CherryHill ADVISORY

AI Part 2:

Building and Reviewing AI Governance

March 18 | 12 PM ET

www.cherryhilladvisory.com

Mike Levy

CIA, CRMA, CISA, CISSP, CDPSE, MBA

CEO & Managing Principal, Cherry Hill Advisory

Connect with Mike on LinkedIn

20+ years of experience in Internal Audit, Cybersecurity, and Risk Management

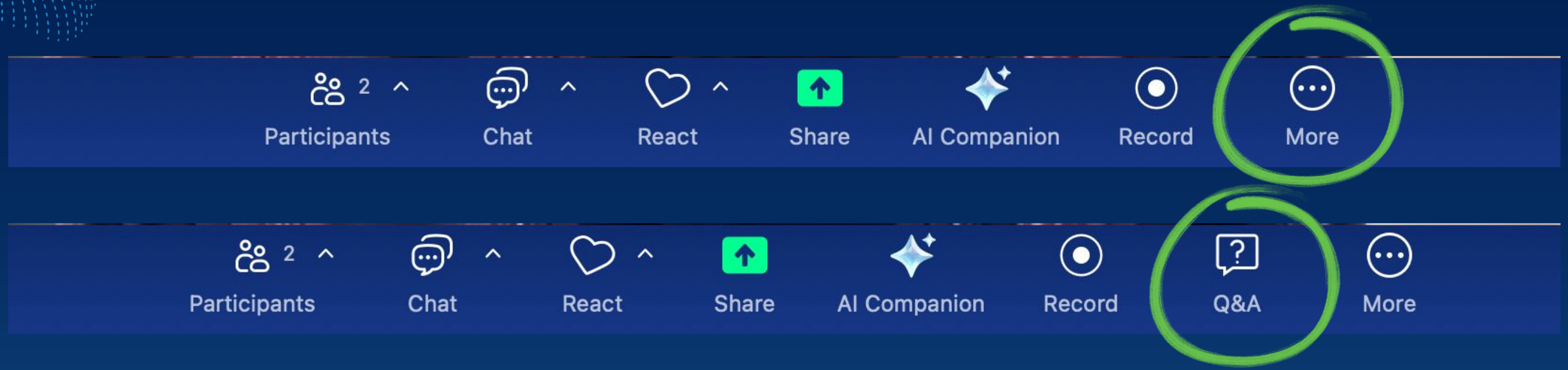
Former Chief Audit Executive and Deloitte Consultant

IIA´s International Internal Audit Standards Board Member

Past Chair (2023-2024), IIA Northern American Board; Global Board Director

Expert in aligning audit functions with evolving cyber risk landscapes

CherryHill ADVISORY



For your questions, the Q&A icon might show up in your screen. If not, you may find it by clicking the three dots with "More."

You have the option to ask anonymously.

AI PART 2:
Building and Reviewing AI Governance

THE PROGRAM WILL BEGIN MOMENTARILY.

CherryHill ADVISORY

NASBA CPE Requirement per CPE hour -

50 minutes of attendance, 3 poll questions

Certificates will be given mid next week or earlier.

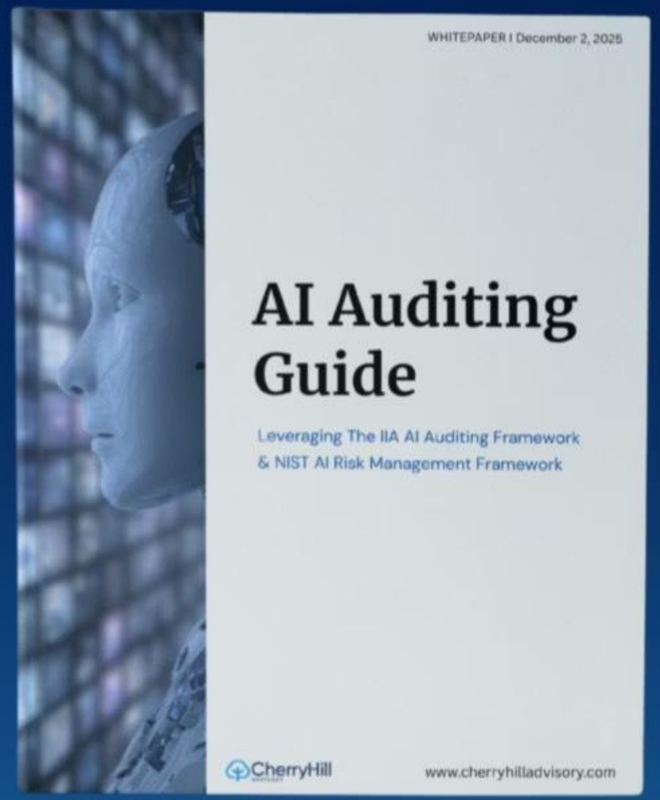
For any concerns, please email
cpe@cherryhilladvisory.com

