ahia
Assoc. of Healthcare Internal Auditors

protiviti®
Global Business Consulting

Reimagining Healthcare Internal Audit: Leading Through Change

Key findings from the latest study conducted by Protiviti and AHIA on internal audit plan priorities for healthcare organizations

Table of Contents

Executive Summary

The continuing rapid rise of AI, alongside evolving regulatory expectations and growing operational complexity, is reshaping the healthcare risk landscape at a never-before-seen pace. What is different in 2026 is not simply that these risks remain on the radar; it is how quickly they are converging. Cyber threats, including ransomware and AI-enabled attacks, remain pervasive. Expanding reliance on third parties, complex workforce models and emerging technologies continue to introduce new dimensions of risk. At the same time, ongoing margin pressures, supply chain disruptions and heightened scrutiny over revenue cycle integrity, financial stewardship and compliance further elevate the importance of a robust and forward-looking internal audit (IA) function.

Leading internal audit functions are challenging themselves by asking, "How can we use AI, analytics and other tools/technologies on every audit we perform and throughout the entire audit lifecycle?" For provider and payer organizations alike, internal audit continues to be looked to as a strategic partner, supporting innovation, evaluating emerging risks and enabling informed decision-making. By aligning audit plans to these evolving priorities, organizations can better anticipate disruption, protect financial and operational performance, and maintain trust with management, patients, members, regulators and other key stakeholders.

Top healthcare internal audit plan priorities

#	Cross-Segment	#	Provider	#	Payer
1	Cybersecurity	1*	Charge capture	1	Claims processing
2	Procurement and supply chain	1*	Revenue cycle compliance and transparency	2	Delegates/vendors/first-tier, downstream and related entities
3	Payroll and benefits	3	Back-end revenue cycle operations	3	Pharmacy/pharmacy benefit manager
4	AI and other emerging technologies	4	Physician arrangements and referrals	4*	Benefit configuration
5*	Joint ventures, third parties and outsourced services	5	Front-end revenue cycle operations	4*	Members
5*	User access and identity management			4*	Risk adjustment/coding

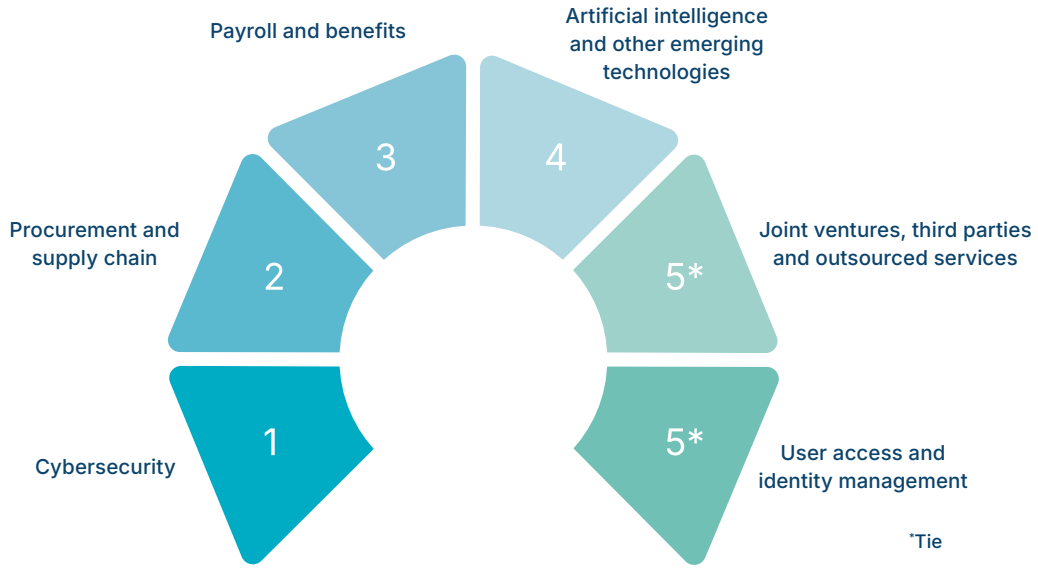
*Tie

Healthcare organizations are navigating unprecedented levels of change that are challenging traditional approaches to governance, risk management and oversight. The rapid adoption of AI, evolving regulatory expectations, escalating cybersecurity threats and sustained financial pressures are redefining the risk landscape. In this environment, internal audit has an opportunity to move beyond assurance and serve as a trusted strategic advisor helping leadership build confidence, manage uncertainty and make informed decisions that enable sustainable transformation and improved performance.

