Deloitte.

2026 Internal Audit
Hot Topics

November 2025

Internal Audit Hot Topics for 2026

Organizations continue to navigate an era of relentless disruption — from shifting economic conditions and geopolitical tension to rapid advances in artificial intelligence (AI) and digital technology. These forces are reshaping how businesses operate and introducing new, interconnected risks across strategy, operations, and technology. For Internal Audit (IA), 2026 presents an opportunity to become a **strategic partner in navigating complexity and driving value**.

At Deloitte, we believe Internal Audit is entering its most transformative era — one that amplifies the value IA can bring to the organization. *Deloitte's Internal Audit Hot Topics for 2026* explores where we believe IA can deliver the greatest impact across the following **Operational** and **Information Technology/Cyber** priorities:

- **Mega Hot Topic:** *Agentic AI* — a defining theme for 2026, presenting both an opportunity for innovation and a new frontier of risk.
- **Operational Internal Audit priority areas:** Mergers & Acquisitions, Business and System Transformations, Regulatory Compliance Readiness, Capital Program Assurance, Supply Chain & Tariffs, Third-Party Risk Management, and Resilient Business.
- **Technology and Cyber Internal Audit priority areas:** Vulnerability Management, Identity & Access Management, Quantum Computing, Operational Technology (OT) & Information Technology (IT) Convergence, Cloud Governance & Security, Application Programming Interfaces, and Network Security.

Together, these topics reflect Deloitte's perspective on how Internal Audit can **strengthen resilience, enable responsible innovation, and elevate trust** — helping organizations move beyond assurance to shape the future of sustainable performance.

In parallel, Deloitte has released a **sister publication — *Internal Audit Operations Focus Areas for 2026* —** which highlights the key operational and strategic priorities emerging within Internal Audit functions themselves, including operating model refresh, leveraging Agentic AI within IA, digital enablement, GRC tool selection, talent development, innovation, connected risk across the three lines, and adoption of the new Global IA Standards.

2026 Mega Hot Topic:
Agentic Artificial Intelligence (AI)

Mega Hot Topic: Agentic AI

Agentic AI: An Emerging Opportunity and Risk for Internal Audit

WHAT IS AGENTIC AI?

Agentic Artificial Intelligence (Agentic AI) refers to AI systems capable of **autonomously planning, executing, and adapting actions** to achieve complex objectives with minimal human intervention. Unlike traditional generative AI tools that primarily respond to prompts, Agentic AI solutions operate more like **digital "agents"—connecting across systems, making decisions, initiating tasks, and learning from outcomes**. By 2026, these solutions are expected to become embedded across business functions, from customer engagement and finance automation to supply chain optimization and cybersecurity defense.

For organizations, Agentic AI offers the potential for exponential efficiency gains and innovation. Yet, its very autonomy introduces new categories of **governance, risk, and control challenges** that Boards and management should navigate carefully.

SELECT RISKS OF AGENTIC AI

While transformative, Agentic AI introduces distinct risks that Internal Audit should assess:

Accountability & Transparency: It is often unclear who is accountable when an AI agent acts independently, complicating incident response and regulatory scrutiny.

Decision-Making Risk: Autonomous systems may make incorrect or biased decisions at scale, leading to compliance, ethical, or reputational failures.

Control Bypass Risk: Agentic solutions may initiate actions outside of established approval chains, exposing organizations to fraud, financial misstatements, or data breaches.

Cyber & Adversarial Attacks: Malicious actors could manipulate AI agents through prompt injection, model poisoning, or system exploitation.

Shadow AI: Business units may deploy Agentic AI without enterprise oversight, creating parallel, uncontrolled processes.

Data Privacy & Breaches: AI agents can inadvertently access, process, or share confidential and sensitive information.

Mega Hot Topic: Agentic AI

Agentic AI: Audit Considerations

AUDIT CONSIDERATIONS RELATED TO AGENTIC AI FOR 2026

To provide the Board and executive leadership with confidence that Agentic AI is well-governed, Internal Audit should focus on targeted reviews in 2026, including:

Governance & Oversight Audits

Evaluate whether the organization has established clear accountability, ownership, and policies for Agentic AI deployment.