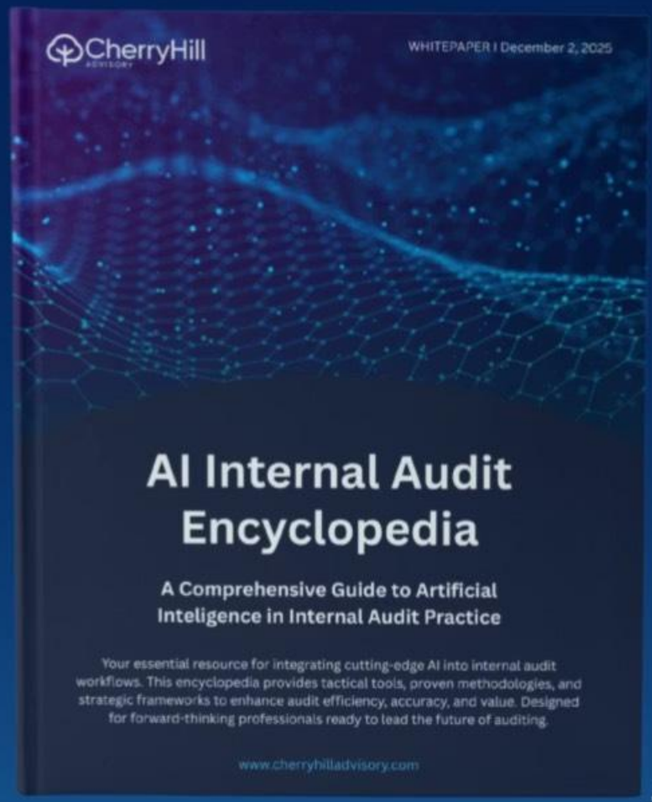
AI PART 2:

Building and Reviewing AI Governance

Resources for today – *Scan QR Code to download resources for free*

CherryHill ADVISORY





AI PART 2:

Building and Reviewing AI Governance

SESSION GOALS

Learning Objectives

Understand how AI oversight should work.

Review model approval steps and documentation.

Judge if governance is strong or missing key parts.

Why AI Governance Is the Next Critical Step

Building on Module 1

Module 1 identified AI risks. Now we focus on the governance layer that actively manages them.

