



LEADERSHIP. ACTION. RESULTS.SM

JULY 2026

THE DUAL MANDATE FOR ASSURANCE – AI FOR IA AND IA FOR AI

ALVAREZ & MARSAL



AI IS CHANGING HOW ORGANIZATIONS MAKE DECISIONS

AI is no longer just a technology initiative—it is becoming a core **business capability** used **across functions**, processes, and decision-making. Organizations that succeed will be those that combine innovation with **strong governance, security, risk management**, and **responsible AI** practices.

Every assurance function is now being asked to modernize itself while providing confidence over enterprise AI.

THE DUAL MANDATE

Mandate One · AI for IA

MODERNIZING ASSURANCE

Using AI to make assurance broader, faster, continuous, and more predictive.

- Full-population testing
- Continuous monitoring
- AI-assisted investigations
- Automated evidence gathering
- Faster reporting

Business AI

Assurance

Internal Audit

Mandate Two · IA for AI

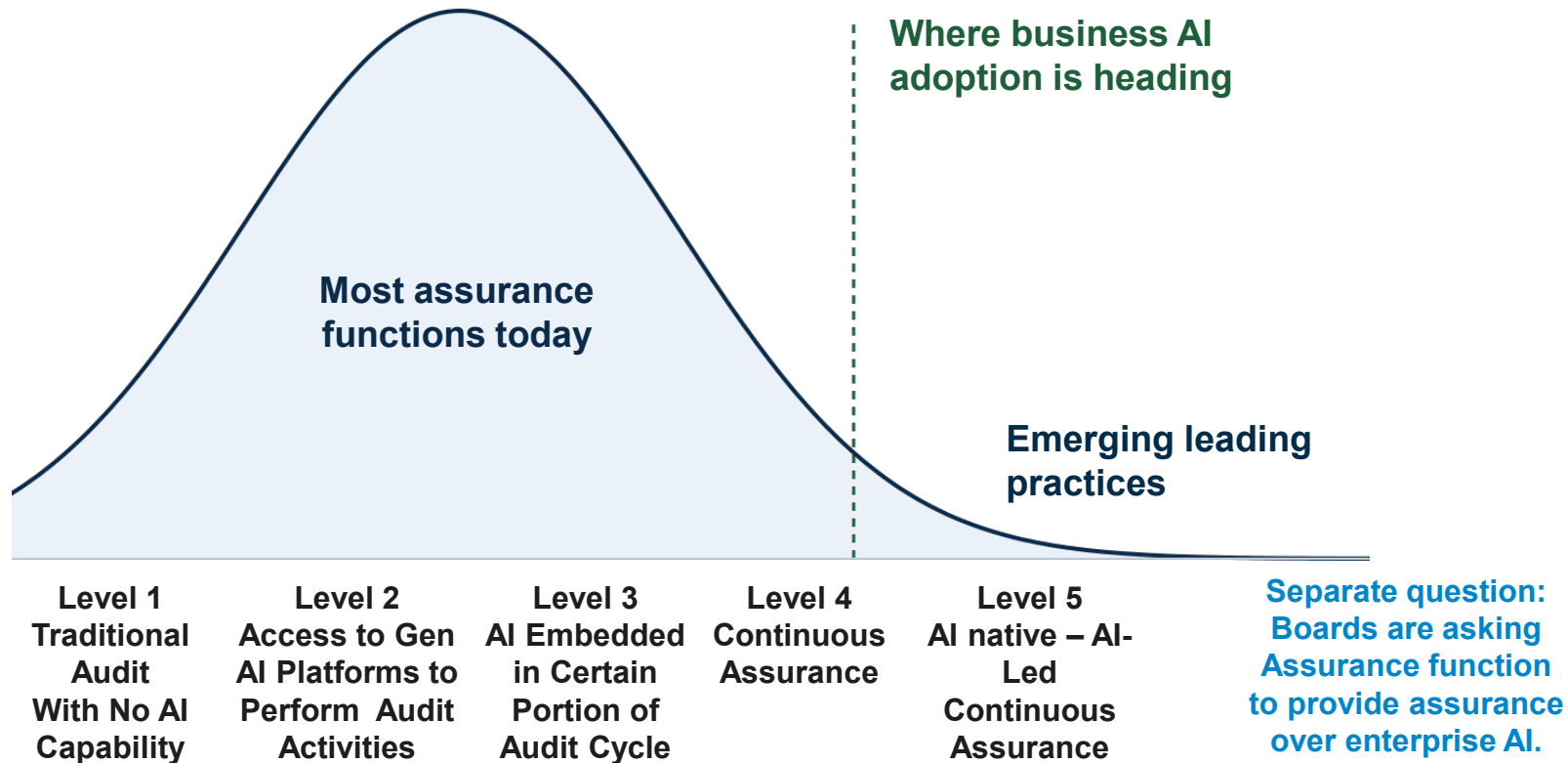
ASSURING ENTERPRISE AI

Providing independent confidence that AI is governed, trusted, secure, compliant, and responsible.