Operational Integration Audits

Consider how Agentic AI solutions are embedded in core business processes and whether appropriate approval workflows, controls, and fail-safes are maintained.

Ethics, Bias, and Model Risk Management Audits

Assess whether models are tested for fairness, explainability, and compliance with regulatory standards.

Shadow AI Risk Assessments

Identify unapproved or unmonitored uses of Agentic AI across business units and evaluate enterprise-wide inventory and monitoring practices.

Cybersecurity & Resilience Audits

Review the controls in place to protect Agentic AI from adversarial attacks, unauthorized access, and data leakage.

Human in the Loop Architecture Review

Evaluation of AI-driven processes and systems to ensure critical decision points utilize human oversight, review, and discretion.

Mega Hot Topic: Agentic AI

Agentic AI: Opportunities for Internal Audit

OPPORTUNITIES FOR INTERNAL AUDIT TO LEVERAGE AGENTIC AI

Internal Audit is uniquely positioned to model responsible adoption by harnessing Agentic AI in its own practices. Opportunities include:

- **Continuous auditing and monitoring:** Deploy AI agents to autonomously test controls, flag anomalies, and track transactions in near real time to expand assurance coverage.
- **Risk sensing and trend analysis:** Integrate agentic tools that continuously scan internal and external data to detect emerging risks and trigger adaptive audit responses.
- **Dynamic audit planning and scoping:** Enable AI-driven analysis of risk registers, operational data, and external indicators to dynamically prioritize audit focus areas.
- **Controls rationalization:** Use AI agents to interpret control documentation, identify redundancies, and recommend streamlined, risk-aligned control frameworks.
- **Quality assurance automation:** Apply agentic AI to review large volumes of audit documentation, highlighting inconsistencies or anomalies against internal methodologies and Global IA Standards for auditor validation.
- **Responsible adoption:** Pilot these use cases within a structured governance framework to ensure transparency, accountability, and ethical AI use within IA operations.

By piloting these use cases, IA can demonstrate the responsible use of Agentic AI while simultaneously improving assurance delivery.

CLOSING PERSPECTIVE ON AGENTIC AI

*Agentic AI will be both a **game-changer and a governance challenge**. For Internal Audit, 2026 presents an **opportunity to be at the forefront** — assuring Boards and management that organizations are not only **protected from the risks** of autonomous AI agents but also **positioned to responsibly unlock their transformative potential**.*


2026 Operational Internal Audit Hot Topics

Operational Internal Audit Hot Topics for 2026

IA's role has never been more critical in helping organizations navigate disruption. As businesses balance transformation, regulation, and resilience, the following seven operational hot topics represent the priority areas for Operational Internal Audit focus in 2026.

01 MERGERS & ACQUISITIONS (M&A)

Why it matters

M&A activity is accelerating as organizations seek growth, technology capabilities, and supply chain diversification. Transactions are increasingly scrutinized by regulators and investors, raising the stakes for effective integration.

Internal Audit Focus Areas

- **Due diligence robustness:** Assess whether compliance, cultural fit, and technology integration risks are thoroughly addressed in the diligence process to avoid costly surprises.
- **Separation and transition integrity:** Review transition service agreements and post-merger separation plans to provide operational continuity and decrease execution risk.
- **Financial reporting and synergy confidence:** Provide independent assurance over financial reporting readiness and validate that synergy targets are realistic, measured, and achieved.
- **Integration governance**: Test the effectiveness of integration governance frameworks, to promote clear accountability, oversight, and tracking of progress against strategic objectives.

02 TRANSFORMATION (SYSTEM & BUSINESS)

Enterprises are modernizing systems, operating models, and business strategies to compete in an AI-enabled economy. Transformation creates value but also significant risk if controls are overlooked.

- **Program governance and oversight:** Test whether transformation initiatives have effective governance, clear steering committee accountability, and transparent risk reporting to the Board.
- **Control design and assurance:** Validate that controls are embedded during system implementation and confirmed through rigorous post–go-live reviews, avoiding costly retrofits.
- **Change management and culture**: Assess the effectiveness of change management strategies, training programs, and cultural alignment to facilitate adoption and decrease disruption.
- **Benefits realization:** Review whether transformation outcomes are tracked against the original investment case, and confirm that intended efficiencies and strategic benefits are achieved.

