IAR The Center of Internal Audit Resources

YAYASAN PENDIDIKAN INTERNAL AUDIT

SNIA

SEMINAR NASIONAL INTERNAL AUDIT

WHAT'S DRIVING **CHANGE**

to Stay Ahead of The Curve for Internal Auditors in The Coming Years ?

3-4 DESEMBER 2025 | THE STONES HOTEL, BALI

PLN mobile

PLN

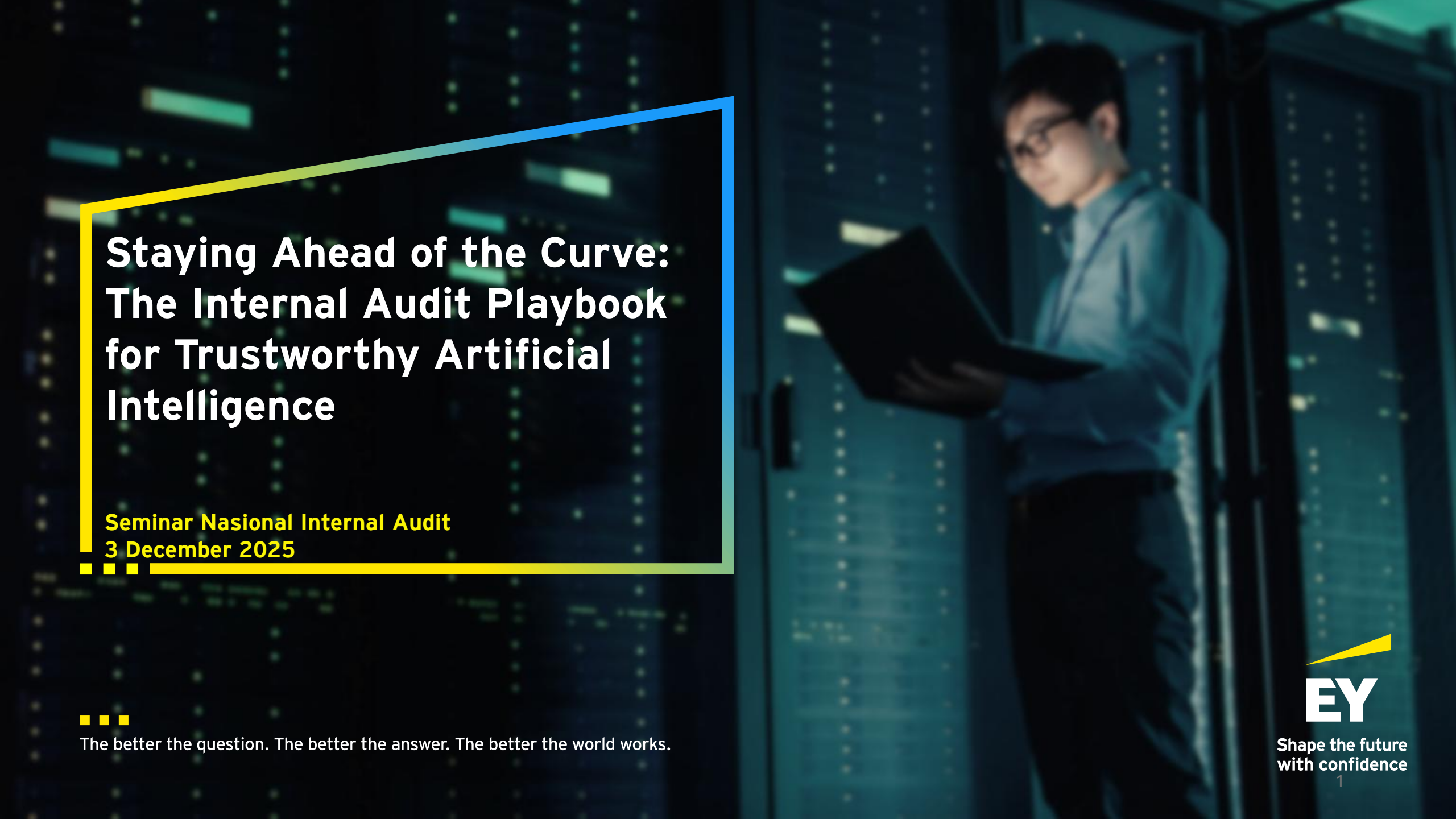
PERTAMINA

mandiri

QIA · QGIA · QHIA · PQIA · CPIA

Staying Ahead of the Curve: The Internal Audit Playbook for Trustworthy Artificial Intelligence