Richard Williams
Managing Director
Global Practice Leader, Healthcare Industry
Protiviti

Cross-Segment Priorities

Top Priorities



The healthcare risk landscape is becoming increasingly interconnected. As organizations embrace AI and digital transformation, new efficiencies are emerging alongside these new risks. Managing those opportunities and risks requires governance models that can adapt as quickly as the environment itself.

01 Cybersecurity

Cybersecurity remains the number one cross-segment internal audit priority for the fourth consecutive year, and the threat environment has accelerated, as healthcare remains the number one targeted sector for ransomware and cyberattacks[1]. Some estimates put the average cost of a U.S. healthcare data breach at approximately $11 million per incident, underscoring the significant financial and operational exposure organizations face. Ransomware-driven outages still routinely exceed 30 days at impacted healthcare organizations, directly disrupting patient care, revenue and reputation. The arrival of AI models such as Anthropic's Mythos, which can discover and exploit vulnerabilities, collapsing the window between disclosure and weaponization, drives the need for organizations to accelerate their cybersecurity maturity even more acutely. At the same time, connected medical devices and operational technology continue to lag enterprise IT in patching, segmentation and monitoring, creating patient-safety exposure. Unstructured data that has proliferated for years within organizations now also creates much more risk with tools able to scan for, find and use that unstructured data in furthering attacks or compromising sensitive information.

Key audit areas to consider include:

- **Security program maturity assessments:** Evaluate posture against recognized security frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 and the U.S. Department of Health and Human Services (HHS) Cybersecurity Performance Goals, as well as consider Payment Card Industry (PCI) compliance assessments for the protection of any cardholder data.
- **Technical security and adversary simulation testing:** Assess the organization's ability to technically detect, protect, respond and recover from a targeted threat-actor event, including phishing or use of voice or video deepfakes. Essentially, simulate the actions a real-world attacker would try to perform.
- **Ransomware readiness and incident response (IR):** Assess tested IR plans, isolated/immutable backups, recovery objectives and post-incident lessons learned.
- **Medical devices and operational technology security:** Confirm device discovery, segmentation, vulnerability management, inventory validation and compensating controls for legacy equipment.
- **Unstructured data protection:** Assess discovery, classification, data loss prevention and access governance across email, Microsoft SharePoint, Microsoft Teams, imaging and ambient documentation.
- **AI and agentic-AI exposure:** Evaluate patching velocity, scoped credentials, human-in-the-loop and kill-switch controls in light of Mythos-class capabilities.
- **Third-party risk management:** Assess how third parties are evaluated for risk and managed throughout their lifecycle, including considerations for resiliency of your organization without these third parties available.

[1] American Hospital Association, "*FBI: Health Care Was Top Target for Ransomware, Other Cyberthreats in 2025*," AHA News, April 10, 2026.

02 Procurement and supply chain

Procurement and supply chain functions remain a top priority for internal audit as healthcare organizations face ongoing margin pressures, cost containment expectations, global supply disruptions and increased reliance on third parties. Rising inflation, labor shortages and global instability have intensified the need for disciplined sourcing, effective use of group purchasing organizations (GPOs), and real-time visibility into spend and inventory.

At the same time, decentralized purchasing and evolving supplier ecosystems introduce risks related to contract compliance, pricing integrity, inventory accuracy and asset management. Internal audit plays a critical role in assessing whether procurement and supply chain operations are well governed, aligned to organizational strategy and supported by strong controls that mitigate financial, operational and compliance risks while maintaining continuity of care.

