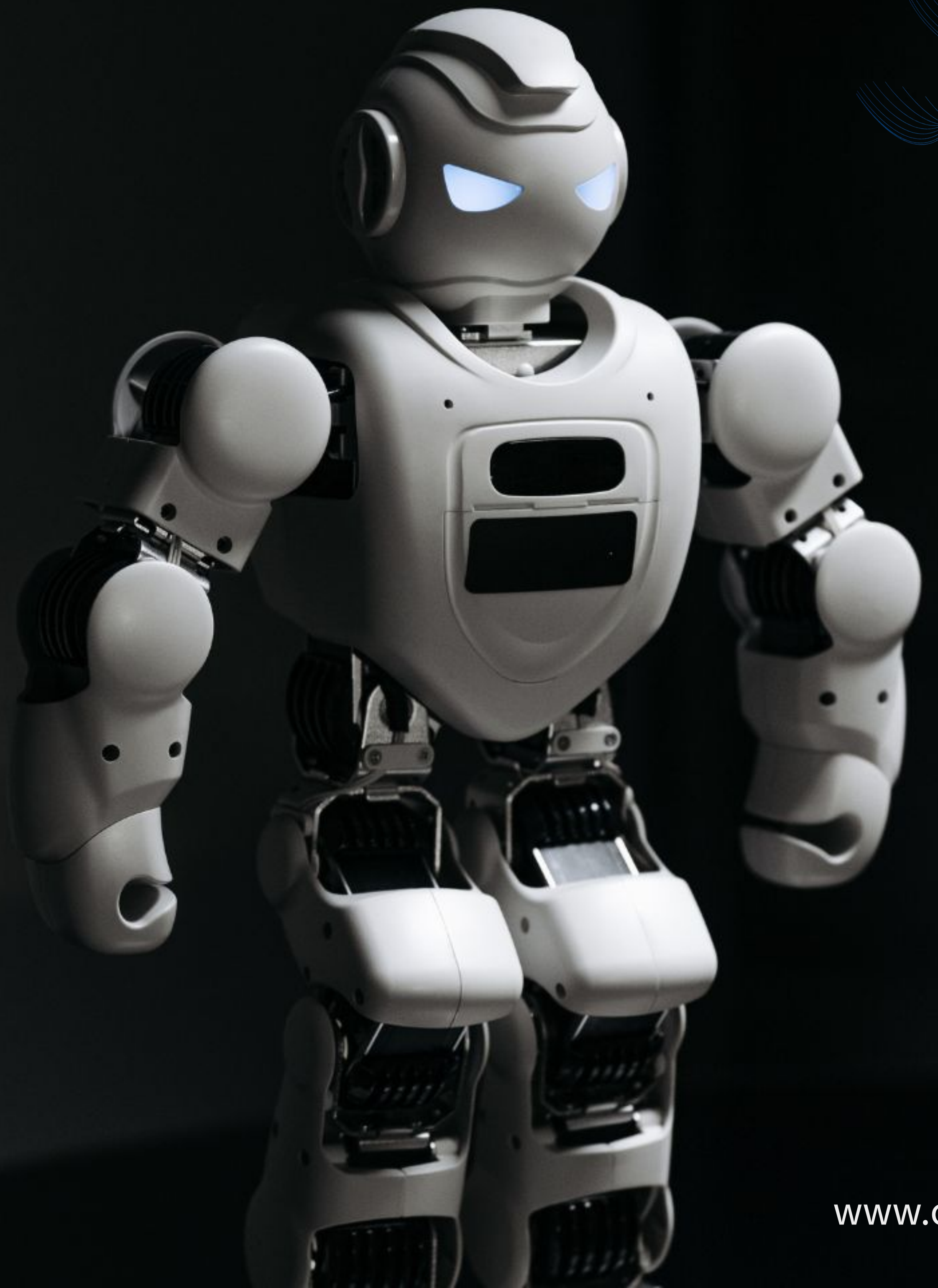
CherryHill
ADVISORY

Risk Radar 2026

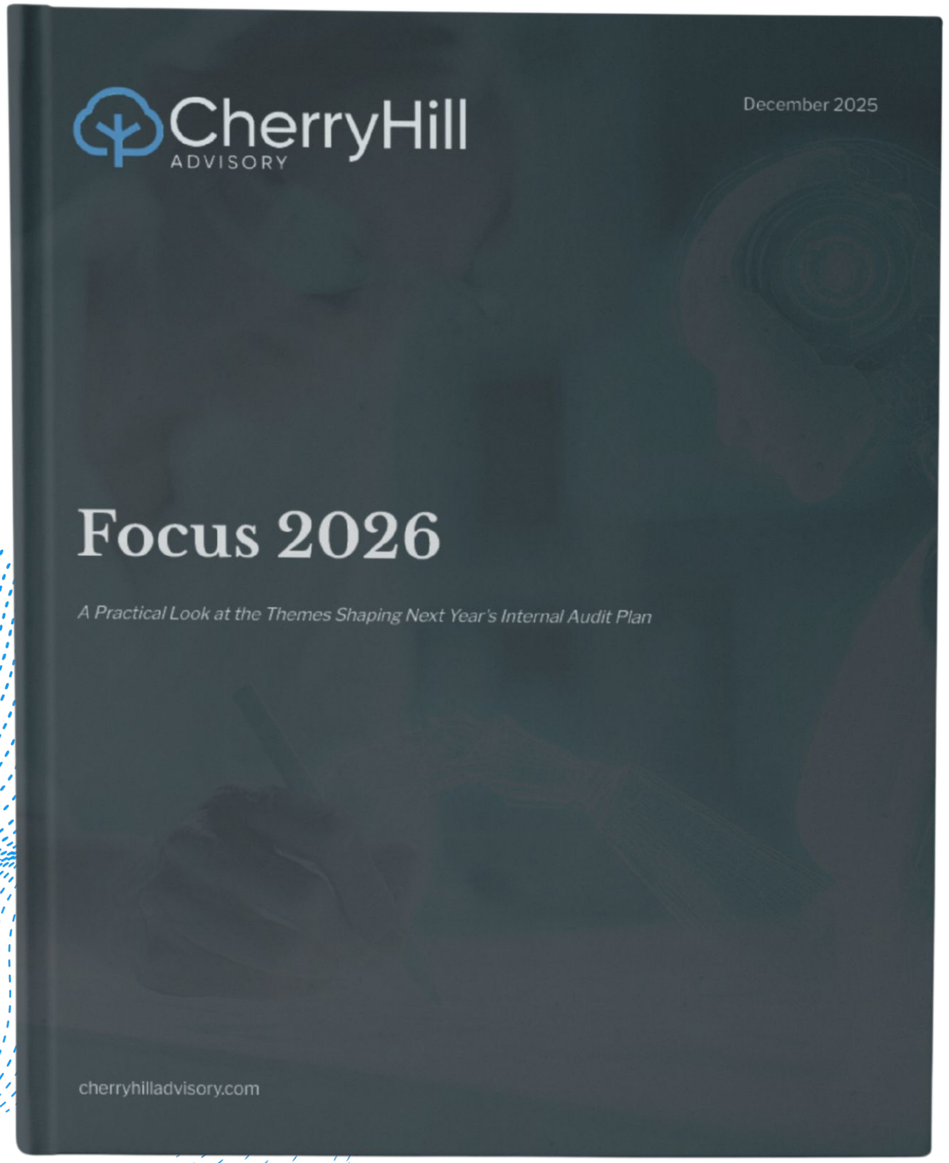
What Internal Audit Should Keep on the Top of Mind This Year

