Deloitte.

Leadership Series

IT Governance and Cyber Risks in Internal Audit

Calgary
May 21, 2026

Introduction

In the meeting with you today…

Xavier Tessier
Director
National IT Internal Audit Leader, Internal Audit

Nicolo' Perin
Assistant Manager
Regional IT Internal Audit Lead, Internal Audit

Agenda

01

IT Governance & Digital Transformation

- IT Governance Overview
- IT Governance impacts on Digital Transformation
- Digital Transformation and Governance Investments

02

Cybersecurity & Technology hot themes

- Key IT & Cyber Risks – Hot themes
- The impact on Internal Audit

03

Case-study

- Cloud Governance and Internal Audit capabilities

IT Governance & Digital Transformation

IT Governance: A Leadership Imperative

What effective IT governance addresses

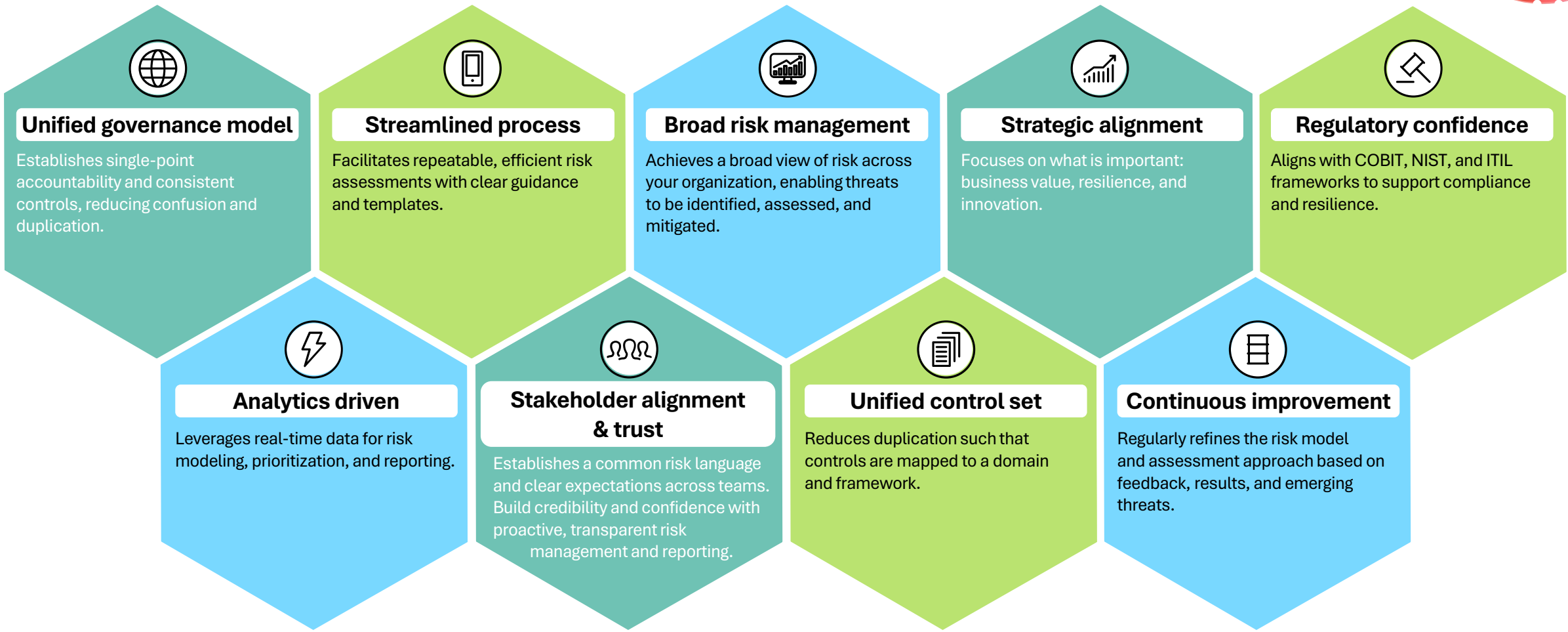
- Clear **ownership**, **accountability** and **decision-making**
- Strategic, long-term **technology investment**
- Governance of **emerging technology risks**
- Clear **performance outcomes** and **KPIs**