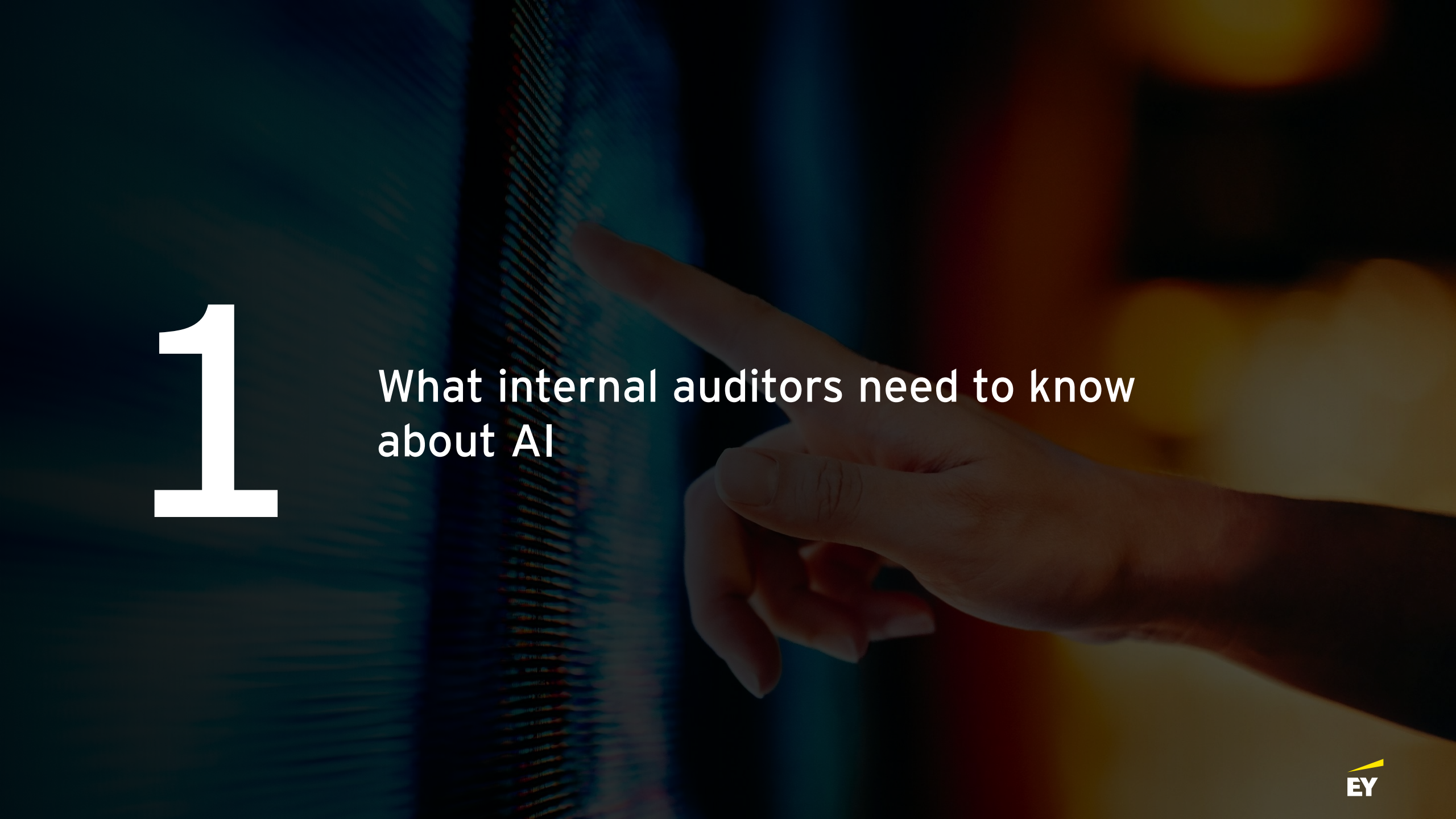
Seminar Nasional Internal Audit
3 December 2025



The better the question. The better the answer. The better the world works.

Shape the future with confidence

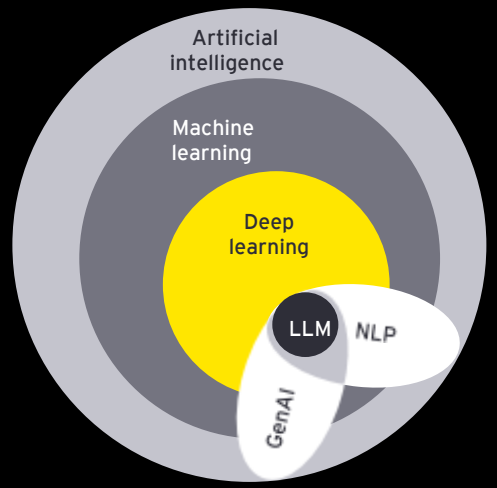
Table of Contents



1

What internal auditors need to know about AI

AI – what internal auditors need to know



AI broadly refers to machines that mimic humanlike cognitive abilities, AI agents, and generative AI (GenAI). AI includes capabilities such as natural language processing, problem-solving, pattern recognition, anomaly identification, and decision-making.

GenAI refers to a subset of AI that is based on probabilistic technology that can create content, including text, images, audio, or video, when prompted by a user.

Through its ease of use, GenAI has democratized artificial intelligence making the technology accessible to any user, whereas other types of artificial intelligence have generally only been accessible to data scientists.