Key audit areas to consider include:

- **Contract utilization and GPO compliance:** Assess utilization of GPOs and approved supplier contracts, including adherence to negotiated pricing, tier commitments and rebate programs, to identify off-contract spend, missed savings opportunities and gaps in contract compliance.
- **Procure-to-pay (P2P) controls and compliance:** Evaluate end-to-end P2P processes to ensure proper approvals, segregation of duties and policy adherence, reducing risk of unauthorized spend, duplicate payments, fraud or noncompliant purchasing activity.
- **Third-party risk management (TPRM):** Assess processes for continuously monitoring supplier onboarding/setup/changes, financial health and contract performance against key performance indicators (KPIs) and/or service level agreements (SLAs), as well as cybersecurity, operational resiliency and regulatory compliance, to mitigate supply disruption and vendor performance and compliance risks.
- **Inventory management and visibility:** Evaluate inventory controls, accuracy and alignment to clinical demand to reduce risk of stockouts impacting care delivery, excess or obsolete inventory, and operational disruptions impacting patient care.
- **Fixed asset management:** Review capitalization, asset tracking, physical inventory procedures, depreciation and disposal controls to ensure fixed assets are safeguarded, patched, accurately recorded and managed in accordance with organizational policies.
- **Procurement data analytics and spend visibility:** Conduct data analytics to identify trends, anomalies and opportunities related to spending patterns, contract utilization, supplier spend and maverick purchasing. Assess whether management has adequate reporting and visibility to support cost control, compliance and strategic decision-making.

03 Payroll and benefits

Payroll and benefits remain high-risk areas for healthcare, driven by ongoing wage and hour litigation, recurring payroll process breakdowns, and heightened compliance risks from expanding unpaid sick leave laws in states such as California, New York, New Jersey and Washington.

Recent lawsuits and class actions make it clear that practices many organizations have relied on for years, such as time rounding, automatic meal deductions, overtime calculations, travel time treatment and exempt versus nonexempt classification, are increasingly being challenged as control failures rather than one-off administrative issues. Organizations should also monitor risks that directly impact cost and compliance, including ghost employees, excessive overtime trends, unexplained labor spikes by department, remote timekeeping practices and potential overstatement of hours worked.

Evolving benefit regulations require organizations to manage complex compliance obligations, including varying accrual rates, eligibility rules, recordkeeping and employee notifications. For multi-state employers, inconsistent application or misunderstanding of these requirements can lead to costly penalties, legal disputes and reputational damage.

Key audit areas to consider include:

- **Unpaid sick leave compliance:** Evaluate whether policies and processes are robust, consistently applied and responsive to changing state mandates.
- **Time rounding and automatic meal deductions:** Evaluate whether rounding rules and meal-deduction practices result in unpaid pre-shift, post-shift or missed-meal work, and whether exceptions are consistently identified, corrected and monitored.
- **Overtime calculations:** Assess whether overtime is calculated correctly across all applicable pay codes, including differentials and nondiscretionary bonuses.
- **Unpaid travel time (e.g., home health, mobile care):** Review controls to ensure compensable travel time between patient locations is captured, paid and appropriately included in payroll and overtime calculations.
- **Employee classification:** Verify employees are correctly classified as exempt or nonexempt based on job duties and compensation structure, and that classifications are consistently applied and periodically reviewed.
- **Employee notifications:** Assess timely and compliant employee notification of sick leave benefits, usage and policy changes.
- **Payroll system integration:** Verify payroll systems are integrated with financial and time-keeping systems to accurately track sick leave accruals, usage and balances.
- **Dependent eligibility:** Confirm dependents enrolled in benefit plans meet established eligibility criteria.

04 Artificial intelligence and other emerging technologies

Adoption of AI and other emerging technologies has expanded rapidly across the healthcare industry, with AI, advanced analytics and automation being applied across functions including clinical documentation/decision support, prior authorization, claims adjudication, member and patient engagement, and back-office automation as a few key examples. Expanding state regulations and anticipated federal guidance; executive actions focused on AI innovation; cybersecurity events caused by frontier AI models; and litigation over algorithm-driven coverage denials are placing greater focus on governance, transparency, fairness and human oversight.