How Internal Audit enables effective IT governance

- Assess the end-to-end system
- Enable decision-ready risk insight
- Assess real decision behaviors
- Evaluate operating model effectiveness
- Focus on what matters most

Benefit across the organization

Key value drivers of IT Governance



Maximizing Value from Digital Transformation Through Effective IT Governance

01 Strategic Impact

- Ensures digital initiatives are **aligned with business strategy**
- Prioritizes investments with highest **business value**
- Transforms IT from a support function to a **value driver**

02 Operational Impact

- Establishes **clear decision-making and accountability**
- Improves coordination across **business and IT functions**
- Enables **consistent execution** of transformation initiatives
- Accelerates delivery by reducing rework and misalignment

03 Risk & Control Impact

- Embeds **risk management and compliance** into digital initiatives
- Reduces failure risk of new technologies and implementations
- Ensures **secure, controlled adoption** of cloud, AI, and digital tools

Value Realization

- Improves **visibility over value delivered** by **digital investments**
- Enables **performance measurement** (KPIs, benefits tracking)
- Supports **consistent execution** and **scalability of transformation initiatives**
- **Strengthens control** over **change** and **reduces implementation risk**

IT governance enables more structured and controlled execution of digital transformation initiatives

Without effective governance, digital transformation initiatives may lead to increased costs and inefficiencies

IT Governance & Investment Impact (*Deloitte Insights*)

- Up to $1.25T value unlocked with aligned strategy
- $1.5T at risk with poor execution
- 75% of leaders struggle to measure transformation value
- +20% improvement in value realization with structured KPIs

Digital transformation value | Deloitte Insights

New Deloitte report finds digital transformation can open up US$1.25 trillion in additional market capitalization

Overview on IT spending - Stats and Facts

According to multiple research and analyst reports, transformation projects and IT Implementations still represent a challenge for today's organizations. This is why Internal audit must play a key role in supporting organizations to increase the success rate of such initiatives.

01

Global spending on digital transformation will reach almost $4 trillion by 2027.

This spending surge represents **55% growth** from 2023 levels, with **manufacturing** and **financial** services leading sector investments. The acceleration reflects post-pandemic urgency combined with **AI-driven opportunities** demanding fundamental infrastructure modernization.

02

70% of digital transformation projects fail to meet their goals.

The persistence of **high failure rates** despite decades of experience suggests **systemic issues** rather than **industry-specific challenges**. Failed transformations cost organizations an **average of 12% of annual revenue** through wasted investment and opportunity costs.

03

47% of ERP implementations experience budget overrun *(averaging 35% over plan)*.

Scope creep, integration complexity, and change management drive **average 18-month delays**. Failed **ERP** projects cost organizations average **$15 million** in direct costs plus operational disruption.