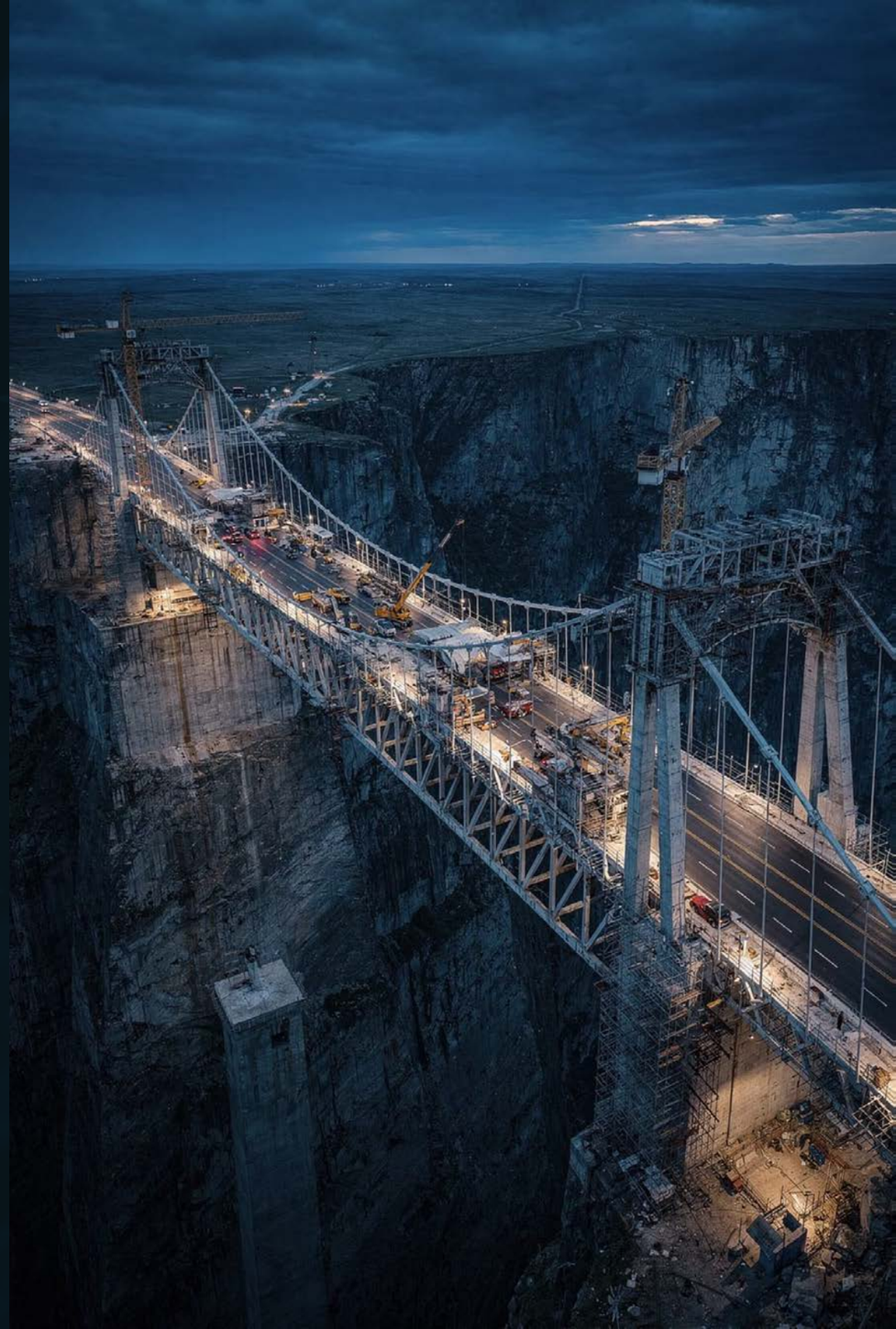
The Retrofit Problem

Governance frameworks are too often built after deployment. Regulatory expectations and stakeholder scrutiny are intensifying.

The Growing Gap

Internal audit must assess governance *effectiveness*, not just existence. This gap is one of today's most significant enterprise risks.

Source: Cherry Hill Advisory AI Auditing Guide (Governance & Controls; Audit Observations)



What We Mean by "AI Governance"

Who approves AI use?

Clear authority and approval gates before deployment

Who owns AI risk?

Named accountability for outcomes and impacts

Who reviews decisions?

Independent validation and challenge mechanisms

Who intervenes when issues arise?

Escalation paths and response protocols

Governance transforms abstract AI principles into concrete organizational accountability.

> AI governance establishes structured accountability, oversight, and control mechanisms to ensure AI systems operate in line with organizational objectives and risk tolerance.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance & Controls) [2] The IIA AI Auditing Framework (Governance & Oversight; Independent Assurance) [3] Cherry Hill Advisory AI Internal Audit Encyclopedia, p.5 (Governance & Oversight)

POLL QUESTION 1 OF 4

How Mature Is Your AI Governance?

Level 1 – Ad Hoc (no defined oversight)

Level 2 – Basic (policy exists but not implemented)

Level 3 – Managed (controls exist, governance not fully integrated)

Level 4 – Integrated (formal reviews, clear accountability)

Level 5 – Leading (continuous monitoring, governance by design)

Why AI Governance Often Breaks Down

Business-Led Adoption

AI tools deployed without central IT or risk involvement, creating visibility gaps and fragmented control environments.

Fragmented Ownership

Responsibilities split across IT, business units, data teams, and compliance, with no single accountable party.

Controls Added After Go-Live

Governance retrofitted post-deployment, when issues are harder and more expensive to remediate.

Limited Ongoing Monitoring

One-time approvals with no mechanisms to detect drift, misuse, or changing risk profiles over time.

