Deloitte.

Information technology (IT) internal audit (IA) topics of interest

2026

Information technology (IT) internal audit (IA) topics of interest

Internal Audit teams face a fast-changing IT landscape shaped by new technologies, regulatory shifts, and evolving cyber risks. This update for 2026 highlights the leading IT domains demanding audit focus, helping leaders anticipate challenges and prioritize efforts to safeguard organizational value and resilience.

Recent priority areas where IT IA is leaning in include:

Vulnerability management

Automated, AI-driven tools enable continuous vulnerability scanning and rapid patching, helping organizations proactively identify and remediate weaknesses as new threats and vulnerabilities emerge in today's fast-evolving technology landscape.

Identity and access management (IAM)

Zero Trust, biometrics, and adaptive access controls are now important as organizations address rising risks and complexity from remote work and cloud adoption, countering identity-based attacks with real-time monitoring.

Resiliency

Predictive analytics and cross-cloud failover, integrated with strategic disaster recovery and business continuity planning can enable organizations to quickly recover and remain resilient against ransomware and supply chain disruptions.

Quantum computing

Quantum computing's rapid development threatens traditional encryption, prompting organizations to pilot quantum-safe cryptography and closely monitor progress to provide digital information and transaction security in a quantum-ready future.

Operational technology (OT) and IT convergence

OT/IT convergence, accelerated by Internet of Things (IoT), enables real-time data sharing and automation but exposes legacy systems to new cyber risks, making integrated security frameworks and real-time monitoring increasingly important.

Cloud governance and security

Multi-cloud and hybrid strategies drive complexity, requiring integrated cloud-native security, automated compliance controls, and broad auditing to address provider risk, data sovereignty, and governance across distributed cloud ecosystems.

Information technology (IT) internal audit (IA) topics of interest

Recent priority areas where IT IA is leaning in include:

Application programming interface (API)

Expanding API sprawl and third-party integrations increase connectivity and risk, making governance, inventory management, secure coding, and automated threat detection important for safeguarding real-time traffic and supporting data accuracy across systems.

Artificial intelligence (AI) technologies

As generative AI and automation accelerate innovation, strengthening governance, transparency, and bias controls becomes important for risk management, regulatory compliance, and sustaining stakeholder confidence in more digital organizations.

Network security

AI-powered threat detection and micro-segmentation redefine network security. Remote work and edge computing reshape network architectures as well as expand digital infrastructures and attack vectors.

Digital transformation assurance

Digital transformation can accelerate with automation and low-code platforms, but effectiveness depends on agile delivery, change management, and embedding assurance and secure design to protect evolving IT environments and realize business value.

Cyberthreats

AI-driven threats, deepfakes, and traditional attacks like ransomware increasingly disrupt IT and business operations, making advanced threat intelligence, real-time monitoring, and robust cybersecurity controls important to counter evolving tactics and vulnerabilities.

Third-party risk management (TPRM)

As organizations rely on digital, interconnected supply chains, TPRM now includes extended enterprise risk, continuous monitoring, and Sustainability compliance to prevent disruptions and breaches originating from external partners.

High-impact areas of focus for IT internal audit

Each IT priority area brings distinct risks and opportunities for Internal Audit. This section outlines the important risk considerations and strategic focus areas for auditors, guiding auditors to deliver assurance, strategic insights, and proactive value in a rapidly evolving technology landscape.

Priority area	Key risks	Potential areas of internal audit focus
Vulnerability management	• AI-driven attacks exploit unpatched vulnerabilities faster than legacy tools can respond, increasing risk of rapid compromise. • Continuous monitoring may miss zero-day threats as attack sophistication outpaces automated detection capabilities.	• Review effectiveness of AI-driven vulnerability scanning and patch management processes for timely threat response. • Assess controls for detecting zero-day vulnerabilities and monitoring emerging threat intelligence sources.
Identity and access management (IAM)	• Weak biometric controls or poor Zero Trust implementation can enable unauthorized access to sensitive systems and data. • Real-time identity monitoring may generate false positives, disrupting legitimate user activity and business operations.	• Evaluate biometric authentication and Zero Trust implementation for alignment with access control policies and leading practices. • Test accuracy and reliability of real-time identity monitoring, including incident response procedures for false positives.
Resiliency	• Predictive analytics failures can lead to missed early warnings, increasing downtime from ransomware or supply chain disruptions. • Overreliance on cross-cloud failover may expose data to inconsistent security controls and regulatory gaps.	• Validate predictive analytics models and early warning systems for accuracy in identifying potential disruptions. • Review cross-cloud failover plans for consistent security controls and compliance with data protection regulations.
Quantum computing	• Quantum algorithms threaten traditional encryption, risking exposure of sensitive data before quantum-safe solutions are fully deployed. • Early adoption of quantum technologies may introduce operational instability and integration challenges with legacy systems.	• Assess quantum readiness plans, including migration to quantum-safe cryptography and vendor risk management. • Examine integration testing for quantum technologies and contingency plans for operational stability.
Operational technology (OT) and IT convergence	• IoT expansion increases attack surfaces, making legacy OT systems vulnerable to cyber threats targeting integrated environments. • Inadequate real-time monitoring can delay detection of breaches, risking operational shutdowns or safety incidents.	• Test security of legacy OT systems and IoT devices within converged environments. • Review real-time monitoring capabilities and incident response protocols for OT/IT breaches.
Cloud governance and security	• Multi-cloud complexity can obscure visibility, leading to misconfigurations and data breaches across distributed environments. • Automated compliance controls may fail to keep pace with evolving regulations, resulting in non-compliance or audit findings.	• Evaluate visibility and configuration management across multi-cloud environments for data protection and access controls. • Review automated compliance controls for adaptability to new regulations and audit requirements.