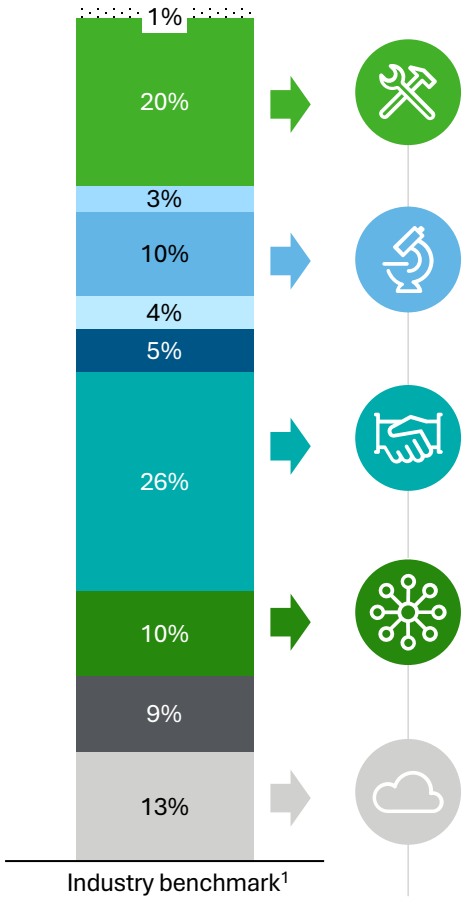
04

Organizations allocate 35% of IT budgets to transformation initiatives.

Deloitte's technology investment research shows transformation consuming increasing share of technology spending.

Reference: Data Transformation Challenge Statistics — 50 Statistics Every Technology Leader Should Know in 2025 | Integrate.io

IT spending by IT technical function and savings potential



ENABLERS		WHY IT MATTERS	QUICK WINS
Application development	*Implement DevOps to increase speed to market and productivity of resources*	**~10%** shaped by existing capabilities	• Set up a **CI/CD pipeline**, use existing tools, and **track metrics** to demonstrate quick value from DevOps
Services	*Stop consumption of marginal or redundant services*	**~15%** depending on starting point/ambition level	• Analysis of **service orchestration** including service catalogue • Establishment of **service lifecycle management** • Investigate **service performance management**
Application support	*Decommission unused applications, eliminating any residual spend on support/maintenance*	**~10%** based on current maturity	• Identify minimally used or inactive applications (6–12 months) using **analytics tools** and **verify redundancy** by comparing them to active systems
Network	*Retender WAN contracts and leverage software-defined networking*	**~5%** based on current architecture	• Examine the ability to **negotiate** with **existing suppliers** to reduce network costs • Use **SDN** to have more control over network traffic flow
Optimize cloud cost	*Review current cloud spend and its components*	**~25%+** of covered financial baseline	• Investigate **alternative delivery options** (e.g., use cloud-native storage instead of dedicated SSDs • Avoid **overprovisioning** of instances • Find smart cost-effective **failover concepts**, etc.)

Legend:

- IT service continuity
- Application development
- IT operations management
- Digital workplace services
- IT service desk
- IT security
- Application support
- Network
- Governance and business mgmt.
- Data center/hosting (internal and external)

[1] *Gartner IT Key Metrics 2025 Industrial Manufacturing (2024)*

Digital transformation future scenarios

"Digital spending is growing rapidly, potentially reaching over 30% of revenue by 2028"

Digital spending is shifting away from IT ownership toward business-led investments

This creates a significant governance challenge, **reinforcing** the **need** for **strong IT governance** to ensure **investments are controlled,** and **delivering value**.

Even if it's **"non-IT budget",** IT governance is **STILL critical** because**:**

01 Technology is still IT-dependent

Even if funded outside IT: cloud systems; data platforms; applications integrations

👉 **All depend on**: IT architecture; cybersecurity data governance; infrastructure
✅ **So:➞ Digital can not be decoupled from IT governance**

02 Harder cost control

If budgets sit outside IT: reduced visibility; lack of centralized prioritization; overlapping investments

👉 **Result**: wasted spend; poor ROI
✅ **So:➞ IT governance provides investment discipline and oversight**

03 Increasing risk exposure

Business-led tech adoption often bypasses: security reviews; compliance processes; testing

👉 **Result**: cyber risk, regulatory risk; operational failures
✅ **So:➞ IT governance ensures control and risk management**