Protiviti's *The Next Phase: AI and Human Collaboration Powering Internal Audit Transformation* further notes that internal audit can leverage AI across the end-to-end audit lifecycle to enhance processes, generate insights and elevate decision-making.[2] That point is particularly relevant here because the survey results show AI moving from a peripheral emerging technology issue to a practical planning, governance and execution priority for healthcare internal audit functions.

Boards and audit committees want assurance that AI and automation investments are generating value and that AI adoption and automated decision-making are being appropriately managed. Internal audit can provide independent assurance that these technologies are governed and monitored effectively and that investments are delivering expected value. Furthermore, internal audit teams are increasingly using AI in their day-to-day activities and, like other functions, are expected to do so in a responsible and well-governed manner, treating AI-generated content as input to be validated, not evidence to be accepted at face value.

[2] Protiviti, *The Next Phase: AI and Human Collaboration Powering Internal Audit Transformation*, July 2025.

Key audit areas to consider include:

- **AI governance structures, policies and procedures:** Assess roles, responsibilities, committee structure and escalation paths to govern AI and evaluate effectiveness of AI-related policies and procedures. Verify alignment of existing AI governance frameworks with third-party, legal, compliance, data governance and cybersecurity frameworks.
- **AI inventory:** Evaluate effectiveness of AI intake, inventory and risk-tiering processes. Assess controls over unsanctioned use or shadow AI, with periodic reassessment as organizational maturity and adoption evolve.
- **Targeted high-risk AI assessments:** Assess data quality and pre-processing, alignment of AI methodology with intended use, AI testing (including bias detection and explainability), model validation and recalibration processes, ongoing performance monitoring, and human-in-the-loop controls for high-risk use cases (e.g., patient care, clinical decision-making, billing and coding, coverage determinations).
- **AI strategy and initiatives:** Evaluate the organizational strategy for the use of AI, including defining appropriate AI initiatives in alignment with overarching business and technology objectives and key strategic metrics.
- **ROI and value realization:** Evaluate business-case discipline, benefits tracking and post-implementation reviews used to assess whether AI adoption is delivering expected value and is aligned to the AI strategy.
- **Ongoing AI monitoring and oversight:** Monitor key data points impacted by AI (e.g., coding and documentation accuracy, denial and appeal overturn rates, patient safety events, grievances) against pre-AI baselines to identify model drift, unintended impacts or adverse effects, and evaluate user override and acceptance patterns to assess human-review effectiveness.
- **Automation:** Evaluate governance and controls over automated processes (e.g., robotic process automation, rules-based decisioning, workflow automation), including process design, exception handling, monitoring, and impacts on accuracy, completeness and compliance.

Please refer to Appendix A for further discussion on the impact that AI, automation and advanced analytics are having on internal audit functions.

Internal audit teams are increasingly using AI in their day-to-day activities, and are expected to do so in a responsible and well-governed manner.

05* Joint ventures, third parties and outsourced services

Healthcare organizations are increasingly dependent on joint ventures and third-party providers to support core clinical, financial and operational functions. These arrangements introduce elevated exposure to regulatory noncompliance, financial leakage, data privacy breaches and operational disruption, particularly where vendors access protected health information (PHI), manage or support revenue cycle activities, or operate under complex performance-based contracts.

Internal audit can provide independent assurance that governance, oversight and accountability mechanisms are effectively designed and operating across the full third-party lifecycle. This includes validating adherence to payment terms, enforcement of SLAs, and alignment with regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and related Business Associate Agreements (BAA). Given the scale, criticality and regulatory scrutiny of these relationships, third-party and outsourced service provider oversight remains a top priority for internal audit.