January 21 | 12 PM ET



www.cherryhilladvisory.com

Resources


CherryHill
ADVISORY
December 2025
Focus 2026
A Practical Look at the Themes Shaping Next Year's Internal Audit Plan
cherryhilladvisory.com

A Practical Look At The Themes Shaping Next Year's Internal Audit Plan

Scan QR Code to download **Focus 2026** for free

Mike Levy

CIA, CRMA, CISA, CISSP, CDPSE, MBA

CEO & Managing Principal, Cherry Hill Advisory

20+ years of experience in internal audit, cybersecurity, and risk management

Former Chief Audit Executive and Deloitte consultant

Expert in aligning audit functions with evolving cyber risk landscapes

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

IIA's International Internal Audit Standards Board Member

CherryHill
ADVISORY

NATIONAL REGISTRY OF CPE SPONSORS

CPE INFORMATION

To receive your CPE certificate, please ensure your screen name displays your full name. This is required for proper documentation and certificate issuance.

Certificates will be emailed within 5-7 business days from today's date to the email address you used during registration. Please allow adequate time for processing and check your spam folder if you don't see it in your inbox.

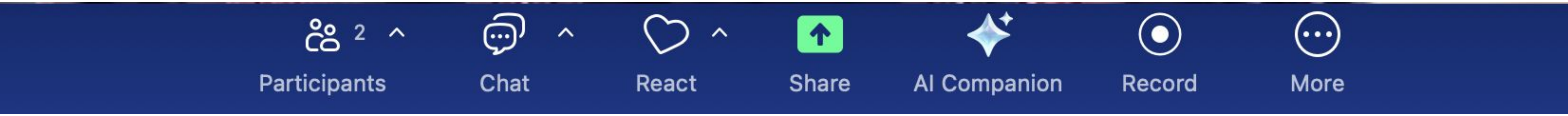
For any CPE related questions email cpe@cherryhilladvisory.com.

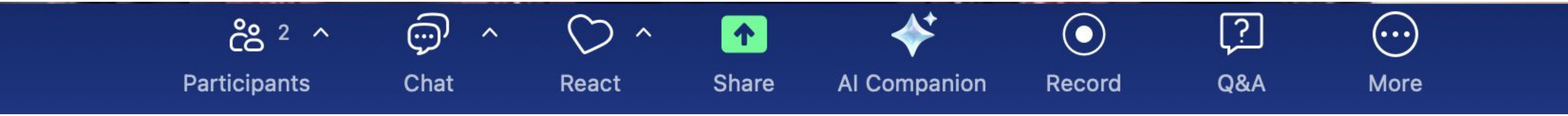
Make sure to stay engaged USING THE POLLING QUESTIONS REQUIRED throughout the entire session to qualify for the full CPE credit hours.

Meet interactive requirements: Answer a *minimum* of three poll questions per credit hour.

CherryHill
ADVISORY

Questions and Answers





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.

What You Will Take Away

This session delivers actionable insights to strengthen your 2026 audit planning and elevate your strategic value to the organization.

Risk Velocity

Understand why the pace of risk change is accelerating and what it means for audit responsiveness and planning cycles.

Priority Risks

Identify which emerging and evolving risks demand immediate audit attention and resource allocation in 2026.

Shifting Expectations

Recognize how audit committee and stakeholder expectations are evolving toward forward-looking insights and strategic relevance.

Planning Actions

Gain practical steps to refine your audit approach, improve stakeholder dialogue, and enhance audit plan flexibility.

Agenda

01

The 2026 Risk Environment

Explore the forces driving increased risk velocity and complexity in modern organizations.

02

Major Enterprise Risk Areas

Deep dive into eight critical risk domains that will shape audit priorities over the next 18 months.

03

Audit Planning Implications

Translate risk insights into practical planning decisions and resource allocation strategies.

04

Audience Polling and Discussion

Interactive segments to gauge perspectives, share experiences, and explore common challenges.

05

Key Takeaways

Actionable recommendations you can implement immediately to strengthen your 2026 audit approach.