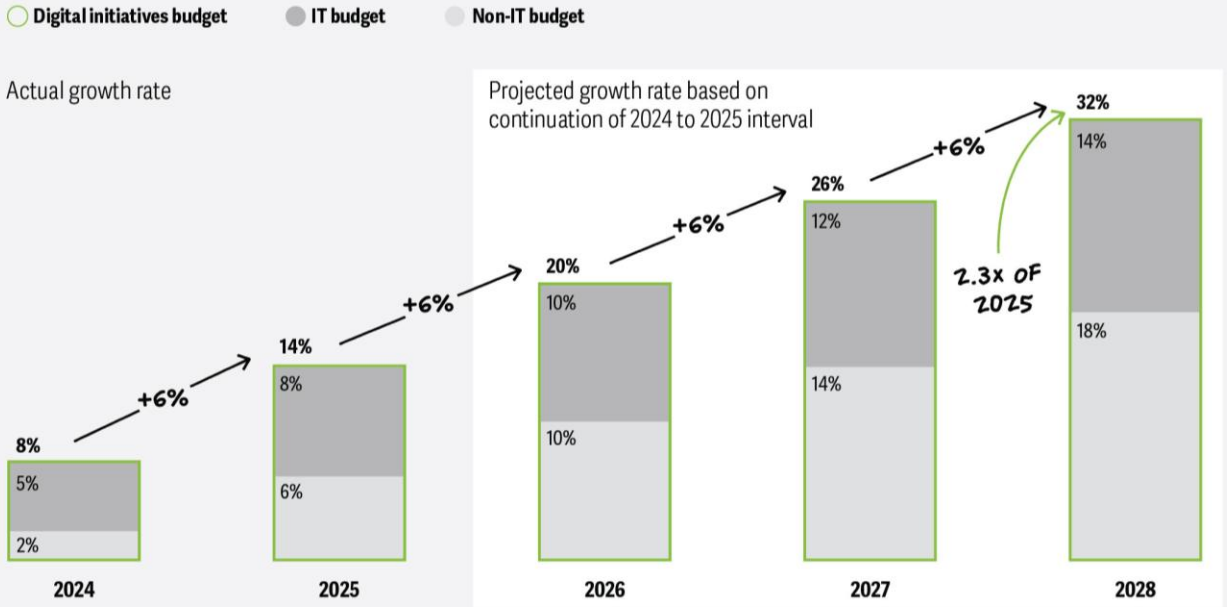
04 Unclear value realization

Without centralized governance: no unified KPIs; no benefits tracking; no prioritization

✅ **So:➞ IT governance ensures ROI tracking and value realization**

At the current pace of growth, digital budgets would reach 32% of revenue by 2028

Question: Please provide the following information on your organization's annual revenue, IT budget, and digital transformation budget to the nearest whole 100 million or whole billion



Note: Percentages might differ due to rounding off base dollar values.

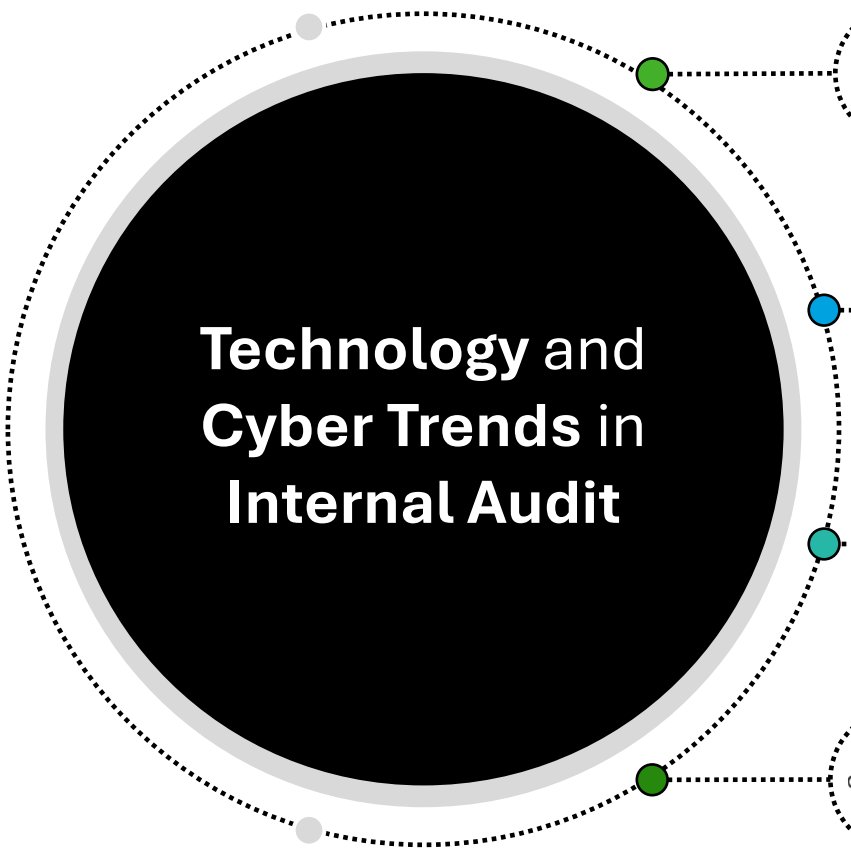
Source: Deloitte Center for Integrated Research analysis of data collected from May to June 2025 from US business and technology leaders.