Operational Internal Audit Hot Topics for 2026 continued

03 CAPITAL PROGRAM ASSURANCE

Why it matters

Effective oversight of capital programs is critical to determine strategic alignment, disciplined capital allocation, and value preservation. As organizations balance competing funding priorities and pursue partnerships to share risk, strong governance throughout the project lifecycle helps prevent dilutive or inefficient investments.

Internal Audit Focus Areas

- **Capital governance and prioritization:** Assess whether capital allocation frameworks and governance processes effectively prioritize projects based on strategic value, risk, and return.
- **Financial discipline and integrity**: Evaluate cost controls, procurement practices, and partnership structures to promote transparency, accountability, and equitable risk sharing.
- **Sustainability and reporting assurance:** Provide independent assurance that Sustainability-related disclosures tied to capital projects are accurate, consistent, and free from greenwashing risk.
- **Resilience and lifecycle oversight:** Test whether governance discipline — including adherence to stage gates and approval criteria — is maintained throughout the project lifecycle to prevent value erosion.

04 SUPPLY CHAIN & TARIFFS

Geopolitical volatility, tariffs, and climate disruption are reshaping supply chains. Resilient and ethical sourcing is no longer optional — it's a license to operate.

- **Resilience and diversification:** Assess whether supply chain strategies are designed to withstand disruption, including diversification of sourcing and monitoring of tariff exposures.
- **Supplier governance and integrity:** Test controls over supplier onboarding, ongoing monitoring, and ethical compliance, determining alignment with regulations on forced labor and sustainability.
- **Cybersecurity of logistics systems:** Review the resilience of digital logistics and inventory platforms against cyber threats, ransomware, and system outages.
- **Contingency and recovery planning:** Evaluate the contract terms and conditions in place to mitigate damage due to supplier failure and the strength of contingency plans, including backup sourcing, rapid re-routing, and crisis response capabilities.

9

Operational Internal Audit Hot Topics for 2026 continued

05 REGULATORY COMPLIANCE READINESS & REMEDIATION

Why it matters

The pace of regulatory change across AI, Sustainability, data privacy, and financial reporting continues to accelerate. Strong monitoring of changing landscapes and agility is essential. Proactive compliance and remediation are essential to avoid reputational and financial penalties.

Internal Audit Focus Areas

- **Regulatory readiness & overlap:** Conduct readiness reviews and gap assessments, mapping overlaps across jurisdictions and emerging rule sets (AI & Digital, Operational Resilience, Prudential & Financial Reporting, Sustainability & Conduct) to highlight risks and reduce compliance duplication.
- **Remediation governance:** Evaluate how regulatory findings are tracked, escalated, and closed — to confirm that remediation is timely, consistent, and independently overseen.
- **Data integrity & reporting confidence:** Test the reliability of financial, prudential, and Sustainability reporting by reviewing data lineage, audit trails, and controls supporting disclosures.
- **Compliance culture & accountability**: Assess tone at the top, governance structures, and regional variations to facilitate a sustainable, enterprise-wide compliance culture.
- **Third-party reliance:** Provide assurance that outsourced and third-party services critical to regulatory compliance are governed, monitored, and resilient.

06 RESILIENT BUSINESS

Disruption is constant — from cyber incidents to climate events. Boards are demanding evidence that resilience is not just regulatory compliance but an embedded organizational capability.

- **Enterprise resilience by design:** Review whether resilience frameworks and scenario planning are comprehensive, regularly updated, and aligned with organizational strategy.
- **Cyber and climate readiness:** Test the effectiveness of cyber defenses and climate resilience capabilities to determine that the business can withstand the most likely and most severe disruptions.
- **Governance and crisis leadership:** Evaluate the role of governance, including Board and executive oversight, in directing and monitoring crisis management and recovery activities.
- **Operational integration:** Assess whether resilience practices are embedded into day-to-day operations — not treated as standalone exercises — to build a culture of preparedness and agility.