> AI systems introduce unique risks including model drift, bias, and lack of transparency, which require continuous governance rather than one-time controls.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance & Controls; Practical Audit Findings) [2] The IIA AI Auditing Framework (Model Lifecycle Controls; Monitoring) [3] Cherry Hill Advisory AI Internal Audit Encyclopedia, p.6 (Bias, Transparency, Explainability)

Common Issues Identified in AI Governance Reviews

Lack of formal governance structure

No council or defined oversight body to guide AI initiatives.

Incomplete or outdated AI inventory

Organizations struggle to track all AI models in use, their purpose, and their risks.

Unclear ownership of AI systems and risks

Ambiguity over who is accountable for AI development, deployment, and outcomes.

Weak or inconsistent approval processes

AI models go live without rigorous review or adherence to established policies.

Limited or no post-deployment monitoring

Failure to continuously track AI performance, drift, and unexpected impacts after launch.

Insufficient documentation to support decisions

Lack of clear records for design choices, risk assessments, and model validation.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance & Controls; Practical Audit Findings) [2] The IIA AI Auditing Framework (Governance & Oversight; Model Lifecycle Controls)

Issue #1 – No Clear Governance Structure

- No formal AI governance council or oversight body.
- Lack of cross-functional representation (IT, risk, legal, audit).
- Decisions made inconsistently across business units.
- No centralized accountability for AI risk.

Without formal governance, AI oversight becomes fragmented and reactive.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance & Controls) [2] The IIA AI Auditing Framework (Governance Structure; Roles & Responsibilities)

Issue #2 – Incomplete AI Inventory

- Organizations cannot identify all AI systems in use (including shadow AI).
- Missing key attributes like business purpose, data sources, ownership, and risk classification.
- Inventory is not updated regularly, leading to an inaccurate view of AI landscape.
- No clear process for adding new AI systems to the inventory.

If you don't know where AI exists, you cannot govern it.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance Controls; Inventory Gaps) [2] The IIA AI Auditing Framework – Practitioner's Guide (AI Inventory / Model Inventory Controls)

Issue #3 – Weak Approval Processes

- “Pilot” systems move to production without formal approval.
- Approvals lack documentation or clear criteria.
- No consistent review gates before deployment.
- Business-driven deployments bypass governance.

Approval exists in theory, but not in practice.

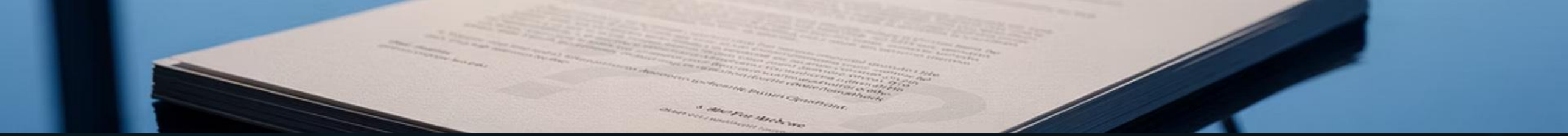
Source: [1] Cherry Hill Advisory AI Auditing Guide (Approval Processes; Governance Failures) [2] The IIA AI Auditing Framework (Model Approval & Validation Controls)

Issue #4 – No Ongoing Monitoring

- No tracking of model performance or drift.
- No monitoring of bias, fairness, or outcomes.
- No triggers for re-review or re-approval.
- Issues detected only after incidents occur.

AI risk changes over time, governance must too.

Source: [1] Cherry Hill Advisory AI Internal Audit Encyclopedia, p.53 (AI Model Performance Degradation) [2] NIST AI Risk Management Framework (Manage Function – Monitoring & Risk Response)



Issue #5 – Poor Documentation & Explainability

- Critical documentation is missing, including approval decisions, risk assessments, and testing results.
- Technical documentation exists but lacks clear business-level explanations for AI model functionality.
- Stakeholders struggle to understand AI system behavior, its purpose, or the rationale behind its outputs.
- No documentation trail to support audit or regulatory review.

No documentation = no accountability.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Documentation & Governance Controls) [2] Cherry Hill Advisory AI Internal Audit Encyclopedia, p.8, p.12 (Transparency; Explainability)

Roles in AI Oversight

Business Owner

Accountable for use case definition, outcomes, and business impact of AI deployment.

