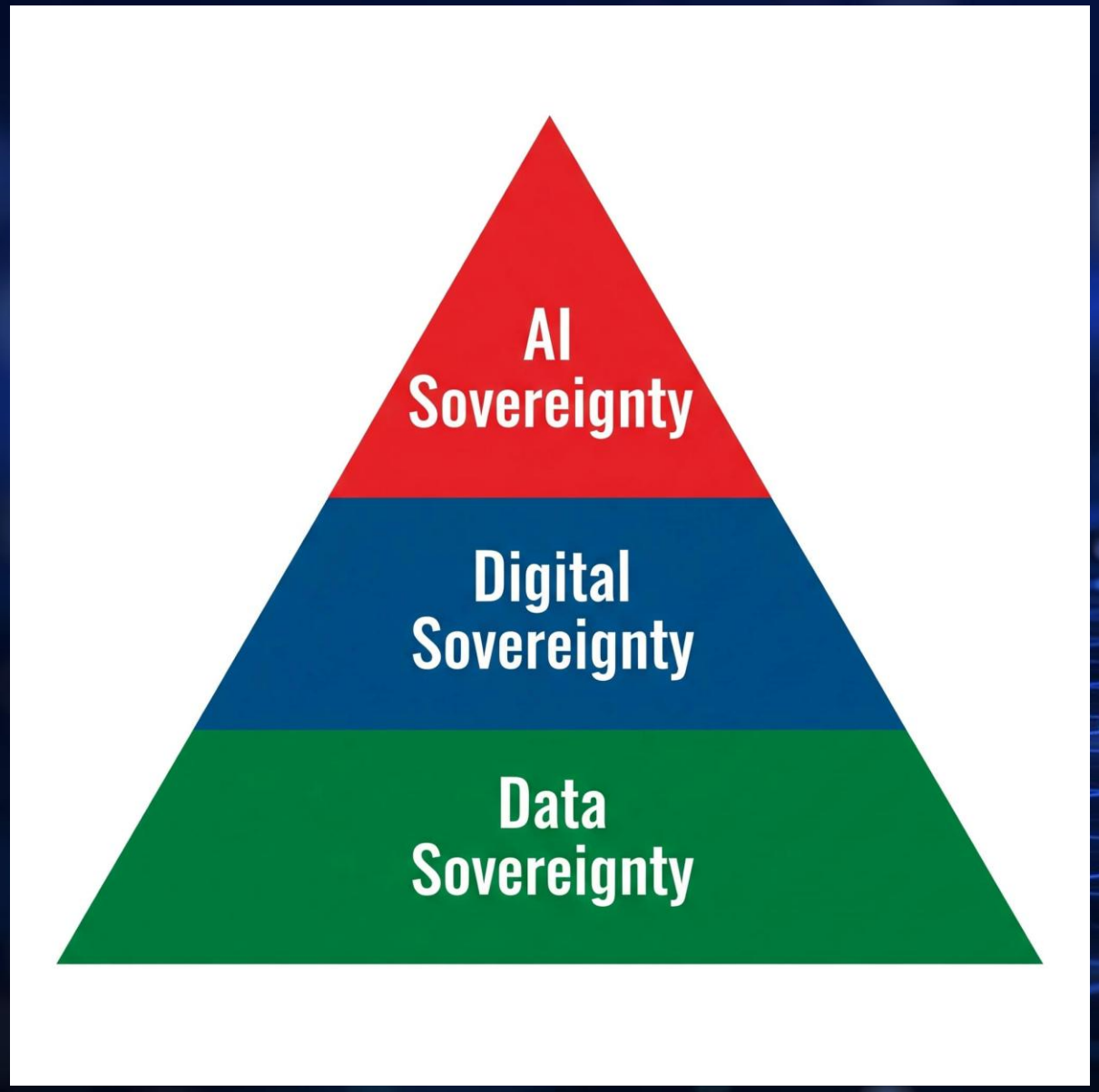
Data, Digital, and AI Sovereignty

Understanding the Pyramid of Technological Technological Sovereignty

From Data Sovereignty to Digital Sovereignty

From Digital Sovereignty to AI Sovereignty

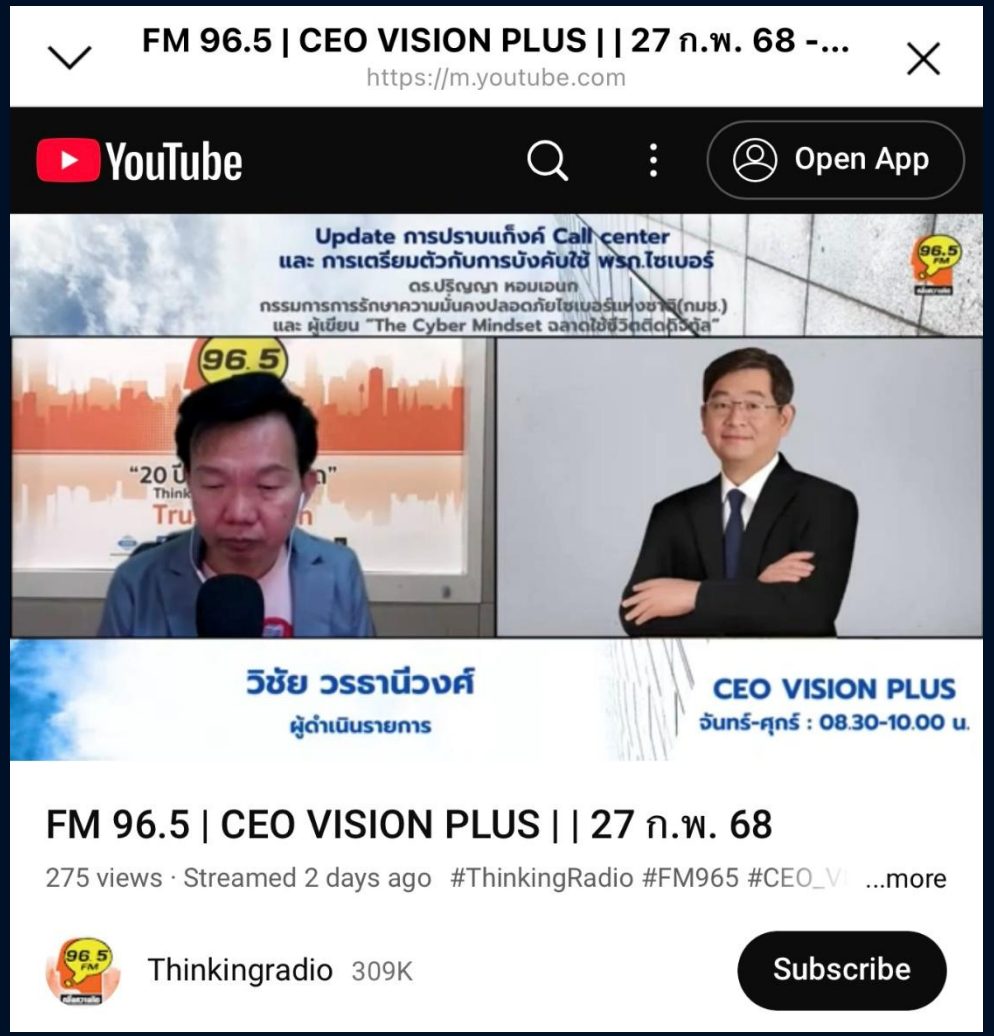
“Sovereignty in the Age of AI: Governing Data, Infrastructure, and Intelligence”



FM 100.5 MHz. 16:30 SUN

FM 96.5 MHz. 8:30 AM @ Thursday

FM 96.5 MHz. 8:30 AM @ Thursday



Further reading links

CDIC : https://www.cdicconference.com

ACIS : https://www.acisonline.net

Cybertron : https://www.cybertron.co.th

My Blog : https://www.prinya.org

YouTube :
"The Cyber Mindset Series" PodCast

THANK YOU!

ACIS Professional Center Co., Ltd.
140/1 Kian Gwan Building2 18th Floor, Wireless Road, Lumpini,
Pathumwan, Bangkok 10330

www.acisonline.net

Tel : +66 (88) 022 2624