Why 2026 Is Different

The Risk Environment Has Changed

World Economic Forum, Global Risks Report 2025
Gartner, Top Risks for Internal Audit Leaders (2024)
Deloitte, Global Risk Management Survey (2024)

Accelerated Business Cycles

Technology innovation, market disruption, and competitive pressures are compressing strategic planning horizons. What once took years now unfolds in quarters, leaving less time to identify and respond to emerging risks.

Interconnected Operations

Organizations operate through complex ecosystems of third parties, cloud platforms, and integrated systems. A failure in one node can cascade rapidly across the enterprise, amplifying impact and reducing response time.

Regulatory Intensity

Regulators are expanding scope, increasing enforcement activity, and demanding more proactive risk management. The cost of non-compliance, financial, reputational, and operational continues to rise.

Zero Tolerance for Failure

Stakeholders, customers, and boards expect organizations to anticipate and prevent failures rather than react after the fact. The margin for error has effectively disappeared in many risk areas.

Audit Committee Expectations

Institute of Internal Auditors – North American Pulse of Internal Audit
NACD – Audit Committee Agenda

What Boards Are Asking For

Early Risk Visibility

Boards want to hear about emerging risks before they materialize into issues. Internal audit is expected to provide early warning signals, not post-mortem analysis.

Plain Language Insights

Technical audit findings must translate into clear business implications. Boards expect concise, actionable communication that drives decision-making.

Clear Prioritization

Audit committees are increasingly skeptical of comprehensive multi-year plans. They want focused, risk-based coverage that addresses what matters most right now.

Forward-Looking Perspective

Historical compliance reporting is table stakes. The real value comes from helping the board understand what risks are on the horizon and how prepared the organization is to address them.

Enterprise Risk Landscape Overview

IIA · NIST · World Economic Forum · Gartner · ACFE

Key Risk Areas for 2026

The following eight risk domains represent the most significant challenges facing organizations as they plan for 2026. Each area demands specific audit attention, skilled resources, and tailored methodologies.

AI and Automation

Rapid deployment of artificial intelligence in critical business processes with immature governance frameworks.

Data Quality and Governance

Poor data integrity undermining decision-making, reporting accuracy, and regulatory compliance.

Regulatory Compliance

Expanding regulatory expectations with principles-based requirements demanding judgment and interpretation.

Fraud in Digital Environments

Sophisticated social engineering and payment fraud schemes exploiting remote work and digital channels.

Cybersecurity and Third Parties

Expanding attack surfaces through vendor relationships, cloud services, and interconnected systems.

Technology Debt and Transformation

Legacy systems constraining innovation while digital transformation initiatives introduce new complexity.

Geopolitical and Supply Chain

Trade tensions, sanctions, and disruption forcing organizations to rethink efficiency-first operating models.

Strategic and Business Model Risk

Untested strategy assumptions and competitive shifts that can emerge slowly but accelerate rapidly.

POLL #1

How Fast Are Risks Changing?

> Question: How would you describe the pace at which key risks are changing in your organization?

A. Mostly Stable

Our risk profile remains relatively consistent year over year with predictable changes.

B. Gradual Change

We see steady evolution in our risk landscape that we can plan for and manage proactively.

C. Rapid Change

Significant shifts are occurring frequently, requiring continuous monitoring and adjustment.

D. Constant Change

Our risk environment is in perpetual flux with new threats emerging continuously.

E. Unsure

We lack sufficient visibility into the pace of risk change across our organization.

Discussion Point: What this means for audit planning, organizations experiencing rapid or constant change must adopt more flexible, continuous planning approaches rather than annual cycles.

NIST AI Risk Management Framework
EU Artificial Intelligence Act
IIA – Auditing Artificial Intelligence

Artificial Intelligence Risk

Why AI Is a Core Audit Topic

Artificial intelligence has moved from experimental use cases to mission-critical business applications at remarkable speed. Organizations are deploying AI for credit decisions, fraud detection, customer service, hiring, pricing, and countless other functions, often without fully understanding the risks involved.

Embedded Decision-Making

AI systems are making or influencing decisions that directly affect customers, employees, and business outcomes, often with limited human oversight.

Speed Over Control

Competitive pressure drives rapid AI deployment, frequently outpacing the development of appropriate governance, testing, and monitoring controls.

Unclear Accountability

Organizations struggle to define who owns AI risk, IT, business units, data science teams, or risk functions, leading to gaps in oversight.

Regulatory Attention

Regulators worldwide are establishing AI governance expectations, with enforcement actions beginning to emerge for discriminatory or unexplained AI outcomes.

AI Risk: Audit Insights

What We Commonly See

Internal audit teams examining AI governance consistently encounter similar gaps across industries and organization types. These patterns represent significant exposure that audit committees should understand.

No Complete AI Inventory

Most organizations cannot produce a comprehensive list of where AI is deployed, what data it uses, or what decisions it influences. Shadow AI, tools adopted by business units without IT or risk oversight, compounds this challenge.

Limited Model Oversight

AI models often lack ongoing performance monitoring, bias testing, or validation processes. Once deployed, many systems operate with minimal scrutiny until a problem surfaces publicly.

Weak Documentation and Explainability

Organizations struggle to explain how AI systems reach conclusions, making it difficult to identify errors, defend decisions to regulators, or maintain stakeholder trust. Documentation is frequently incomplete or technical rather than business-focused.

Inconsistent Monitoring Over Time

Even when initial controls exist, ongoing monitoring often degrades. Model drift, data quality changes, and evolving business contexts can silently erode AI effectiveness and safety without detection.