- AI inventory and risk classification
- Governance and accountability
- Model and data controls
- Regulatory compliance
- Board assurance

SETTING THE CONTEXT

WHERE DOES YOUR ASSURANCE STAND ON THE AI JOURNEY?



~39%

of assurance functions were using AI in 2025.

~80%

expected to be using AI through 2026.

46%

say their function adopts AI more slowly than the business it assures.

Source: IIA North American Pulse 2025

Every organization in this room sits somewhere on this journey. The objective this evening is to explore what it takes to move to the next stage, wherever you stand today.

WHY THE ASSURANCE GAP IS WIDENING

The pace, scale, and complexity of business risks are outstripping traditional assurance approaches. AI enables assurance to become broader, faster and more continuous, not just more efficient.

WHAT TRADITIONAL METHODS CAN COVER

- Sample testing
- Periodic audits
- Manual evidence collection
- Retrospective reviews
- Transactions assurance
- Human judgement

WHAT ASSURANCE MUST NOW COVER

- Exploding data volumes**
Full transaction populations, unstructured data, third-party platforms
- Machine speed decisions**
AI now acts inside credit, claims, pricing, and procurement in real time
- Expanding regulatory expectations**
The EU AI Act is phasing in now and India's frameworks are tightening
- Budget constraints**
Functions reporting cuts nearly doubled between 2024 and 2025, 11% to 19%
- AI-enabled fraud risk**
Fewer than 40% organizations feel prepared to detect AI-enabled fraud

AI-ENABLED ASSURANCE

- 100% population testing
- Continuous assurance
- AI-assisted evidence collection
- Predicting emerging risk
- Intelligent assurance
- Human judgement, augmented by AI

The widening gap between business risk and assurance capacity is redefining the role of Internal Audit. AI enables assurance teams to spend less time gathering evidence and more time exercising judgement.

BUILDING AN AI-ENABLED ASSURANCE FUNCTION

AI succeeds only when it is supported by trusted data, structured workflows, and strong governance.

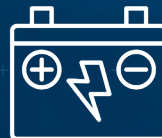
- 01 Trusted enterprise data**
Connected data, quality and lineage, standardized data models
- 02 Risk and control intelligence**
Risk library, control framework, process taxonomy, dynamic assessment
- 03 AI and analytics layer**
Predictive analytics, anomaly detection, generative and agentic AI

Intelligent Assurance

- 04 Workflow and case management**
Evidence repository, investigation workflows, issue lifecycle, audit trail
- 05 Human judgement**
Skepticism, materiality, context, challenge, and decision making
- 06 Governance and oversight**
AI governance, model monitoring, access controls, responsible AI

What accelerates adoption:

- Trusted enterprise data
- Executive sponsorship
- Standardized workflows
- AI-ready skills
- Integrated platforms
- Governance framework



What holds organizations back:

- Fragmented data
- Point solutions
- Skills gap
- Unclear ownership
- Change resistance
- Weak governance

AI is just one capability within the assurance operating model. Organizations that invest only in AI, without strengthening data, workflows, and governance, often struggle to realize sustainable value.

LESSONS LEARNED: OPERATIONAL PITFALLS IN AI JOURNEY

OBSERVED OPERATIONAL PITFALLS



No Clear Business Problem and Value Definition

Many organizations purchase AI platforms before defining measurable business outcomes, resulting in low adoption and limited business value.



Poor Quality Training Data and Legacy Silos

Incomplete, inconsistent, or biased data leads to inaccurate predictions, unreliable recommendations, and loss of stakeholder confidence.



Blind Trust and Lack of “Human-in-the-Loop” Oversight

AI should augment not replace human judgment. Organizations relying solely on AI outputs increase operational and regulatory risk.



Lack of Governance, Standards, and Accountability

Organizations often deploy AI faster than policies, standards, and accountability structures can mature.



No Continuous Monitoring, Testing, and Model Governance

AI models degrade over time due to changing data, business conditions, and evolving threats.



Weak Change Management and Adoption Readiness

Technology alone does not deliver value. Adoption depends on leadership commitment, employee trust, training, and responsible use.

STRATEGIC RECOMMENDATIONS



Define Clear Business Use Cases First

Define clear business use cases first, prioritize by value and feasibility, and then select the appropriate AI solution.



Establish Robust Data Governance

Establish robust data governance, including ownership, quality controls, lineage, metadata, and continuous monitoring.



Implement Human-in-the-Loop Reviews

Implement human-in-the-loop reviews, approval workflows, and escalation mechanisms for critical decisions.



Define Enterprise AI Governance

Define enterprise AI governance covering policies, ethics, model lifecycle management, security, privacy, and regulatory compliance.