Key factors exacerbating the role of internal audit in auditing AI

- **Increasing stakeholder demands** for desired outcomes and risk mitigation – institutional and activist investors – as well as consumers, employees and business partners – are asking more difficult questions around how companies are managing AI-related risks and issues.
- **Evolving global regulations** continue to focus on companies' use of AI – jurisdictions and regulatory bodies around the world are developing guidance on the design, use and deployment of AI, including risk management.
- **Ad hoc and siloed approach** to managing AI risks and opportunities – AI issues span across various functions within a company, and ownership of data, risks and controls may be unclear or unassigned. Integration of AI issues into existing governance and oversight models is limited, potentially resulting in unidentified gaps in risk coverage across the company.
- **Heightened demand for AI skill sets/upskilling talent** to deliver capabilities and manage associated risks – increase hiring and training to address organizational ambitions and risk management activities, including oversight and governance of AI processes, risks and controls.

AI regulation in Indonesia

Surat Edaran Menteri Komunikasi dan Informatika No. 9 Tahun 2023

SURAT EDARAN MENTERI
KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA
NOMOR 9 TAHUN 2023
TENTANG
ETIKA KECERDASAN ARTIFISIAL

- A guideline for the ethical use of Artificial Intelligence.
- Serves as an authoritative reference for business entities (pelaku usaha) and electronic system operators (penyelenggara sistem elektronik), particularly in the formulation of internal policies governing the utilization of Artificial Intelligence.

Peta Jalan Kecerdasan Artifisial Nasional

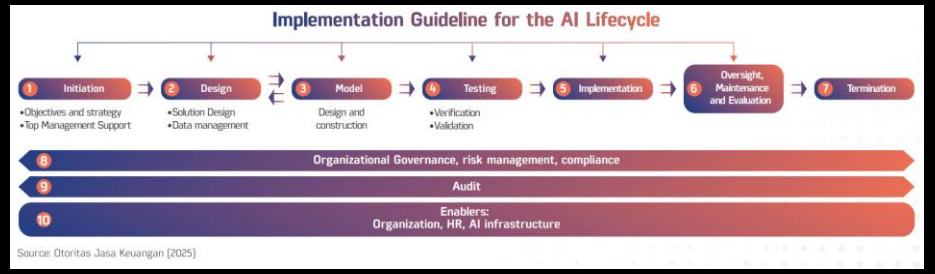
KOMDIGI

- Currently in progress. The White Paper (Buku Putih) on the National AI Roadmap was opened for public consultation in August 2025.
- Intended to serve as a foundational basis for designing policy and regulatory strategies related to the governance of Artificial Intelligence utilization in Indonesia.
- Structured around four key pillars: (1) Ethics and Policy, (2) Talent Development, (3) Infrastructure and Data Development, and (4) Industrial Innovation and Research.

Tata Kelola Kecerdasan Artifisial Perbankan Indonesia

OJK OTORITAS JASA KEUANGAN

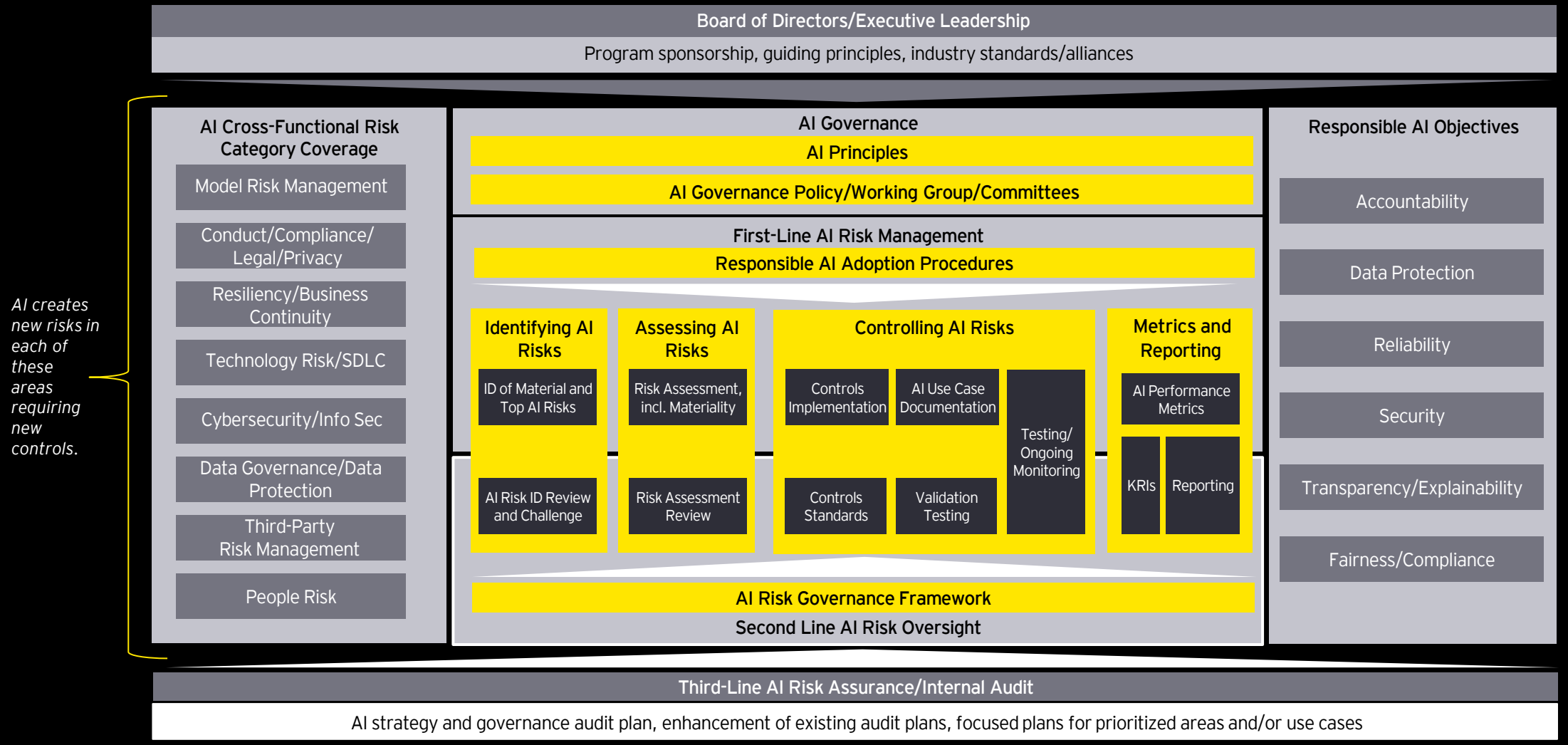
- Published in April 2025.
- Provides guidance for banks in Indonesia to ensure that Artificial Intelligence—including advanced AI systems—is developed and implemented in a responsible manner.
- Designed to complement digital transformation policies issued by OJK for the banking sector.
- Developed with reference to international best practices, including the EU AI Act and the Basel Committee on Banking Supervision guidance.
- Addresses AI system development and application comprehensively across the entire AI lifecycle and the banking business cycle to ensure that such systems are ethical, safe, and compliant with applicable regulations.