Cybersecurity and Third-Party Risk

One Ecosystem, Many Entry Points

NIST Cybersecurity Framework 2.0
IBM – Cost of a Data Breach Report
CISA – Supply Chain Risk Guidance

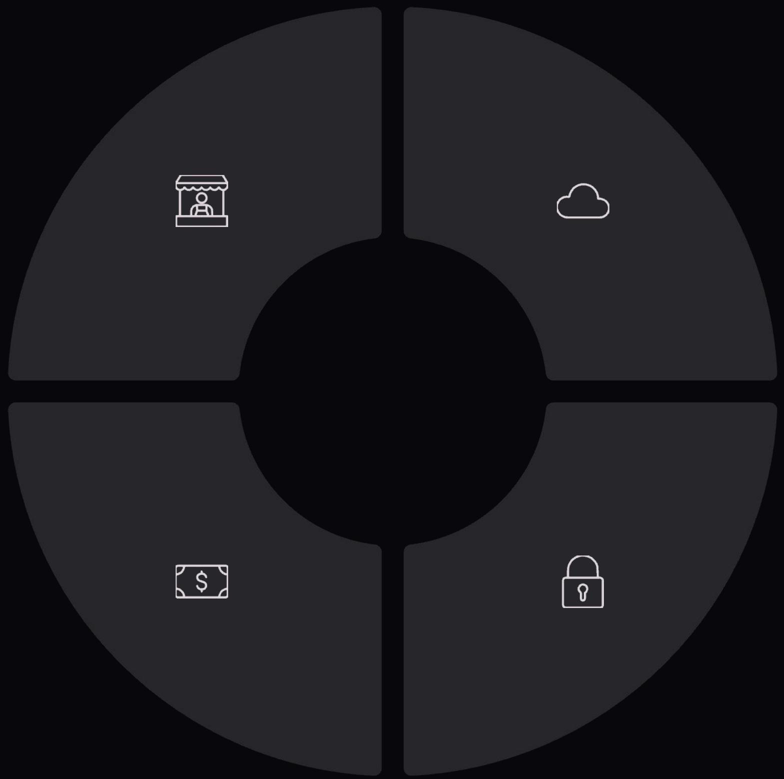
Modern organizations operate through extended ecosystems where boundaries between internal systems and external partners have largely dissolved. This interconnection creates efficiency and capability but also introduces vulnerability at every connection point.

Vendor-Driven Breaches

High-profile breaches increasingly originate from third-party vendors with access to sensitive systems or data, making vendor security a direct organizational risk.

Financial and Reputational Impact

Cyber incidents generate direct costs through response, recovery, and remediation, plus indirect costs through customer attrition, regulatory fines, and long-term brand damage.



Cloud and API Exposure

Cloud migration and API integrations expand the attack surface, with misconfigurations and weak access controls creating unexpected vulnerabilities.

Ransomware and Disruption

Ransomware attacks have evolved from nuisance to existential threat, capable of shutting down operations, corrupting data, and destroying stakeholder confidence.

POLL #2

Where Is Audit Attention Most Needed?

> Question: Which technology-driven risk area requires the most attention in your audit plan today?

A. AI and Automation

Governance, testing, and monitoring of artificial intelligence systems and automated decision-making.

B. Cybersecurity and Third Parties

Vendor security, incident response, and protection against external threats and breaches.

C. Data Quality and Governance

Data integrity, ownership, and controls supporting critical reporting and decision-making.

D. Technology Debt

Legacy system risks, digital transformation execution, and integration challenges.

E. Not a Primary Focus

Technology risks are not currently a primary area of concentration for our audit plan.

Discussion Point: Resource concentration and trade-offs, most audit teams cannot cover all technology risks comprehensively. How are you prioritizing among competing demands?

Cyber and Third-Party Risk: Audit Focus

What Audit Should Prioritize

Vendor Risk Tiering

Ensure the organization has a rational framework for categorizing vendor risk based on data access, system connectivity, and business criticality, not just spend levels.

Continuous Monitoring

Move beyond annual vendor assessments to continuous monitoring of security posture, incident notifications, and control effectiveness for critical vendors.

Incident Response Readiness

Test whether incident response plans are current, roles are clear, and the organization can execute under pressure, including scenarios involving vendor-originated incidents.

Board-Level Reporting

Validate that cyber risk reporting to the board is meaningful, forward-looking, and includes vendor-related exposure rather than purely technical metrics.

Data Quality and Governance Risk

Gartner – Data Governance & Analytics Research
IAPP – Global Privacy & Data Regulation

The Foundation Risk

Data quality often receives less attention than more visible risks, yet it underpins nearly every critical business process, regulatory report, and strategic decision. When data breaks, everything downstream becomes unreliable.

Poor Data Drives Bad Decisions

Executives making strategic choices based on inaccurate, incomplete, or inconsistent data will inevitably reach flawed conclusions, often discovering problems only after commitments are made.

Manual Controls Don't Scale

Organizations frequently rely on spreadsheets, manual reconciliations, and individual heroics to compensate for weak data systems. This approach fails as complexity and volume increase.