Operational Internal Audit Hot Topics for 2026 continued

07 THIRD-PARTY RISK MANAGEMENT (TPRM)

Why it matters

Organizations increasingly operate within complex ecosystems of third and fourth parties — as well as partnerships and joint ventures (JV) formed to share risk and manage constrained capital. These interconnected relationships expand the organization's risk surface, while regulatory regimes such as European Union (EU) Digital Operational Resilience Act (DORA) and the UK Critical Third Parties framework are imposing higher expectations for oversight, resilience, and accountability.

Internal Audit Focus Areas

- **End-to-end lifecycle assurance:** Review governance and controls across the lifecycle of third parties, partners, and JVs — from onboarding to exit — facilitating consistent oversight and accountability.
- **Concentration and resilience risk:** Evaluate exposure to key providers and strategic partners, including JVs, and assess contingency and exit plans.
- **Partnership governance:** Assess how partnership and JV agreements define roles, risk-sharing mechanisms, and performance oversight.
- **Regulatory compliance:** Confirm that third-party and partnership practices meet emerging oversight requirements (e.g., DORA, UK Critical Third Parties, U.S. banking guidance).
- **Extended ecosystem visibility:** Evaluate monitoring and reporting of subcontractors and fourth-party relationships to facilitate transparency and risk coverage.

CLOSING PERSPECTIVE ON OPERATIONAL INTERNAL AUDIT

*2026 presents a defining moment for Internal Audit. Boards and executives will **expect assurance not just over traditional risks**, but over how effectively the enterprise is **embedding resilience, compliance, and transformation discipline** into its operational fabric. By considering these seven operational hot topics, Internal Audit can **provide assurance that organizations are future-ready** — while also modeling the adaptive, technology-enabled practices required to thrive.*

2026 Information Technology and Cyber Internal Audit Hot Topics

Information Technology & Cyber Internal Audit Hot Topics for 2026

As organizations accelerate digital transformation, the IT and cyber landscape is reshaped by AI-powered attacks, emerging quantum threats, and the convergence of IT and OT systems. Cloud complexity, identity risks, and Application Programming Interface (API) sprawl further expand the attack surface. For Boards, assurance is no longer about whether cyber defenses exist — but whether they are resilient, adaptive, and governed by design. Internal Audit should provide confidence that technology and cyber risks are being managed in line with the organization's appetite and regulatory.

01 VULNERABILITY MANAGEMENT

Why it matters

Exploits move faster than ever, with AI-driven scanning tools enabling adversaries to weaponize vulnerabilities at machine speed. Timely detection and patching are essential to protect enterprise resilience.

Internal Audit Focus Areas

- **Scanning and patching discipline:** Assess whether vulnerability management programs are proactive, automated, and effective in keeping pace with fast-moving exploits.
- **Threat intelligence integration:** Review how external intelligence and AI-driven analytics are incorporated into monitoring and patching strategies.
- **Zero-day readiness:** Evaluate governance and response plans for emerging zero-day vulnerabilities to confirm the organization can act swiftly and decisively.

02 IDENTITY & ACCESS MANAGEMENT (IAM)

With cloud, remote work, and digital-first operations, identity is the new perimeter. Weak IAM is now the most common entry point for attackers.

- **Maturity and framework alignment:** Review IAM practices against leading standards (e.g., Zero Trust, National Institute of Standards and Technology (NIST)) to identify maturity gaps.
- **Privileged access controls:** Test oversight of privileged accounts, logging, and monitoring to mitigate insider and external threat risks.
- **Authentication resilience:** Evaluate multi-factor authentication (MFA) coverage and reliability across employees, partners, and customers.
- **Real-time monitoring:** Assess incident detection and response capabilities to determine whether identity monitoring balances security with business continuity.

Information Technology & Cyber Internal Audit Hot Topics for 2026 continued

03 QUANTUM COMPUTING

Why it matters

Quantum breakthroughs threaten to break current encryption standards, creating systemic risk to sensitive data. Preparing for quantum-safe cryptography is now an enterprise imperative.