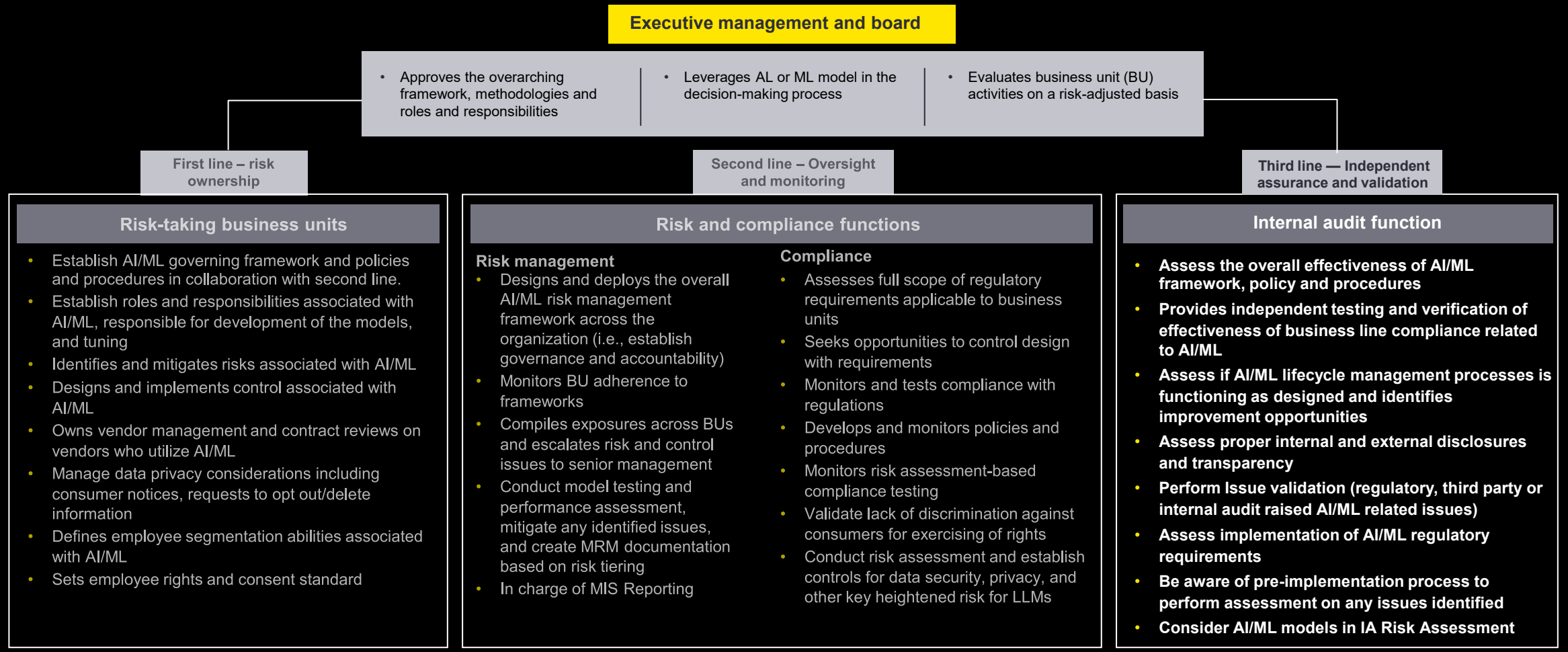
2

Internal audit – your role in governance

AI requires cross-functional governance and controls coverage



AI governance: Responsibilities of three lines model on AI adoption



The role of internal audit over responsible AI (RAI)