Regulatory Exposure Increasing

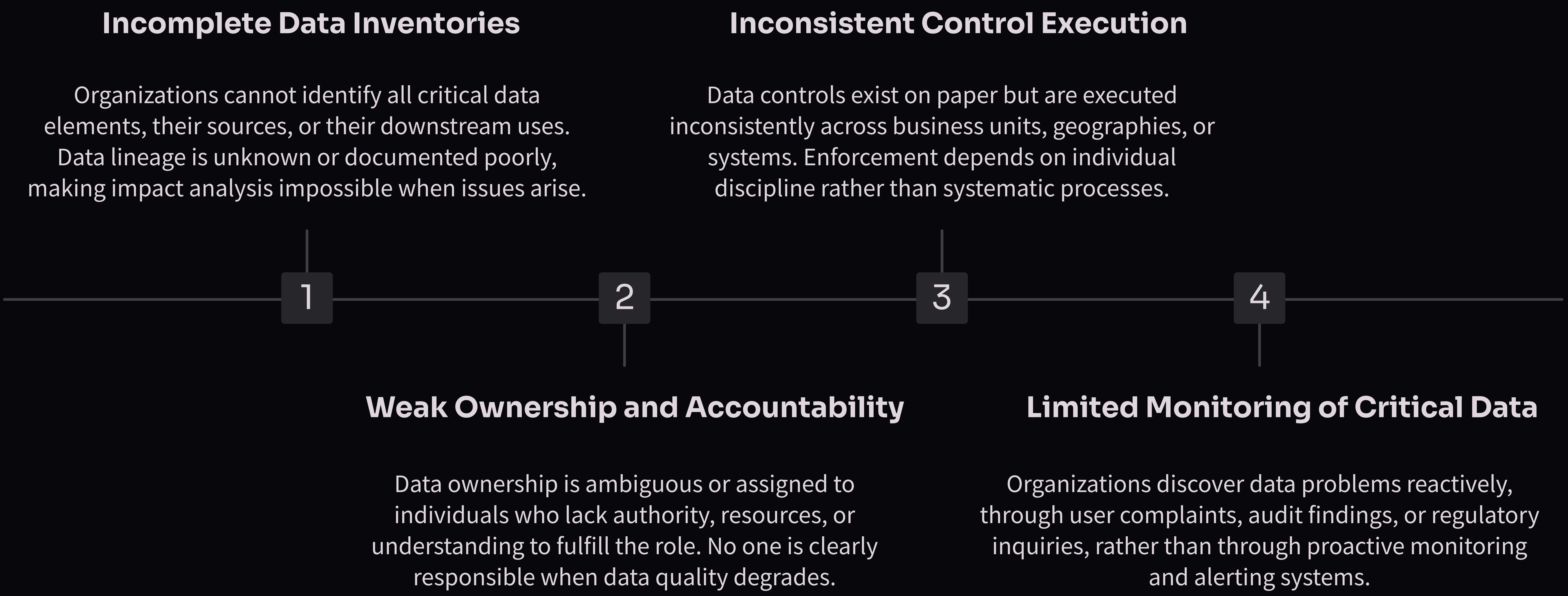
Regulators are intensifying scrutiny of data used in compliance reporting, risk calculations, and customer communications. Errors can trigger enforcement actions and restatements.

Trust in Reporting at Risk

When stakeholders question data reliability, confidence in management, forecasts, and strategy erodes, damage that extends well beyond the immediate data issue.

Data Risk: Audit Insights

Common Breakdowns



1

Incomplete Data Inventories

Organizations cannot identify all critical data elements, their sources, or their downstream uses. Data lineage is unknown or documented poorly, making impact analysis impossible when issues arise.

2

Weak Ownership and Accountability

Data ownership is ambiguous or assigned to individuals who lack authority, resources, or understanding to fulfill the role. No one is clearly responsible when data quality degrades.

3

Inconsistent Control Execution

Data controls exist on paper but are executed inconsistently across business units, geographies, or systems. Enforcement depends on individual discipline rather than systematic processes.

4

Limited Monitoring of Critical Data

Organizations discover data problems reactively, through user complaints, audit findings, or regulatory inquiries, rather than through proactive monitoring and alerting systems.

Digital Transformation and Technology Debt

Innovation Comes With Hidden Risk

Organizations face a dual challenge: maintaining aging legacy systems while simultaneously pursuing ambitious digital transformation initiatives. Both sides of this equation create risk that audit must understand and address.

- **Legacy Systems Consume Budgets**

  Outdated technology requires increasing maintenance investment while constraining innovation. Key personnel with institutional knowledge retire, leaving systems that few understand.

- **Cloud Migrations Add Complexity**

  Moving to cloud environments introduces new security models, vendor dependencies, and architectural patterns that IT teams must master while maintaining operations.

- **Integration Failures**

  Connecting new systems to existing infrastructure creates fragile integration points where data can be lost, duplicated, or corrupted. Testing often fails to catch these issues until production.

- **Speed Over Discipline**

  Business pressure to deliver transformation quickly can override proper controls, testing, and change management. Technical shortcuts become permanent problems.

Technology Debt: Audit Insights

McKinsey & Company – Digital Transformation Research
Gartner – Technical Debt & Legacy Systems

What Often Goes Wrong

Technology transformation initiatives consistently encounter similar execution risks. Internal audit teams examining these programs should look for these common failure patterns.

1

No Visibility Into Technical Debt

IT cannot quantify the extent of technical debt or its business impact. There is no systematic process for identifying aging systems, security vulnerabilities, or unsupported technologies requiring attention.

2

Weak Governance Over Transformation

Transformation programs lack clear accountability, milestone tracking, or escalation processes. Project governance exists but focuses on schedule and budget rather than risk and value delivery.

3

Limited Post-Implementation Review

Once systems go live, teams move immediately to the next initiative without assessing whether intended benefits materialized, controls function properly, or users adopted new processes.

4

Security Gaps During Change

Transformation creates temporary security exposures, test environments with production data, elevated access during migration, decommissioned systems still connected, that organizations fail to manage systematically.

Regulatory Compliance Risk

U.S. DOJ – Evaluation of Corporate Compliance Programs
OECD – Regulatory Policy Outlook

More Rules, More Judgment

Expanding Regulatory Scope

Regulators are broadening their reach into areas previously considered outside traditional oversight, data privacy, AI ethics, climate disclosure, cybersecurity, and third-party relationships. Organizations must monitor and respond to requirements across multiple jurisdictions and regulators.

Principles-Based Expectations

Regulations increasingly emphasize principles and outcomes rather than prescriptive rules. This creates interpretive challenges: what constitutes "reasonable" oversight, "adequate" testing, or "appropriate" governance? Organizations must exercise judgment with limited guidance.