High-impact areas of focus for IT internal audit

Priority area	Key risks	Potential areas of internal audit focus
Application programming interface (API)	• Unmanaged API sprawl increases risk of unauthorized data access and exposure through insecure endpoints. • Third-party integrations may introduce vulnerabilities, enabling attackers to bypass internal security controls.	• Assess API inventory management and security standards for exposure risks and unauthorized access. • Review third-party API integration testing and monitoring for vulnerabilities and compliance with security policies.
Artificial intelligence (AI) technologies	• Poorly governed AI models can perpetuate bias or make unethical decisions, damaging reputation and regulatory standing. • Inadequate model monitoring may allow undetected drift, leading to inaccurate outputs and business disruption.	• Examine AI governance frameworks for bias mitigation, ethical standards, and regulatory compliance. • Review model monitoring processes for detecting drift and ensuring accuracy of AI outputs.
Network security	• AI-powered attacks can evade traditional network defenses, increasing risk of undetected breaches and data loss. • Micro-segmentation misconfigurations may inadvertently block critical services or expose sensitive assets to external threats.	• Test effectiveness of AI-powered network threat detection and response capabilities. • Review micro-segmentation implementation for proper configuration and protection of critical assets.
Digital transformation assurance	• Rapid automation and low-code adoption may introduce security gaps and compliance risks in newly digitized processes. • Ineffective change management can result in failed projects, wasted investment, and disruption to core business operations.	• Assess security and compliance controls in automated and low-code digital processes. • Review change management procedures for effectiveness in supporting successful digital transformation projects.
Cyberthreats	• AI-driven phishing and deepfake attacks are harder to detect, increasing risk of successful social engineering. • Collaboration gaps with external partners may delay threat intelligence sharing, weakening overall cyber defense.	• Evaluate detection and response capabilities for AI-driven phishing and deepfake threats. • Review external collaboration protocols for timely sharing and integration of threat intelligence.
Third-party risk management (TPRM)	• Extended enterprise risk is difficult to monitor, increasing exposure to unknown vulnerabilities in extended supply chains. • Sustainability non-compliance by vendors can lead to reputational damage and regulatory penalties for the organization.	• Assess extended enterprise risk identification and monitoring processes within the robust supply chain. • Review vendor Sustainability compliance assessments and escalation procedures for non-compliance incidents.

Elevating IT IA – Turning technology risks into business opportunities

- Deloitte guides organizations in confidently navigating **complex technology risks.**
- Backed by **deep specialization** in cyber, data governance, business systems, and emerging tech, we provide thorough audits and actionable insights.
- We advise clients to strengthen controls, enhance IT investments, and **build trust**.

Main Differentiator

By integrating specialists throughout the project delivery, Deloitte can provide more relevant and practical recommendations to IT and business stakeholders.

Our capabilities – 850+ core IT IA professionals, plus...