Internal audit's role for RAI

Compete — remove friction and establish networks to accelerate AI innovation speed-to-market and scale:

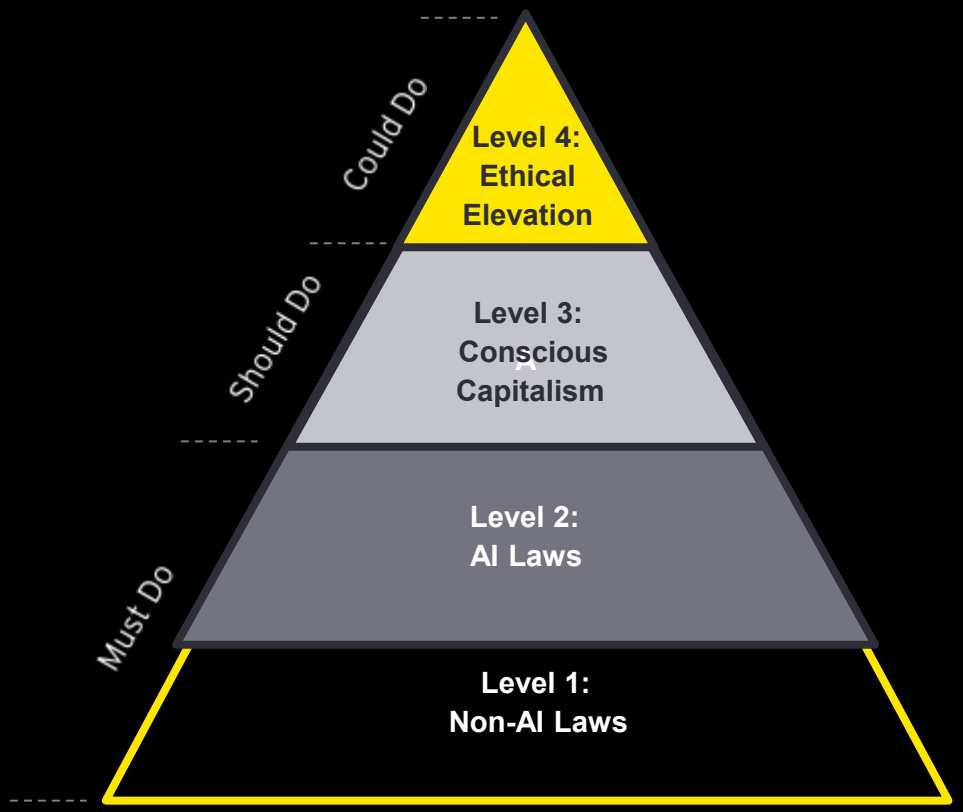
- Integral to defining how organizations will approach/use AI
- Ensures a focused, consistent and adaptable approach to innovation and scaling
- Fosters brand trust through ethical AI and transparency

Protect — safeguard the company's assets and preserve value with AI through:

- Shielding against misuse while ensuring the security of AI systems and privacy of data used and generated by AI
- Mitigates negative outcomes through AI monitoring
- Risk mitigation from external vendors who supply AI services

Comply — adhere to regulatory/legal requirements and company values:

- Respond quickly to regulatory changes, applying rules accurately.
- Turn legal requirements into executable steps swiftly.
- Perform compliance readiness review.



Defining the scope of internal audit over AI

Effective AI risk management requires foundational knowledge of concepts that define the scope of AI risk in an organization.

RAI risk universe

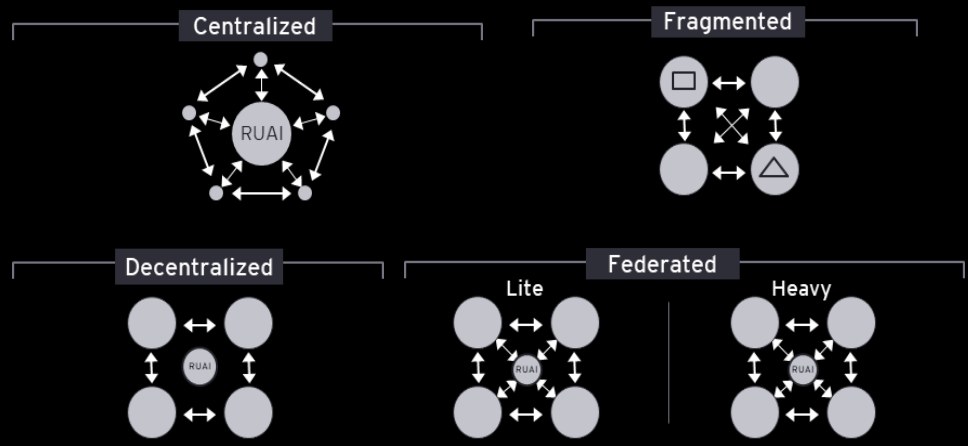
How are you defining your AI Risk Universe?