Data Owner

Responsible for data quality, lineage, access controls, and compliance with privacy requirements.

IT and Security

Ensures technical integrity, cybersecurity, infrastructure resilience, and access management.

Risk and Compliance

Validates risk assessments, regulatory alignment, and adherence to internal policies.

Legal or Privacy

Reviews contractual terms, intellectual property rights, and privacy law compliance.

Internal Audit

Provides independent assurance over governance design and operating effectiveness.

> Effective AI governance requires clear separation between risk ownership, oversight, and independent assurance to prevent conflicts of interest.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Roles & Responsibilities) [2] The IIA Three Lines Model [3] Cherry Hill Advisory AI Internal Audit Encyclopedia (Accountability; Governance Structure)

The Risk of Shared Ownership

Accountability Becomes Unclear

When everyone is responsible, no one is truly accountable. Shared ownership dilutes decision authority.

Decisions Fall Between Functions

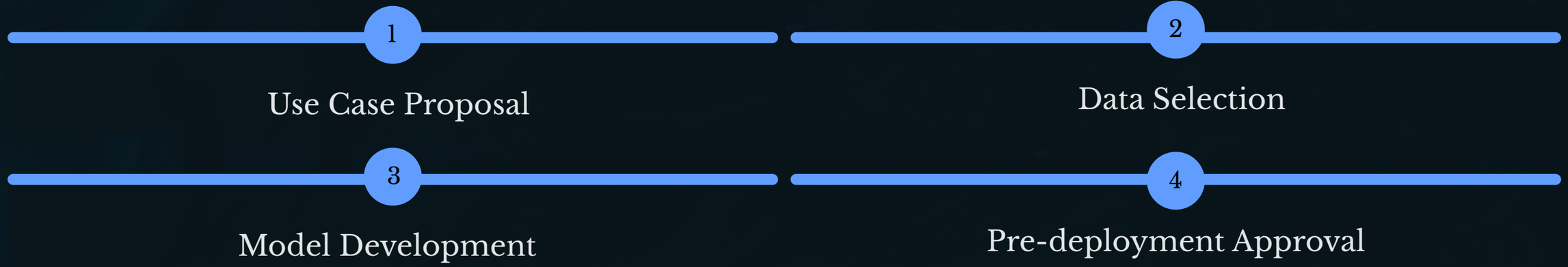
Critical judgments are deferred or avoided as teams assume another group will handle the issue.

Issues Surface Too Late

Without clear ownership, problems escalate undetected until they become material incidents or regulatory concerns.

Source: Cherry Hill Advisory AI Auditing Guide (Governance & Accountability Risks)

The AI Lifecycle: An Oversight Perspective [1]



Effective governance requires controls and decision points at every stage, not just at deployment. Each phase presents distinct risks requiring different oversight mechanisms.

> AI risk evolves across the lifecycle, from data selection and model development to deployment and ongoing monitoring.

Source: [1] NIST AI Risk Management Framework (AI RMF 1.0) [2] NIST AI Risk Management Framework (Map, Measure, Manage Functions) [3] Cherry Hill Advisory AI Internal Audit Encyclopedia, p.15 (Lifecycle Stages)

POLL QUESTION 2 OF 4

Where Are the Biggest AI Oversight Gaps?

- Use Case Approval
- Data Selection
- Pre-Deployment Review
- Post-Deployment Monitoring
- Not Sure

What Should Exist Before AI Goes Live

Defined Business Purpose

Clear articulation of what the AI will do and why it's needed.

Approved Data Sources

Documented origin, quality standards, and usage rights.

Risk & Impact Assessment

Evaluation of potential harms, bias, and operational risks.

Testing or Validation

Evidence that the model performs as intended.

Named Accountable Owner

A specific individual responsible for outcomes.

Without these elements, deployment should not proceed.

Key AI risks at this stage include data quality issues, embedded bias, and lack of model explainability.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Approval & Governance Controls) [2] Cherry Hill Advisory AI Internal Audit Encyclopedia, p.14, p.6, p.8 (Data Quality; Bias; Explainability) [3] Cherry Hill Advisory AI Internal Audit Encyclopedia, p.14 (Data Foundations for AI)

Common Approval Weaknesses

Informal or Rushed Approvals

"We needed it fast, so we skipped the formal process this time."