550+

Cyber IA

- Cybersecurity
- Cyber risk strategy
- Cyber maturity assessments

1,900+

IT Specialists

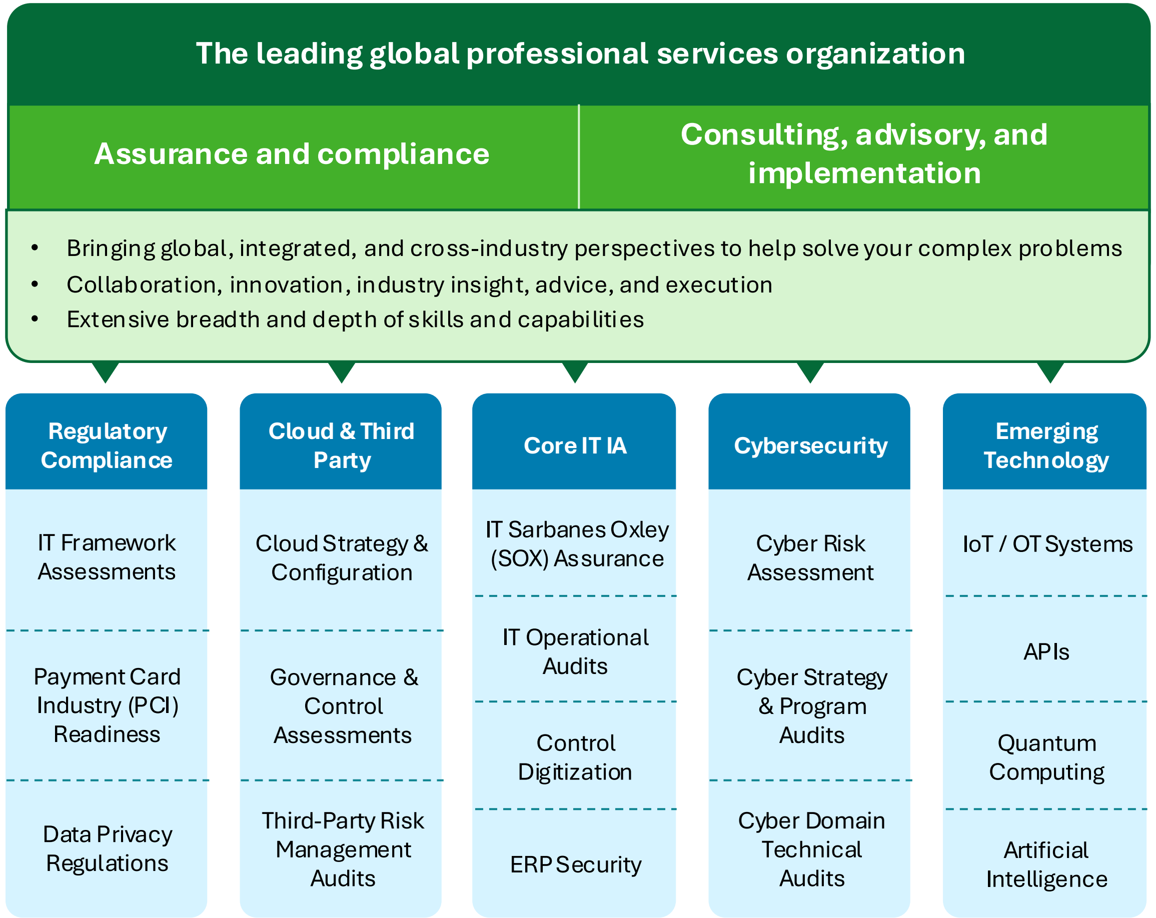
- Emerging technology
- Third-party assurance
- Enterprise resource planning (ERP) tools

1,250+

Certifications earned by our internal audit professionals (Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Project Management Professionals (PMP, Certified Internal Auditors (CIA), etc.)

Collaborating with the Institute of Internal Auditors (IIA) and industry associations on technology risk and cybersecurity standards.

Risk-focused experience powering client impact—delivers insight, trust, and measurable results. As the **largest global professional services network** in the world, Deloitte has extensive reach across technologies, industries and geographies.



The leading global professional services organization

Assurance and compliance

Consulting, advisory, and implementation

- Bringing global, integrated, and cross-industry perspectives to help solve your complex problems
- Collaboration, innovation, industry insight, advice, and execution
- Extensive breadth and depth of skills and capabilities

Regulatory Compliance

- IT Framework Assessments
- Payment Card Industry (PCI) Readiness
- Data Privacy Regulations

Cloud & Third Party

- Cloud Strategy & Configuration
- Governance & Control Assessments
- Third-Party Risk Management Audits

Core IT IA

- IT Sarbanes Oxley (SOX) Assurance
- IT Operational Audits
- Control Digitization
- ERP Security

Cybersecurity

- Cyber Risk Assessment
- Cyber Strategy & Program Audits
- Cyber Domain Technical Audits

Emerging Technology

- IoT / OT Systems
- APIs
- Quantum Computing
- Artificial Intelligence

Contacts

For more information contact our team today:

Vipul Patel

Audit & Assurance
Managing Director
IT Internal Audit Leader
Deloitte & Touche LLP
vbpatel@deloitte.com

Greg Boehmer

Audit & Assurance
Managing Director
Cyber Internal Audit Leader
Deloitte & Touche LLP
gboehmer@deloitte.com

Pete Low

Audit & Assurance
Managing Director
IT Internal Audit
Deloitte & Touche LLP
plow@deloitte.com

Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

The services described herein are illustrative in nature and are intended to demonstrate our experience and capabilities in these areas; however, due to independence restrictions that may apply to audit clients (including affiliates) of Deloitte & Touche LLP, we may be unable to provide certain services based on individual facts and circumstances.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.