Deloitte. Insights | deloitteinsights.com

Technology and Cyber Risks in Internal Audit

Technology and Cyber Trends Driving Internal Audit Risk Focus

The establishment of an effective technology and digital framework represents one of the biggest areas of both risk and opportunity for organizations. Optimized frameworks can deliver cost reductions, support management of risks in line with appetite, and enable innovation and delivery of strategic goals. This is particularly important in the cost constrained environment in which many organizations currently operate. A general overview if the technology and cyber risks in Internal Audit is shown below.



Cybersecurity and Cyber Resilience

Organizations face increasing **challenges** in maintaining **robust cybersecurity controls** in line with evolving threats. Internal Audit focuses on assessing the **effectiveness** of **security governance**, **incident response capabilities**, and **resilience** measures to ensure business continuity and protection of critical assets.

Supply Chain Risks and Third-Party Risk Management

Reliance on **third-party vendors** continues to grow, increasing exposure to **external risks**. Internal Audit evaluates the effectiveness of third-party risk management frameworks, including **vendor selection**, **monitoring**, and **compliance** with security and contractual requirements.

Cloud Security & Governance

The adoption of **cloud technologies** introduces new risks related to **data security**, **access management**, and **regulatory compliance**. Internal Audit assesses governance structures, control frameworks, as well as monitoring mechanisms to ensure secure and compliant use of cloud environments.

Digital Transformation Program

Digital transformation initiatives are **expanding rapidly**, often with **decentralized ownership**. Internal Audit focuses on evaluating **governance**, **risk management**, and **value realization processes** to ensure initiatives are aligned with business objectives and deliver expected outcomes.

The Cybersecurity and Cyber Resilience Threat Landscape

5 Key Risks in 2026

01

AI-Transformed Threat Landscape

Generative AI accelerates attack velocity, enables deepfakes & autonomous phishing at scale

02

Human Error

Social engineering, insider threats & credential misuse remain the #1 breach vector

03

Supply Chain Attacks

Third-party & software supply chain compromises targeting interconnected ecosystems

04

IoT & OT Attack Surface

Expanding connected device landscape with legacy OT systems lacking modern controls

05

IIA Topical Requirements

New mandatory cybersecurity standards from the Institute of Internal Auditors

INTERNAL AUDIT RESPONSE

5 Actions IA Should Take

Assess Cybersecurity Program Maturity

Evaluate controls against NIST CSF, ISO 27001 & CIS benchmarks; identify gaps

Supply Chain Security Audits

Assess third-party risk management programs & software bill of materials (SBOM)

Audit AI-Enabled Attack Vectors

Review AI governance, deepfake detection controls & automated threat response

Ransomware Threat Response Readiness

Test incident response plans, backups, BCP & tabletop exercise effectiveness, but also include access-controls and identity management.