Considering risk from different pillars and lens is necessary for holistic risk management of the AI program – strategic lens, operations lens, model lens, regulatory lens.

RAI operating model

What is the AI development operating model at your organization?

While each operating model structure is best applied to different environments in which an organization operates, each model also brings in different challenges and risk that need consideration



Assess your organization's RAI journey – how does internal auditors lean in?

A review of the overall enterprise AI governance is of heightened interest across several stakeholder groups including the Audit Committees and Board of Directors.

AI governance audit scope areas

Illustrative questions that the governance audit helps answer:

- What AI-related legal or compliance considerations/requirements are deemed applicable to the organization?
- Does the company plan to restrict users from using open-source AI models in the future, or will this be permitted? Is there any policy in place for this?
- Have we considered the safety of AI architecture?

Initial questions for internal audit to assess their firm's GenAI maturity

Strategy

- Is your company's business model prepared for accelerating GenAI opportunities and risk mitigation?
- Has your organization incorporated GenAI into strategic decision-making and business case/benefits analysis?
- What is your organization's internal and external GenAI communication strategy?
- Does your organization have the right external alliances and partnerships to enable achieving its GenAI goals?
- How does your organization define long-term value for GenAI?

Governance

- Does your organization have a formal committee dedicated to GenAI Governance?
- What is management's role setting the GenAI strategy and in managing associated risks?
- Does your organization have a GenAI risk policy?
- How does your organization cascade GenAI throughout the three lines of defense (3LoD)?
- Does your company clearly understand its priority GenAI issues across all stakeholders?

Risk management

- Has your organization incorporated elevated GenAI risks into existing frameworks or taxonomies?
- How does your organization provide program assurance for GenAI initiatives to ensure they deliver intended outcomes?
- Has your organization assessed its processes, technology/tools, and models are sufficient to enable managing the GenAI lifecycle?
- Does your organization embed risk and controls into GenAI lifecycle?

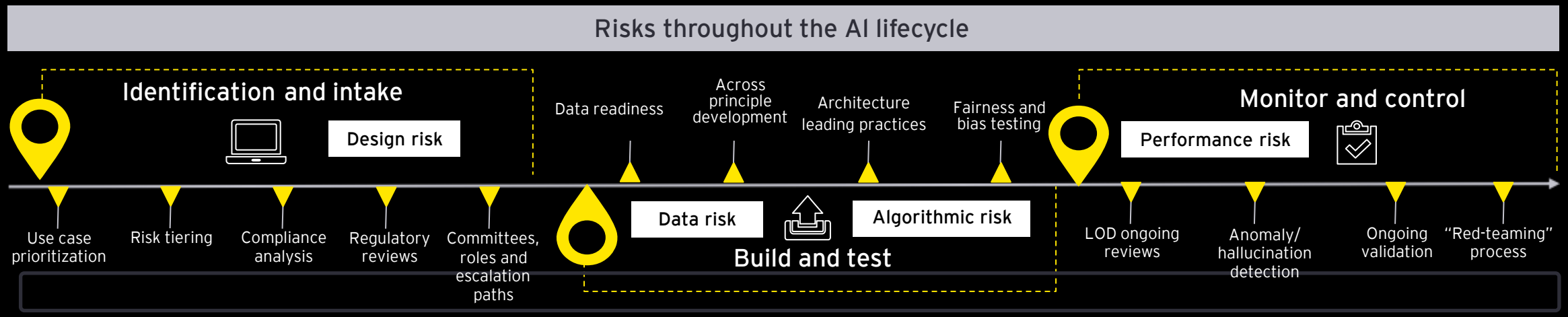
Metrics and targets

- What is the process to inventory, approve and track progress of GenAI use?
- Has your organization defined specific metrics or targets to measure and monitor GenAI impacts?
- How does your organization evaluate GenAI performance and create accountability for achieving targets?
- Has your organization established reporting and communication channels for GenAI-related initiatives?

3

Internal audit - risk and controls considerations

Understanding the RAI control environment



Technology risk, third-party risk, conduct/compliance/legal risk, business process risk