"Pilot" Systems Becoming Permanent

"It was just a test, but now it's running in production without official approval."

Little Documentation of Decisions

"Someone approved it, but we don't have a record of who or on what basis."

These patterns indicate governance in name only: policies exist, but adherence is optional.

Source: Cherry Hill Advisory AI Auditing Guide (Approval Process Failures)

Post-Deployment Oversight: The Forgotten Phase

Effective Governance Continues After Launch

01

Performance Monitoring

Track accuracy, fairness metrics, and business outcomes against baseline expectations

02

Review for Drift or Misuse

Detect model degradation, unintended applications, or changes in data patterns

03

Re-Approval When Use Changes

Require governance review if scope, data, or business context evolves

> AI models can degrade over time due to model drift, requiring continuous monitoring and periodic revalidation.

Source: [1] Cherry Hill Advisory AI Internal Audit Encyclopedia, p.53 (Model Performance Degradation)[2] NIST AI Risk Management Framework (Manage Function)

POLL QUESTION 3 OF 4

The Reality of AI Monitoring

How is AI performance monitored after deployment in your organization today?

- Continuous monitoring
- Periodic review
- Informal feedback
- Not monitored
- Not sure

Key Governance Documents Auditors Should Expect

AI Governance Policy	AI Inventory / Registry	Approval Records
Defines roles, approval gates, risk appetite, and escalation procedures.	Comprehensive list of all AI systems, owners, risk ratings, and status.	Documentation of who approved each system, when, and on what basis.
Model Documentation	**Monitoring Evidence**	**AI Governance Platforms**
Purpose, data sources, testing results, and limitations.	Logs, dashboards, or reports demonstrating ongoing oversight.	Tools automating lifecycle tracking, model monitoring, and compliance dashboards.

Effective documentation supports transparency, traceability, and explainability of AI decisions.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance Documentation) [2] The IIA AI Auditing Framework (Governance & Lifecycle Documentation Controls) [3] Cherry Hill Advisory AI Internal Audit Encyclopedia (Transparency; Explainability)

The AI Inventory as a Foundational Control

A robust AI inventory is more than a list, it is a **living control** that enables risk-based oversight.

Without an inventory, governance is reactive and incomplete.

Where AI Is Used

Business function, process, and geography

What Data It Relies On

Sources, sensitivity, and quality

What Decisions It Influences

Impact on customers, employees, or operations

Who Owns It

Accountable party and support teams

Relative Risk Level

Inherent and residual risk classification

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance Controls) [2] The IIA AI Auditing Framework (AI Inventory / Model Registry Controls)

What Auditors Should Watch For with AI Governance Tools

Vendor Claims vs. Reality

Tools may promise comprehensive governance but deliver narrow functionality. Test whether the tool addresses your organization's specific risks.

Integration and Data Quality

Governance tools are only as good as the data fed into them. Incomplete inventories or bypassed workflows create false assurance.

Tool Governance Itself

Who approves changes to the governance platform? The tool managing AI risk must itself be governed and auditable.

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance Tools & Risks) [2] The IIA AI Auditing Framework (Control Environment & Oversight)

AI Governance Tools in Practice

Organizations are turning to specialized platforms to manage AI at scale, automating what used to be manual spreadsheet tracking.

These tools strengthen governance but introduce new dependencies auditors should understand.

Model lifecycle management platforms tracking development, approval, and deployment

Responsible AI toolkits testing for bias, fairness, and explainability

AI-specific testing tools

Integrated platforms combining inventory, risk assessment, and monitoring

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance Tooling) [2] The IIA AI Auditing Framework (Responsible AI & Monitoring Controls)

Documentation vs. Explainability

1

Technical Documentation Alone Is Not Enough

Data scientists can document model architecture and training methods, but this does not help business leaders or auditors understand what the AI actually does or why it matters.

2

Governance Requires Business-Level Explainability

Effective oversight depends on clear, non-technical answers: What problem does this solve? What decisions does it make? What could go wrong? Who is affected?

Trustworthy AI demands transparency for all stakeholders.