Under-Resourced Compliance Teams

Compliance teams struggle to keep pace with regulatory change while managing day-to-day requirements. Smaller organizations lack specialized expertise, while larger ones face coordination challenges across decentralized compliance functions.

Higher Cost of Failure

Regulatory penalties are increasing in size and frequency. Beyond fines, organizations face consent orders, business restrictions, heightened supervision, and reputational damage that can take years to overcome.

POLL #3

Is Audit Focused on the Right Risks?

> Question: How well does your current audit plan align with the organization's top enterprise risks?

A. Unsure

We lack a clear view of how our audit coverage maps to the organization's actual risk profile.

B. Limited Alignment

Our audit plan reflects historical priorities and cyclical coverage rather than current enterprise risks.

C. Some Alignment

We address several key risks but miss important emerging areas due to resource or capability constraints.

D. Balanced Approach

We maintain reasonable coverage of top risks while preserving some cyclical audits and compliance requirements.

E. Strong Alignment

Our audit plan directly targets the organization's most significant risks with appropriate depth and frequency.

Discussion Point: What drives misalignment, common causes include stakeholder pressure for cyclical coverage, limited risk assessment processes, capability gaps, and difficulty saying no to audit requests.

Geopolitical and Supply Chain Risk

Efficiency vs Resilience

World Economic Forum – Global Risks Report
McKinsey – Geopolitical & Supply Chain Risk

For decades, organizations optimized supply chains for cost and efficiency, creating lean, just-in-time operations with minimal redundancy. Recent disruptions have exposed the fragility of these models and forced a fundamental reassessment of the risk-reward tradeoff.

Single-Source Dependencies

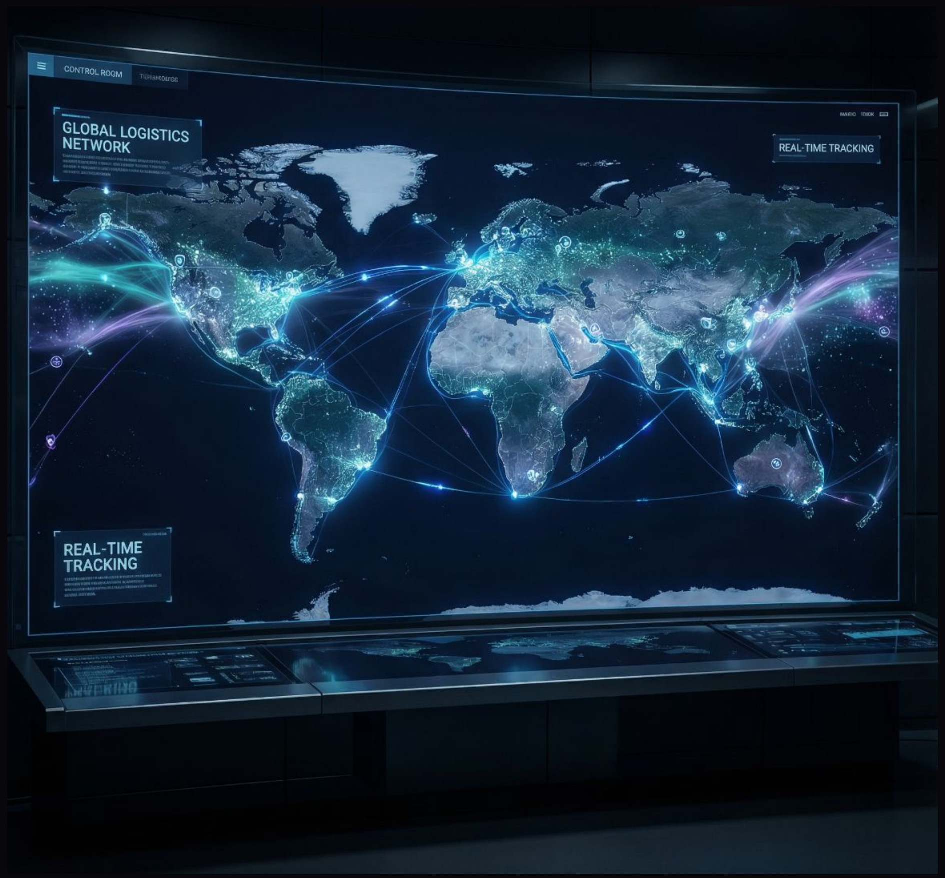
Concentration of critical suppliers in specific geographies or with individual vendors creates vulnerability when disruption occurs through natural disasters, political instability, or vendor failure.

Trade and Sanctions Exposure

Tariffs, export controls, and sanctions regimes shift rapidly, potentially stranding investments or cutting off access to markets, suppliers, or technologies overnight.

Disruption as the Norm

Supply chain disruption has moved from occasional crisis to persistent challenge. Organizations must build capability to identify, assess, and respond to continuous supply chain volatility.



> “Supply chain resilience is no longer optional, it's a strategic imperative that requires investment, redundancy, and ongoing risk assessment.”

Fraud Risk in Digital Environments

ACFE – Report to the Nations 2024
FBI – Internet Crime Report (IC3)

Fraud Has Changed

The shift to digital operations and remote work has fundamentally altered the fraud landscape. Traditional fraud schemes have evolved, and new attack vectors have emerged that many organizations are not prepared to defend against.

Social Engineering Dominates

Sophisticated phishing, business email compromise, and impersonation schemes target employees through digital channels, exploiting trust and urgency to bypass technical controls.

Payment Fraud Accelerating

Digital payment systems create new opportunities for fraudulent transactions, vendor impersonation, and account takeover. Detection often occurs only after funds are irretrievably lost.

Analytics Now Essential

Traditional sampling-based audit approaches cannot detect sophisticated fraud in high-volume digital transactions. Organizations must deploy analytics and continuous monitoring to identify anomalies and patterns.