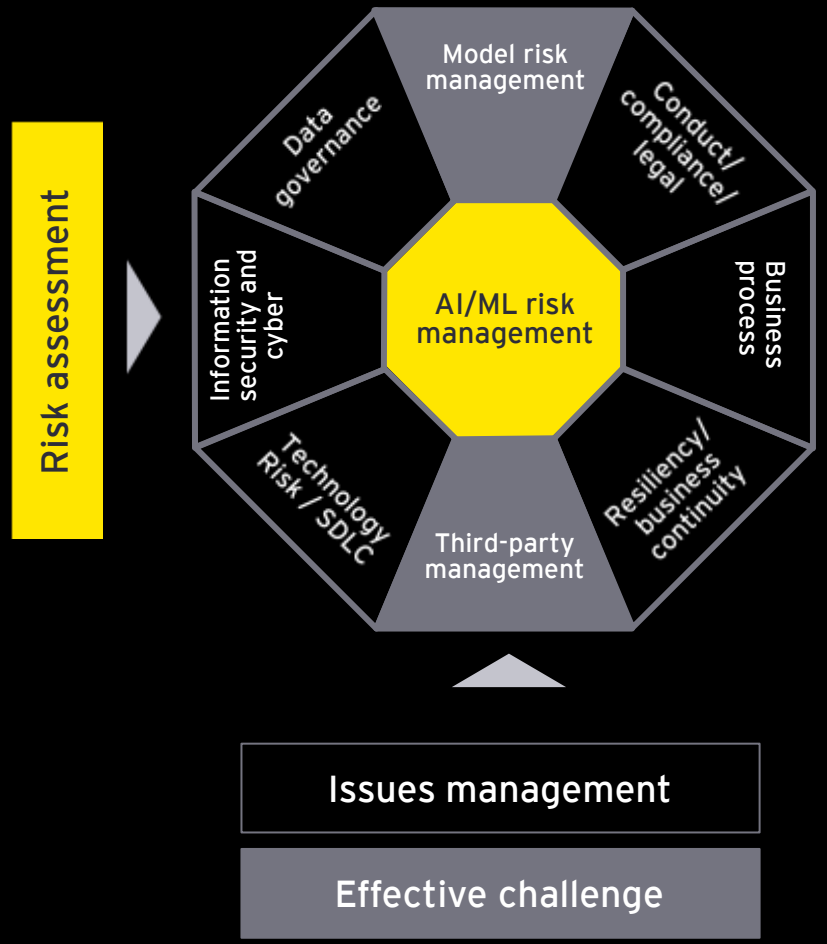
Managing risks through net new controls and legacy control readiness

Net new control activities

- Consistent AI definition
- Model risk tiering
- Model documentation
- Model inventory framework
- Ethics and privacy assessments
- Two lines of defense operating model (development and vetting)
- Ongoing monitoring and controls
- Human-in-the-loop
- Roles and responsibilities clearly defined

Cross-functional governance and control coverage for AI/ML

Key control principles establish the foundational controls for AI/ML agnostic to the underlying use case/technique



Key control principles	
1. Validation	**2. Verification**

▸ Assessing "fit-for-purpose"
  ▸ Conceptual soundness
  ▸ Explainability/transparency
  ▸ Benchmarking/sensitivity analysis/outcomes analysis
  ▸ Limitations and uncertainties
	▸ Implementation testing
	▸ System integration
	▸ Change controls
	▸ Data verification (accurate, complete and consistent)

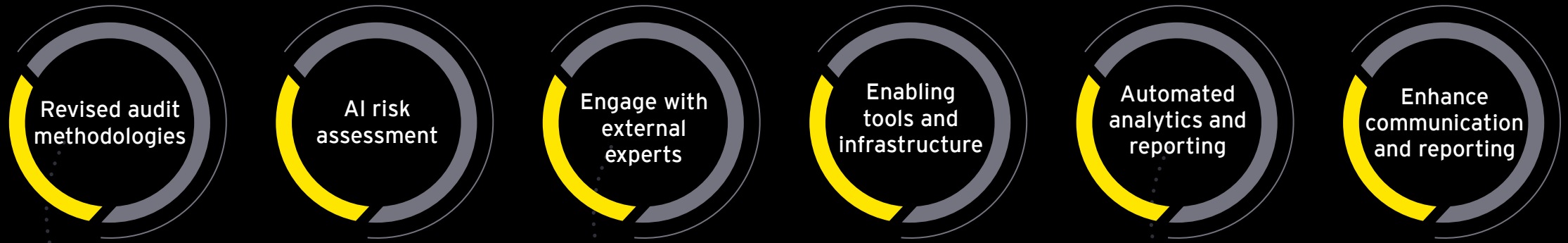
3. Preventive controls	**4. Operational resiliency/ stress testing**
▸ Kill switches/circuit breakers based on monitoring indicators and/or human assessment ▸ Embed preventive controls as part of design and implementation	▸ Business continuity and disaster recovery ▸ Cyber attack simulation/testing ▸ Resiliency testing and scenario analysis
5. Ecosystem Monitoring	**6. Human control/override**
▸ Automated and real-time monitoring based on KPIs/ KRIs ▸ Ongoing performance monitoring - outcomes analysis, benchmarking, accuracy, data drift	▸ Mechanism for humans to take control or override ▸ Understanding of monitoring indicators and failsafe mechanisms
7. Rules, regulations and laws	**8. Organization's code of conduct**
▸ Compliance with rules, regulations and laws	▸ Compliance with organization's code of conduct

4

Internal audit – key priorities and considerations

Internal Audit AI Readiness

Transforming internal audit for AI-driven complexity: new skills, strategic partnerships, and evolving roles



- Develop methodologies for auditing AI algorithms, including validation of model accuracy, fairness, and performance over time.
- Use scenario analysis to assess the impact of different risk scenarios on AI systems and incorporate these insights into audit plans.