> Explainability ensures stakeholders can understand how and why AI-driven decisions are made, not just how models are built. [2]

Source: [1] Cherry Hill Advisory AI Auditing Guide (Documentation Practices) [2] Cherry Hill Advisory AI Internal Audit Encyclopedia, p.8, p.12 (Transparency; Explainability)

How to Evaluate Governance Effectiveness

Stronger Governance

Clear Accountability

Named owners with defined responsibilities [1]

Repeatable Approvals

Consistent process with documented gates [1]

Ongoing Monitoring

Evidence of active oversight post-deployment [2]

Evidence of Challenge

Questions raised and addressed before approval [2]

Weaker Governance

Policies Without Operation

Documents exist but aren't followed in practice [1]

One-Time Approvals

No subsequent review or re-validation [1]

Unclear Ownership

Shared or rotating responsibility [2]

No Challenge Function

Rubber-stamp approvals without scrutiny [2]

Source: [1] Cherry Hill Advisory AI Auditing Guide (Governance Evaluation Criteria; Governance & Controls; Operating Effectiveness Gaps*) [2] The IIA AI Auditing Framework* (Governance & Oversight; Independent Assurance / Challenge Mechanisms)

POLL QUESTION 4 OF 4

Recognizing Governance Red Flags

Which signal most strongly suggests weak AI governance at an organization?

- No AI Policy Exists
- No AI Inventory Maintained
- Limited or Missing Documentation
- No Post-Deployment Monitoring
- All of the Above

Each red flag is concerning, but the combination indicates **systemic governance failure**.

How Internal Audit Adds Value

Testing Governance Design and Operation

Assess whether controls are properly designed and actually functioning as intended.

Clarifying Ownership and Accountability

Identify gaps where responsibilities are unclear or improperly assigned.

Escalating Gaps Before Issues Arise

Provide early warning to leadership about governance weaknesses before they become incidents.

Evaluating AI Governance Tools

Assess whether platforms actually strengthen controls or create new risks and dependencies.

Source: Cherry Hill Advisory AI Auditing Guide (Role of Internal Audit)

How to Audit AI Governance

Auditing AI governance does not require technical expertise, it requires the same disciplined inquiry applied to any governance structure: **Does it exist? Is it designed well? Does it actually work?**

- Confirm Controls
- Evaluate Roles
- Test Approvals
- Assess Monitoring

Source: Cherry Hill Advisory AI Auditing Guide (Audit Approach)

Audit Steps in Detail

01

Confirm Foundational Controls Exist

Request the AI governance policy, inventory, and approval records. If these cannot be produced, document the gap.

02

Evaluate Role Clarity

Map the Three Lines. Identify who owns each AI system, who set policies, and who provides independent oversight.

03

Test the Approval Process

Sample AI systems from the inventory. Assess whether approvals were formal, timely, and evidence-based.

04

Assess Post-Deployment Monitoring

Request monitoring reports or dashboards. Evaluate whether thresholds exist and exceptions are escalated.

05

Report

Assess governance as strong, needs improvement, or inadequate. Report to the Audit Committee with actionable recommendations.

Source: The IIA AI Auditing Framework (Audit Methodology; Governance Assessment)

How This Fits Into Existing Audit Work

In Module 1, we learned to identify AI risks in plain language. Now we're examining the governance structures that manage those risks.

AI governance doesn't exist in isolation, it intersects with established audit domains:

IT Governance

System development lifecycle, change management, access controls

Data Governance

Data quality, lineage, privacy, and retention policies

Third-Party Risk

Vendor due diligence, contractual protections, ongoing monitoring

Enterprise Risk Management

Risk identification, assessment, mitigation, and reporting

Integrate AI considerations into existing audit programs rather than treating it as entirely separate.

Source: Cherry Hill Advisory AI Auditing Guide (Integration into Audit Programs)

Tools for Developing & Reviewing AI Governance

AI Governance Policy Template

Defines roles, risk appetite, approval gates, and escalation procedures to establish a formal governance structure.

AI Inventory / Registry

Centralized inventory of all AI systems, including ownership, purpose, and risk classification to support oversight and auditability.

AI Approval Records Template

Documents who approved each AI system, when, and on what basis, creating auditable evidence of governance decisions.

AI Model Documentation Template

Captures business purpose, data sources, testing results, and limitations to support transparency and explainability.

AI Monitoring Evidence Tracker

Tracks performance, drift, incidents, and ongoing oversight activities to ensure governance continues post-deployment.