Remote Work Reduces Deterrence

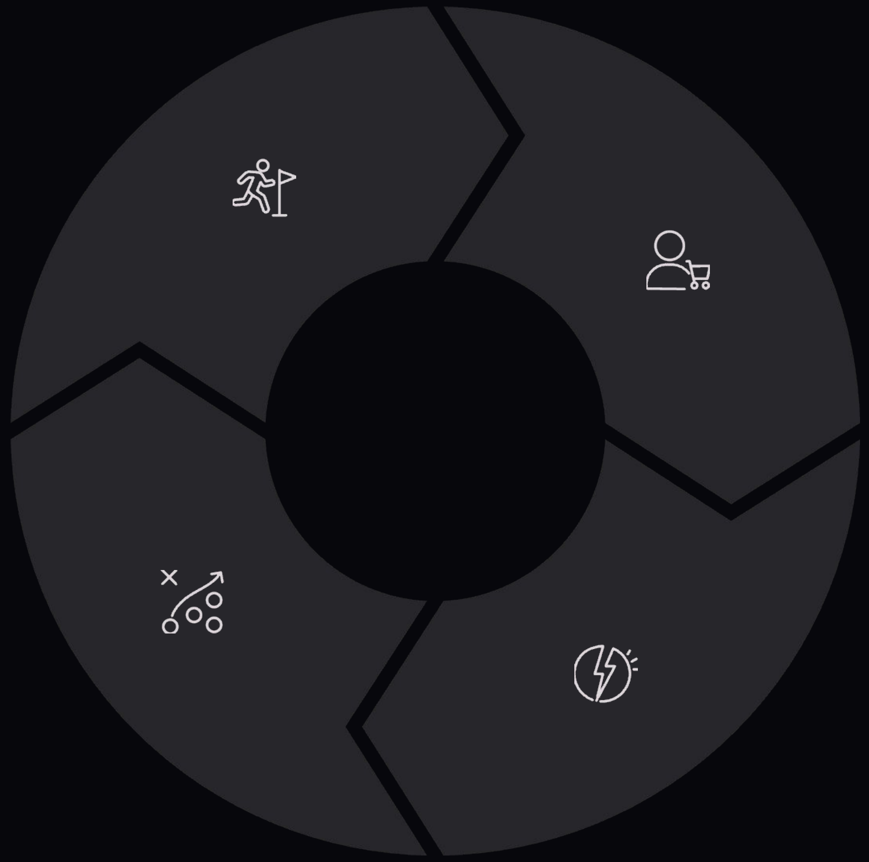
Physical separation weakens informal controls, casual conversations, observation, and peer awareness, that historically deterred fraud. Employees work in isolation with less oversight.

Strategic and Business Model Risk

IIA – North American Pulse of Internal Audit
McKinsey – Strategy & Competitive Risk

Slow Risks That Turn Fast

Strategic risks often develop gradually, making them easy to overlook or rationalize. However, once they reach an inflection point, these risks can accelerate rapidly and fundamentally threaten the business model.



Competitive Shifts

New entrants with different cost structures, business models, or technologies can erode market position before incumbent organizations recognize the threat and respond effectively.

Untested Strategy Assumptions

Strategic plans rest on assumptions about markets, capabilities, and competitive responses. When these assumptions prove incorrect, strategies can fail, often without clear early warning indicators.

Customer Behavior Changes

Evolving customer preferences, channel shifts, and changing expectations can undermine core business assumptions about what customers value and how they want to engage.

Technology-Driven Disruption

Emerging technologies can make existing products, services, or delivery models obsolete. Organizations comfortable with current technology may miss signals of impending disruption.

POLL #4

Is Audit Still Looking Back?

> Question: How often does internal audit provide forward-looking insights to management and the board?

A. Unsure

We have not defined what forward-looking audit work means for our organization.

B. Rarely

Our work focuses almost exclusively on historical compliance and control testing.

C. Frequently

Forward-looking risk insights are a core deliverable in most of our audit engagements and reporting.

D. Occasionally

We provide forward-looking perspectives on an ad-hoc basis when findings suggest emerging issues.

E. Regularly, Inconsistently

We attempt to include forward-looking insights but lack a systematic approach or consistent methodology.

Discussion Point: What enables forward-looking work, key factors include stakeholder demand, audit team skills, access to the right data, and willingness to move beyond traditional compliance-focused methodologies.

CherryHill ADVISORY

Preparing Internal Audit for 2026

What Must Change

Adapting internal audit to the 2026 risk environment requires fundamental shifts in approach, capabilities, and stakeholder relationships. Incremental adjustments will not suffice.

Fewer, Higher-Impact Audits

Abandon the illusion of comprehensive coverage. Concentrate resources on risks that matter most, accepting that some areas will receive less frequent attention.

Better Use of Data and Analytics

Invest in analytics capabilities that enable continuous monitoring, anomaly detection, and population-level insights rather than sample-based testing.

Stronger Stakeholder Dialogue

Move from report-out to ongoing dialogue. Understand stakeholder concerns early and often. Make audit work relevant to what keeps executives and board members awake at night.

Flexibility to Adjust Plans

Build agility into audit plans. Reserve capacity for emerging risks. Accept that the plan approved in January may look different by June, and that's appropriate.

Practical Planning Takeaways

What You Can Do Now

1 **Reassess Risk Priorities**

Review your risk assessment with fresh eyes. Challenge assumptions about what risks matter most. Validate priorities with board members and executives individually. their perspectives may differ from formal risk assessments.

2 **Challenge Cyclical Planning**

Identify audits that appear in your plan primarily because they were there last year. Ask whether these audits address current risks or serve other stakeholders' needs. Be prepared to justify, or eliminate them.