Internal Audit Focus Areas

- **Quantum readiness roadmap**: Evaluate the organization's plan for migrating to quantum-safe cryptography and protecting high-value data assets.
- **Encryption transition governance:** Review whether strategies and timelines for cryptographic upgrades are aligned with regulatory and industry guidance.
- **Vendor and ecosystem resilience:** Assess reliance on third-party providers and their readiness for quantum security risks.

04 OPERATIONAL TECHNOLOGY (OT) & IT CONVERGENCE

Internet of Things (IoT), industrial automation, and digital integration are driving convergence of OT and IT systems. While this creates efficiencies, it also exposes legacy infrastructure to cyber threats.

- **Incident response integration:** Test joint OT/IT incident response plans, facilitating effective segregation, detection, and escalation protocols.
- **Legacy asset security:** Review patching, monitoring, and governance of legacy OT systems vulnerable to modern cyber threats.
- **Asset inventory integrity:** Assess whether all OT and IoT assets are identified, tracked, and managed within enterprise risk frameworks.
- **Safety-critical resilience:** Evaluate controls to protect physical safety and operational continuity in converged OT/IT environments.

Information Technology & Cyber Internal Audit Hot Topics for 2026 continued

05 CLOUD GOVERNANCE & SECURITY

Why it matters

By 2026, most organizations operate in hybrid and multi-cloud environments. Governance challenges span compliance, sovereignty, resilience, and cost.

Internal Audit Focus Areas

- **Configuration assurance:** Review cloud configuration management and monitoring to prevent misconfigurations and breaches.
- **Regulatory compliance**: Test adherence to General Data Protection Regulation (GDPR), Network and Information Security Directive 2 (NIS2), DORA, and local data sovereignty requirements across jurisdictions.
- **Data governance and sovereignty:** Assess controls for secure storage, access, and transfer of data across global operations.
- **Vendor resilience and sustainability:** Evaluate provider diversification, resilience planning, and Sustainability alignment of cloud strategies.

06 APPLICATION PROGRAMMING INTERFACES (APIs)

APIs enable agility and innovation but also introduce new attack vectors. Unmanaged sprawl creates blind spots in digital ecosystems.

- **API inventory and governance:** Review the completeness of enterprise-wide API inventories and governance frameworks.
- **Security assurance:** Test coding practices, penetration test results, and monitoring processes for API vulnerabilities.
- **Third-party integrations:** Assess the risks introduced by external APIs and confirm compliance with enterprise security standards.