AI Governance Platforms Evaluation Tool

Compares governance tools (e.g., monitoring, bias testing, lifecycle management) to support tool selection and implementation.

AI Part 2 Resource Pack

Scan QR Code to download for free

AI Resource Pack

This pack includes all of the **templates and tools shared during our AI Part 2 session**. These resources are designed to help you implement what we covered and start using AI more effectively in your day-to-day work.

For the best experience, we recommend viewing and editing these files in **Google Docs** and **Google Sheets**.

Key Takeaways

AI governance is about oversight, not technology.

You are evaluating decision-making processes, not algorithms.

Approval and monitoring are critical control points.

Strong governance requires clear gates before deployment and ongoing oversight after.

Documentation is what enables accountability.

If decisions are not recorded, they cannot be challenged or audited.

You do not need technical depth to assess governance.

Focus on process, roles, and evidence, not the model itself.

Next Steps

1

Immediate Actions

- Review or build your AI inventory.
- Assess current approval processes and identify gaps.
- Evaluate post-deployment monitoring.
- Clarify ownership for high-risk AI systems.

2

Building Capability

- Train audit teams on AI governance fundamentals.
- Integrate AI into existing audit plans.
- Develop AI-focused audit procedures.
- Strengthen relationships with AI owners and risk functions.

CherryHill ADVISORY

LEARNING NEVER STOPS

UPCOMING CPE WEBINARS, REGISTER FOR FREE

AI PART 2:

Building and Reviewing AI Governance

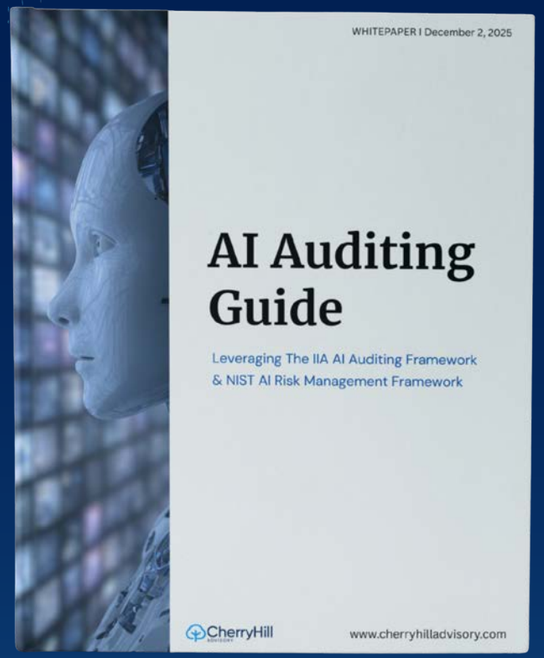
Resources

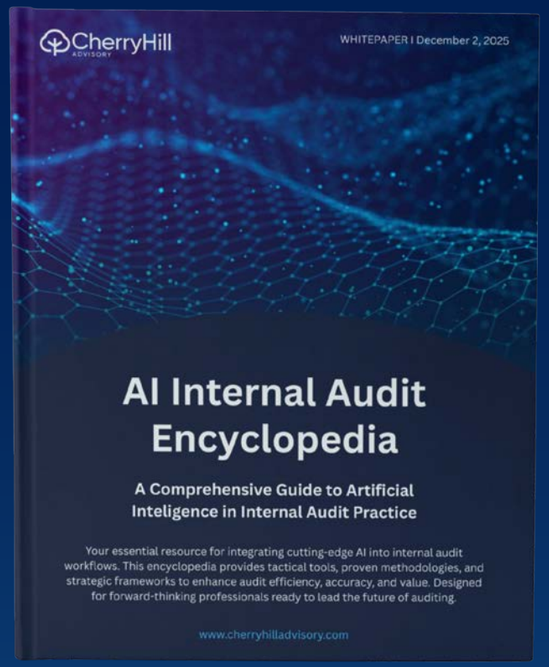
Scan QR Code to download **resources** for free

AI PART 2:

Building and Reviewing AI Governance

CherryHill ADVISORY





The IIA's AI Auditing Framework

The IIA's Three Lines Model

NIST AI Risk Management Framework (AI RMF 1.0)

CherryHill ADVISORY

AI PART 2:

Building and Reviewing AI Governance

Question & Answer

Thank you! Don’t forget to connect with me on

LinkedIn