- Early engagement with AI teams to understand objectives, design and potential risks
- Use structured AI Risk and Governance Assessment frameworks
- Regulatory Mapping
- Audit work-programs and playbooks
- Definition of risk, impact, KPIs and related performance metrices
- Facilitate joint risk assessment workshops for alignment and insights

- Collaborate with external experts, consultants, and industry groups to stay informed about the latest trends, best practices, and emerging risks in AI.
- Regularly benchmark IA practices against industry standards and leading practices to ensure continuous improvement and relevance.

- Utilize smart audit software with automated workflows; built in work-programs and playbooks; supporting automated testing and reporting
- Enhance reporting capabilities – interactive dashboards
- Introduce model evaluation tools and reports
- Integrate AI-powered tools into IA's own processes - predictive analytics for identifying emerging risks, automated risk assessment platforms, etc.

- Automated monitoring of action plans
- Customized report generation based on templates
- Deep dive into performance with visual analytics
- Trend analysis of past audits

- Enhance communication with functions like General Counsel's Office (GCO) and Engineering to stay updated on regulatory changes and ensure compliance.
- Form a cross-functional committee and hold regular meetings, or set up dedicated channels and reporting mechanisms.

Key Considerations – Skills Required

90% of organizations are investing in training to address AI-related talent gaps

Knowledge and skills

Auditing an AI application requires:

- Functional understanding of foundation models and AI capabilities
- Awareness of the AI lifecycle
- Skills to identify, evaluate and respond to AI risks
- Ability to identify process level risk arising from the use of AI and develop mitigation strategies
- Knowledge of best-in-class tools/techniques/frameworks/ assessments available for AI risk management
- Model tisk management; qualitative and quantitative assessment
- Knowledge of existing compliance requirements – privacy, SOX, etc.
- Application/cloud security, cyber resilience and BCP
- Experience with audit software and data analytics tools

Training needs

Additional trainings would be required to upskill traditional internal audit functions

Collaborate

Collaborate with specialists – data scientists, legal experts, etc., with the requisite knowledge, skill, and ability related to AI.

Seek external help from a third-party internal audit service provider.

Recruit

Recruiting where there is a skills shortage

AI Use Cases for Internal Audit

Processing

Process and synthesize information like human beings and in exceptional speed

1 Process walkthrough aggregator

Organize and structure audit process walkthrough notes and cross reference with regulations, policies, procedures, and control commentary to produce refined workpaper notes.

2 QA and methodology

Review audit workpapers for quality issues (language, formatting, and alignment with organizational standards), adherence to methodology, and general IIA standards.

3 Process, risk and control diagnostics

Review, assess and rationalize process, risk, control descriptions and linkage. Identify description deficiencies, duplicate controls to decommission, and thematic gaps.

Retrieval

Retrieves specific relevant information with contextual understanding

4 Audit planning

Generation of prioritized risk and control matrix, enriched with external forward-looking risk and threat guidance from authoritative sources (NIST, ISACA, DHS, etc)

5 Issue management

Automatically review, interpret and map issues to risk themes, and establish linkages to Product Risk Classification taxonomy and impacted regulation

6 Interpretation and summarization of unstructured data

Ingest, interpret and summarize governance, regulatory, contract (underwriting, vendor, etc.) documents to allow users to search contextually and summarize on-demand

New content

Generate new content by recognizing patterns across multiple sources

7 Business intelligence automation

Utilize natural language user prompts to automatically generate intuitive and insightful visualizations, charts, and summaries to present and communicate data. Provide quantified data support for areas of non-compliance.

8 CAE/Audit committee summary reports

Generate summary reports for CAE and audit committees using AI to interpret testing outcomes and existing monitoring routines, alongside semi-automated qualitative commentary on associated risks and controls.

9 Audit Report Drafting

GenAI automated first draft of audit report, utilizing workpapers, findings, conclusion, and qualified risk/control commentary, that also adheres to organization's report template for overall structure, length and methodology.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

ey.com/id

APPENDIX

How Can EY Help?

EY Internal Audit offerings

Internal audit strategy session:

- Alignment of internal strategy with client's strategy on AI
- Audit lifecycle scan for AI
- Use case development and priority
- Data and technical feasibility
- People agenda and AI skills assessment

Perform internal audit over the AI program:

- Enterprise readiness assessment
- AI governance audit
- Regulatory gap assessment
- Use case development, deployment and monitoring
- AI lifecycle audit
- AI change management audit

Internal audit use case:

- Facilitating workshops to build internal audit specific use cases including but not limited to information processing, information retrieval, and new content generation.

Internal audit team training:

- Customize the training content to the specific needs and operational context.
- Share a wealth of practical examples and case studies to illustrate various concepts, making the training relatable and impactful.
- Provide informed regulatory insight of the evolving AI-related compliance and regulatory landscape.
- Facilitate dynamic and interactive learning experiences, engaging participants and promoting deeper understanding.

Illustrative learning catalog:

- AI overview
- AI for internal auditors
- AI fraud considerations
- Prompt engineering
- IA use case demo
- AI risk management overview