Information Technology & Cyber Internal Audit Hot Topics for 2026 continued

07 NETWORK SECURITY

Why it matters

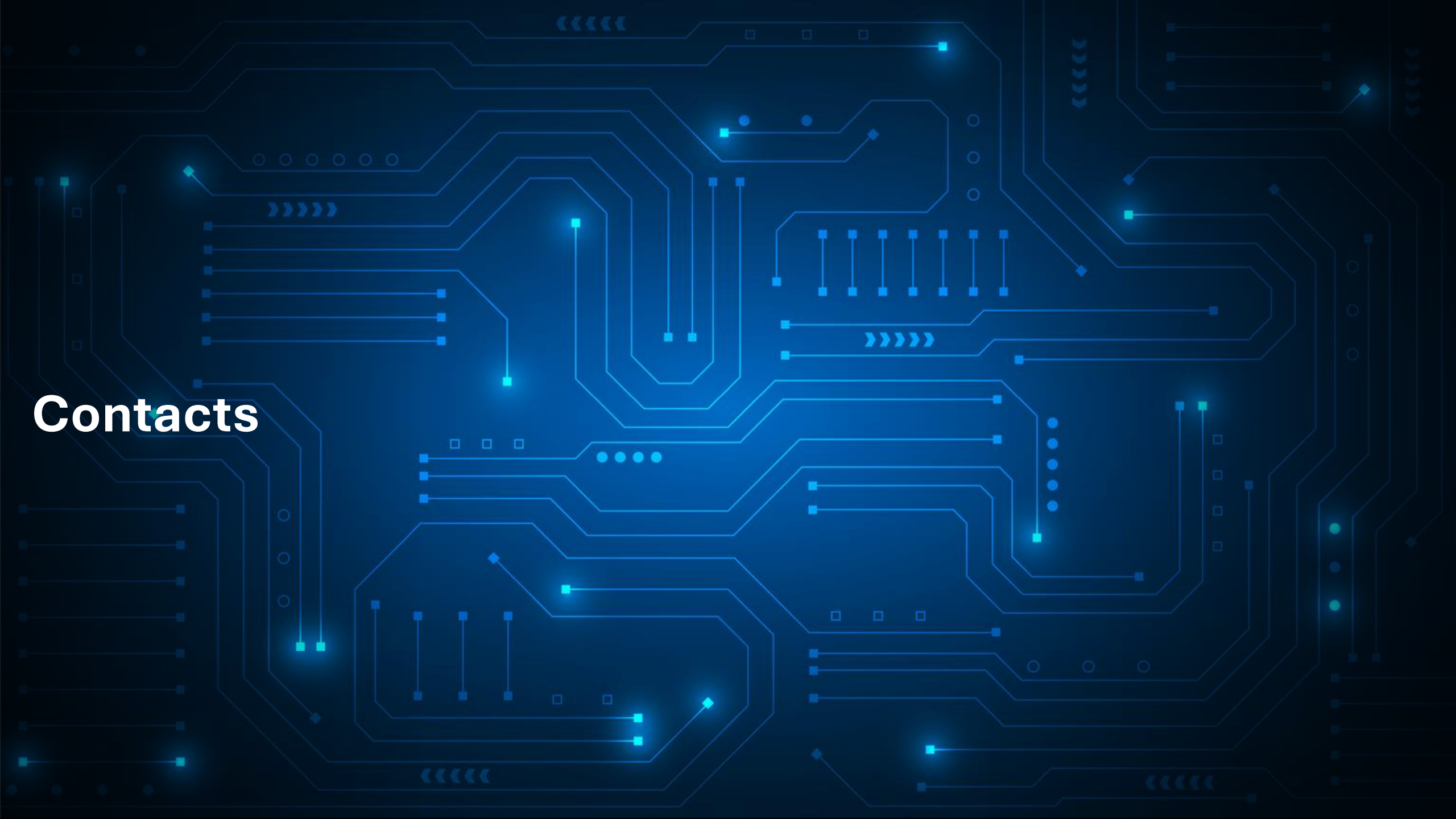
Network defenses underpin the foundation of the enterprise risk posture. In 2026, attackers are leveraging AI and edge computing vulnerabilities to outpace traditional security models.

Internal Audit Focus Areas

- **AI-driven detection:** Evaluate whether network defenses leverage AI-enabled threat detection and response to stay ahead of adversaries.
- **Micro-segmentation assurance:** Test the accuracy of segmentation controls to prevent both over-restriction and exposure of critical assets.
- **Edge and endpoint resilience:** Review protections for remote and edge environments, facilitating coverage across the extended enterprise.

CLOSING PERSPECTIVE ON IT AND CYBER INTERNAL AUDIT

*Cyber and digital risks in 2026 are **faster, interconnected, and harder to contain**. Boards and Audit Committees should expect Internal Audit to **bring forward evidence-based assurance** across vulnerability, identity, quantum, OT/IT, cloud, API, and network domains — so that the organization is both **protected and future-ready**.*


Contacts

Contacts

Steffen Pietz
Partner
Deloitte Switzerland
spietz@deloitte.ch

Alan Murray
Director
Deloitte Switzerland
awmurray@deloitte.ch

Olivier Lagrange
Senior Manager
Deloitte Switzerland
olagrange@deloitte.ch

Nicole Guyot
Senior Manager
Deloitte Switzerland
nguyot@deloitte.ch

Filipa Alves
Assistant Manager
Deloitte Switzerland
afalves@deloitte.ch

Paola Wong Hernandez
Manager
Deloitte Switzerland
pswonghernandez@deloitte.ch

Philipp Christ
Manager
Deloitte Switzerland
pchrist@deloitte.ch

Alyssa Pasini
Analyst
Deloitte Switzerland
aapasini@deloitte.ch

Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845