Continuously Monitor Model Performance

Continuously monitor model performance, drift, bias, security events, and business outcomes, with periodic recalibration where required.



Invest in AI Literacy and Executive Sponsorship

Invest in AI literacy, executive sponsorship, communication, and organizational change management.



Assurance for AI

AI: FROM CONCEPT TO CORE BUSINESS STRATEGY

BFSI: Business Use Cases



Automated Underwriting:

AI models analyze applicant data and medical records to determine risk profiles without human intervention.



Customer Service Chatbots:

24/7 AI support driving 11% higher policy purchase rates.



Fraud Detection: Such as Claim Processing

Machine Learning (ML) algorithms identify fraudulent patterns in claims and applications with 60%+ improved accuracy.



Loan Processing:

Mortgage approval via automated verification.

AI: FROM CONCEPT TO CORE BUSINESS STRATEGY

Technology: Business Use Case



Automated Coding, Code Quality, and Security:

AI writes codes, checks quality, features, syntax, and security



R&D:

Product quality, validation, and feature enhancements



Workflow Automation:

Agentic AI automated workflows in projects



Product Engineering:

Faster designing, documentation, and architecture

AI: FROM CONCEPT TO CORE BUSINESS STRATEGY

Manufacturing: Business Use Case



Predictive Maintenance:

AI-driven ML predictive maintenance on critical production equipment using vibration/temperature sensors paired with ML models to flag imminent failures.



Quality Inspection:

AI Visual Quality Inspection (NxVAE) - unsupervised-learning variance autoencoder (VAE) that learns a "normal" appearance model from unlabeled images, then flags anything that deviates as a defect.



AI Enabled Cameras:

For security and anomaly detection.

BOARD EXPECTS ASSURANCE OF AI USE CASES TO FALL UNDER INTERNAL AUDIT



Board Oversight

Board of Directors · Risk Committee · Audit Committee

Sets AI risk appetite · approves framework · receives quarterly AI risk dashboard · escalation point for material incidents.

1st LINE OF DEFENCE

Own · Build · Operate

ROLES

- Business Functions
- AI Product Owners
- AI/ML Developers and Data Scientists
- IT & Engineering
- Operations
- All AI Users

Accountable for implementation to achieve value while managing day-to-day AI risks.

2nd LINE OF DEFENCE

Govern · Challenge · Monitor

ROLES

- Chief AI Officer (new)
- AI Ethics Committee
- Compliance
- AI Risk Office and Model Risk Management
- Privacy Office
- Legal and Ethics

Accountable for governance, risk management, and control oversight across the enterprise.

3rd LINE OF DEFENCE

Independent Assurance

ROLES

- Internal Audit
- External Auditors and Assessors
- Regulators
- Certification Bodies

Accountable for assurance, independent validation, and reporting.

NEW ROLES: Chief AI Officer · AI Governance Committee · AI Ethics Committee · AI Review Board.

SIX INTERLOCKING RISK DOMAINS THAT IA SHOULD REPORT TO BOARD

01

Model Risk

Reliability • Accuracy • Robustness

- Data source, quality, and lineage, continuous monitoring with alerts for performance degradation, feedback loops to identify concept drift
- SHAP (SHapley Additive exPlanations) values, interpretable ML models for high-risk decisions, clear documentation of model logic

Key Risks:

Inaccurate or
hallucinated outputs

Model drift and
performance decay

Overfitting and lack of
robustness

Inadequate testing and
validation

Lack of explainability

SIX INTERLOCKING RISK DOMAINS THAT IA SHOULD REPORT TO BOARD

02

Bias and Fairness

Equity • Non-discrimination • Inclusion

- Diverse data sourcing and balanced training sets
- Fairness metrics: Demographic parity, equality of odds
- Regular testing across protected classes

Key Risks:

Biased or unfair
outcomes

Disparate impact
across groups

Lack of representative
data

Unintended proxy
discrimination

Lack of bias testing
and mitigation

SIX INTERLOCKING RISK DOMAINS THAT IA SHOULD REPORT TO BOARD

03

Privacy and Data

Privacy • Data Protection • Confidentiality

- Data privacy identification, visibility, anonymization, classifiers
- Data residency, controls of encryption at source, runtime security

Key Risks:

Unauthorized data use
or leakage

Non-compliance with
privacy laws

Excessive data
collection

Inadequate consent
management

Cross-border data
transfer risks

SIX INTERLOCKING RISK DOMAINS THAT IA SHOULD REPORT TO BOARD

04

Security

Adversarial • Resilience • Integrity

- FIDO-2 MFA, LLM proxies
- Prompt injection defenses, and deepfake detection tools
- Conduct regular penetration testing

Key Risks:

Adversarial attacks and
data poisoning

Model theft and
IP leakage

Prompt injection and
jailbreaking

Insecure MLOps and
pipelines

Insider threats and
privilege abuse

SIX INTERLOCKING RISK DOMAINS THAT IA SHOULD REPORT TO BOARD

05

Third-Party and Concentration Risk

Dependency • Outsourcing • Ecosystem Risk

- Due diligence on AI providers
- Contractual protections for AI accountability
- Access to model documentation and audit trails

Key Risks:

Vendor concentration

Third-party model and
data quality

Inadequate due
diligence

Service disruption and
outages

Limited transparency
and visibility

SIX INTERLOCKING RISK DOMAINS THAT IA SHOULD REPORT TO BOARD

06

Compliance and Legal

Regulatory • Ethical • Accountability

- Documentation of AI practices
- Annual compliance reviews
- Alignment with NAIC AI principles and model bulletin requirements

Key Risks:

Non-compliance with AI
regulations

Lack of accountability and
auditability

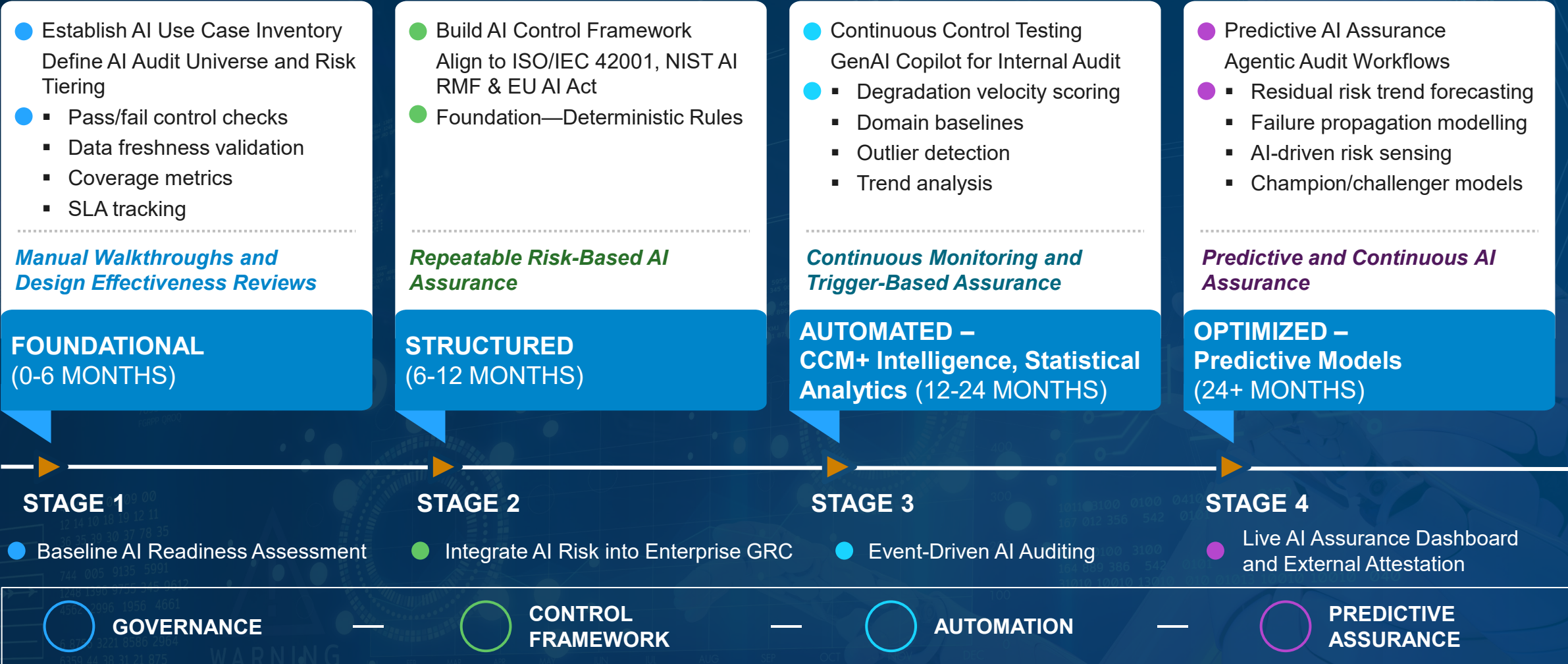
Intellectual property
infringement

Contractual and liability
exposure

Ethical violations and
reputational harm

AI INTERNAL AUDIT MATURITY ROADMAP (24+ MONTHS)

Maturity Journey



Internal Audit evolves from periodic compliance reviews to continuous, risk-driven AI assurance.

One **AI Risk, Security, Compliance, and Governance Hub**—integrate every point tool, accumulate logs and audit trails, **correlate for risk**, and deliver **predictive analytics and dashboards** to the Board.