IIA Cyber Topical Requirement Compliance

Ensure IA activity meets mandatory IIA cybersecurity topical requirement standards

Supply Chain Risks and Third -Party Risk Management

5 Key Risks in 2026

01 Intensified Regulation

Expanding FS regulations (e.g., DORA, CTP) are driving the need for more robust, standardized, and resilient TPRM frameworks.

02 Emerging AI risks

Increased GenAI adoption in third-party ecosystems is elevating risks across data, cybersecurity, privacy, and ethics.

03 Operational Resilience Integration

TPRM is being embedded into resilience frameworks to ensure third-party disruptions remain within impact tolerance.

04 Shift to Risk Intelligence

Organizations are transitioning from self-attestation to analytics-driven risk intelligence for proactive risk management.

05 Expansion to fourth-party risk

Effective risk management now requires visibility into fourth-party dependencies and interconnected ecosystem risks.

INTERNAL AUDIT RESPONSE

5 Actions IA Should Take

Respond to regulatory change

Align audit plans and TPRM assurance with evolving regulatory expectations and governance requirements.

Assess AI third-party risks

Provide independent assurance over controls addressing AI risks in third-party relationships.

Evaluate resilience alignment

Assess whether TPRM supports operational resilience, including stress testing, BCP, and exit planning.

Validate risk intelligence

Evaluate the effectiveness of analytics-driven risk intelligence versus traditional attestation approaches.

Strengthen fourth-party oversight

Assess whether fourth-party risks are effectively identified, monitored, and governed within TPRM frameworks.

Cloud Security & Governance

5 Key Risks in 2026

01 Data sovereignty risks

Geopolitical tensions and regional regulations are driving cloud fragmentation and increasing risks related to data residency, access, and vendor lock-in.

02 Cloud sustainability imperative

ESG expectations are embedding sustainability considerations—such as carbon footprint and ethical sourcing—into cloud strategies and provider selection.

03 Evolving regulations

Expanding data security and privacy regulations (e.g., GDPR, NIS2) are increasing compliance obligations for cloud environments.

04 Cloud supply chain risks

Dependence on cloud providers is creating concentration risk, requiring stronger vendor diversification and resilience strategies.

05 Cloud cost management

Ineffective cloud cost governance can lead to rapid cost escalation, necessitating structured monitoring and optimization practices.

INTERNAL AUDIT RESPONSE

5 Actions IA Should Take

Assess geopolitical risks

Evaluate exposure to geopolitical and data sovereignty risks across cloud providers, including vendor concentration and service disruption scenarios.

Integrate ESG into audits

Incorporate ESG considerations into cloud audits, assessing alignment with sustainability objectives and provider practices.

Enhance security and privacy assurance

Strengthen assurance over cloud data security, privacy controls, and compliance with evolving regulatory requirements.

Review supply chain resilience

Assess the resilience of cloud supply chains, including vendor diversification, contractual protections, and mitigation strategies.

Evaluate cloud cost governance:

Review cloud cost management practices to identify inefficiencies and ensure effective monitoring, optimization, and accountability.

Digital Transformation Program

4 Key Risks in 2026

01

Lack of preparation for a as-a-service transition

The rapid adoption of "as-a-service" solutions can leave customers and support unprepared, leading to change programmes not meeting their objectives during the transition to live operation

02

Over-reliance on third-party to deliver transformation

Agile and value stream change delivery methods drive innovation, retaining in-house expertise remains a challenge

03

Lack in identifying clear requirements and benefits

Many change programmes struggle to fully realise their objectives during the transition to business-as-usual (BAU)

04

Focus solely on effective cost-management and schedule

Risk managers and change assurance teams should identify and track the critical success factors, such as achieving clear outcomes for customers, employees, and regulators.