3 **Invest Selectively in Skills and Tools**

You cannot build every capability simultaneously. Choose 1-2 strategic investments in skills or technology that will meaningfully expand your ability to address priority risks.

4 **Tighten Audit Committee Communication**

Evaluate whether your audit committee reporting focuses on what matters. Reduce compliance-oriented content. Increase forward-looking perspective and plain language insights.

Closing and Key Messages

Final Thoughts

Risk Is Moving Faster Than Plans

Annual audit planning cycles no longer match the velocity of risk change. Internal audit must build flexibility and responsiveness into planning processes while maintaining strategic focus.

Audit Value Comes From Focus

Comprehensive coverage is neither possible nor valuable. Internal audit creates impact by concentrating on risks that matter most to the organization's success and resilience.

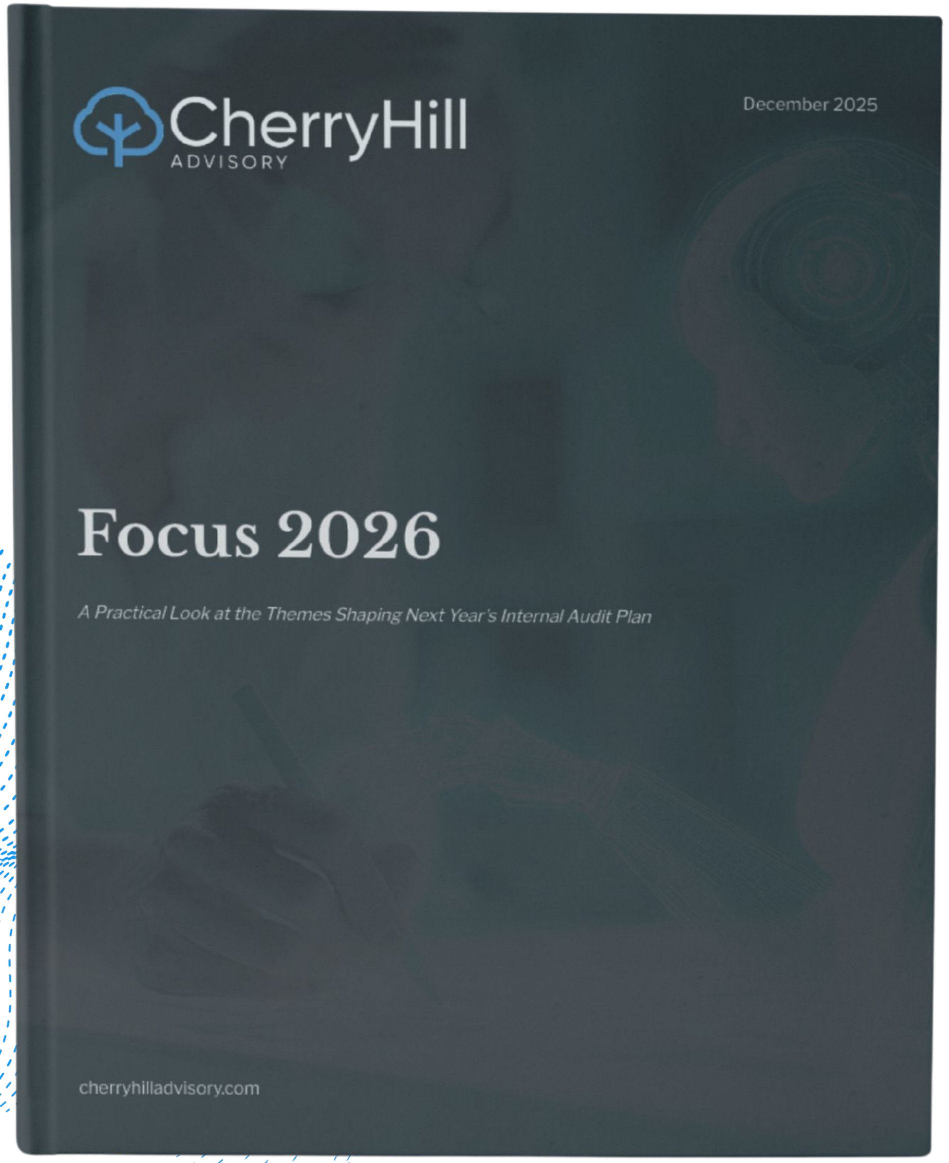
Insight Matters As Much As Assurance

Stakeholders need internal audit to help them understand emerging risks and implications, not only validate that controls worked historically. Forward-looking perspective differentiates high-performing audit functions.

2026 Planning Starts Now

Waiting until year-end to plan for 2026 means entering the year reactively. Begin stakeholder dialogue, capability assessment, and priority setting now to position internal audit for success.

Resources



CherryHill ADVISORY

December 2025

Focus 2026

A Practical Look at the Themes Shaping Next Year's Internal Audit Plan

cherryhilladvisory.com

A Practical Look At The Themes Shaping Next Year's Internal Audit Plan

Scan QR Code to download **Focus 2026** for free

LEARNING NEVER STOPS

Upcoming Live Webinars

All events will be globally accessible (virtual) and eligible for 1 CPE.

Explore upcoming events here

AI Part 1: Understanding AI Risk in Plain Language

Tuesday, February 17, 2026 |
12:00 PM – 1:00 PM EST

AI Part 2: Building and Reviewing AI Governance

Wednesday, March 18, 2026 |
12:00 PM – 1:00 PM EDT

AI Part 3: Auditing AI-Enabled Processes

Wednesday, April 15, 2026 |
12:00 PM – 1:00 PM EDT

AI Part 4: Using AI Inside Internal Audit the Right Way

Tuesday, May 19, 2026 |
12:00 PM – 1:00 PM EDT

Cyber Risk You Can Check Without Being an Engineer

Tuesday, June 16, 2026 |
12:00 PM – 1:00 PM EDT

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

LinkedIn