INTERNAL AUDIT RESPONSE

4 Actions IA Should Take

Challenge the alignment with the strategy

Challenge the approach to strategic prioritization and portfolio management to ensure alignment with strategic objectives and regulatory compliance.

Audit the governance

Evaluate risks at portfolio-level to provide assurance over the business strategy, challenge existing practices, and to proactively assess the risks of inaction, with a stronger emphasis on governance oversight.

Be proactive

Adopt a more proactive approach of embedding audit resources within programs and portfolio to give real-time risk assessment, timely challenge, and value-added feedback.

Build relationships

Implement clear and transparent communication with programme managers to obtain relevant data and decision-making documents and evidences

Case Study

Case Study

Case Study 1

The Vendor's Vendor Incident" — Third-Party + Ecosystem Risk (4th/5th party)

Storyline

A critical vendor uses a managed file transfer tool. A vulnerability in that tool is exploited, and the organization's data is exfiltrated through the vendor ecosystem. You didn't even know that tool existed in your supply chain.

Internal Audit Objectives:

1) Determine whether the organization effectively manages third-party risks across the vendor lifecycle, including onboarding, contracting, and ongoing oversight, in alignment with defined risk appetite and policy expectations.
2) Assess whether the organization has **sufficient visibility** and **governance** over **critical third-party dependencies**, including extended supply chain relationships, to identify and manage associated risks.
3) Evaluate whether **vulnerability management expectations** for third parties are clearly defined, enforced, and supported by evidence, including timely remediation and appropriate handling of exceptions.
4) Assess whether **incident response roles, processes, and communication protocols** with third parties are clearly defined, coordinated, and effective in supporting timely detection, response, and regulatory compliance.

Case Study 2

The Cloud Storage Exposure" — Cyber Resilience + Cloud Governance

Storyline

A business unit accelerates a cloud migration and stands up several storage containers for analytics. A partner later reports that sensitive files were accessible due to an access misconfiguration and poor key/secret handling. Leadership wants to know: Was this a one-off mistake or a governance/control design gap?

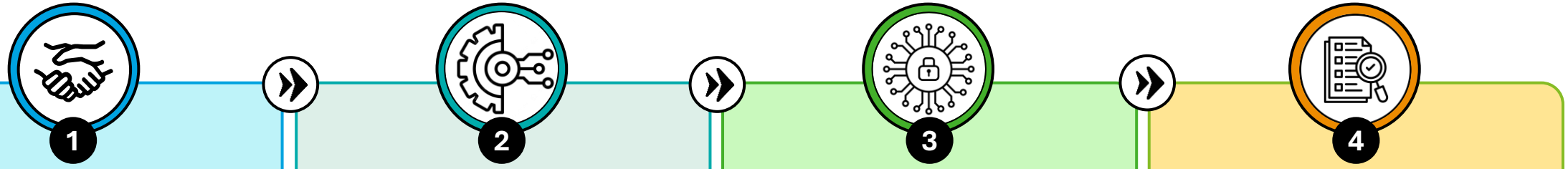
Internal Audit Objectives:

1) Assess whether **roles** and **responsibilities** for cloud security are clearly defined and understood across the organization in alignment with the cloud provider's shared responsibility model.
2) Evaluate whether **identity** and **access controls** are appropriately **designed** and **implemented** to enforce least privilege, secure service account usage, and effective credential and key management.
3) Assess whether **cloud configuration** and **change management processes**, including guardrails and policy enforcement, are effectively **designed** and operating to prevent unauthorized or insecure changes.
4) Evaluate whether **logging, monitoring,** and **alerting** capabilities are sufficient t**o detect, escalate,** and **respond** to unusual or unauthorized activities in a timely manner.
5) Assess whether **incident response processes**, including playbooks and escalation protocols, are clearly defined, tested, and effective in supporting timely containment, communication, and remediation of cloud-related incidents.

Key Takeaways

KEY TAKEAWAYS

IT Governance Is the Key Enabler of Value, Control, and Resilience in Digital Transformation



Strong IT Governance drives value and accountability

Effective **IT governance** is the **foundation** for **aligning technology** with **business strategy investments**, enabling clear decision-making, accountability, and performance measurement across digital initiatives with **structured governance** improving **value realization** by ~20% through **clear KPIs** and **oversight**.

Digital transformation increases both opportunity and risk

While organizations are significantly **increasing investments** in **digital transformation** (35% of IT budgets and ~4T globally by 2027), **high failure rates** and **cost overruns** highlight the need for stronger governance, disciplined execution, as wells as structured performance tracking.

The cyber and technology risk landscape is expanding rapidly

Organizations are facing growing exposure across **cybersecurity, cyber resilience, third-party ecosystems, cloud environments,** and **AI-driven threats**, requiring **integrated risk management** and stronger control frameworks.

Internal Audit is a strategic enabler of resilience and control

Internal Audit plays a critical role in assessing **governance effectiveness**, providing **decision-ready insights**, and ensuring that **risk management, controls**, and **value realization** are embedded across transformation programs.

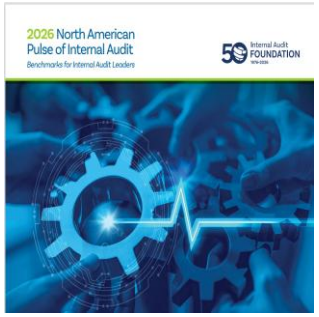
Deloitte POV - Key Internal Audit and Risk Hotspots

2026 North American Pulse of Internal Audit

This report provides benchmarking data on various aspects of internal audit activities, including CAE metrics, budget, staff, audit plans, audit plan analysis, and risk levels. The report also discusses the trends in remote work and sustainability in audits, as well as the responsibilities of internal audit professionals in different types of organizations. It provides valuable benchmarking data for Internal Audit functions in North America. For further details, refer to The Pulse of Internal Audit

Internal Audit Hot Topics

The report discusses key organizational risks that Internal Audit functions should have in their audit plans and provides strategies for reviewing these areas of risk. It emphasizes the need for internal audit to align with the organization's purpose, embrace digital technologies, and drive organizational change and learning. For further details, refer to Internal Audit Hot Topics



Hot Topics for Technology and Digital Risk

The report discusses key Technology and Digital risks facing organizations and highlights priority areas for Internal Audit in 2026 . These include, emerging risks in technology, generative AI, identity and access management, cybersecurity maturity assessments, and technology resiliency and governance. For further details, refer to Hot topics for technology and digital risk 2026

The Leadership Series will resume in September following our summer pause

“stay tuned for upcoming topics”

- Capital Projects
- Joint Venture Governance
- Mergers & Acquisition
- And many more

To stay updated on future sessions with Deloitte

Deloitte.

About Deloitte Canada

At Deloitte, our Purpose is to make an impact that matters. We exist to inspire and help our people, organizations, communities, and countries to thrive. Our work underpins a prosperous society where people can find meaning and opportunity. It builds consumer and business confidence, empowers organizations to find imaginative ways of deploying capital, enables fair, trusted, and functioning social and economic institutions, and allows our friends, families, and communities to enjoy the quality of life that comes with a sustainable future. And as the largest Canadian-owned and operated professional services firm in our country, we are proud to work alongside our clients to make a positive impact for all Canadians.

Deloitte provides industry-leading consulting, audit and assurance, tax, advisory and managed services to nearly 90% of the Fortune Global 500® and thousands of private companies. We bring together world-class capabilities, insights, and services to address clients' most complex business challenges.

Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

To learn more about Deloitte Canada, please connect with us on LinkedIn, X, Instagram, or Facebook.

© 2026 Deloitte LLP and affiliated entities.