Key audit areas to consider include:

- **Third-party risk management:** Assess enterprise processes for vendor risk identification, tiering, due diligence, governance, audit rights and ongoing oversight across the full third-party lifecycle.
- **Contract compliance and financial integrity:** Validate adherence to contract terms (e.g., pricing, payment structures, rebates, incentives) and accuracy and completeness of payments.
- **Service delivery and performance management:** Evaluate monitoring and enforcement of vendor performance against defined KPIs and SLAs, including escalation and remediation processes.
- **Privacy, security and third-party access:** Review controls governing vendor compliance with HIPAA/BAA and systems/sensitive data access including provisioning, monitoring and termination.
- **Business continuity and extended enterprise risk:** Assess critical vendor resiliency and subcontractor (fourth-party) relationship oversight, including business continuity capabilities and contingency planning.

Joint ventures and third-party provider arrangements introduce elevated exposure to regulatory noncompliance, financial leakage, data privacy breaches and operational disruption.

* Tie

05* User access and identity management

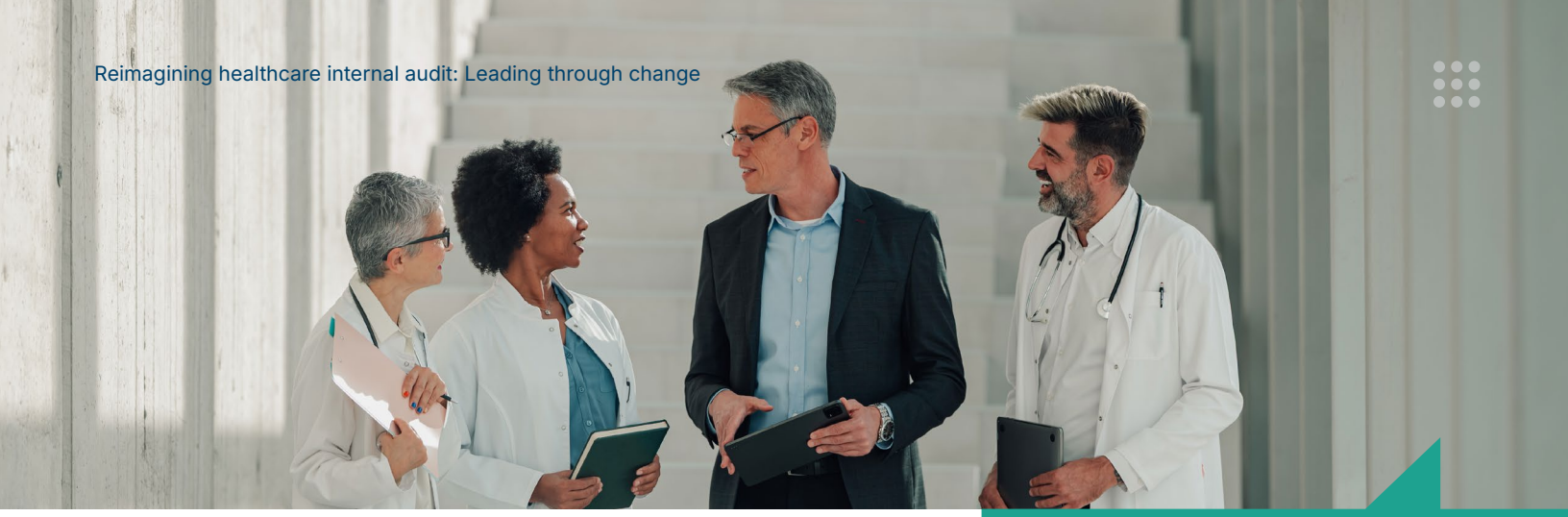
User access management is a top cross-segment priority due to compromised credentials that drive most healthcare breaches and a growing share of payer fraud loss. The challenge is complex: providers run hundreds of clinical applications on legacy platforms resistant to modern Identity and Access Management (IAM) practices, while payers extend access to brokers, delegated entities (e.g., third-party administrators (TPAs), pharmacy benefit managers (PBMs), carve-outs), provider offices and member-directed third-party applications under Centers for Medicare & Medicaid Services (CMS) interoperability rules. Nonhuman identity accounts like service accounts, machine identities, CMS Application Programming Interface (API) keys and AI agents, now outnumber human users roughly 80-to-1, with weak ownership, stale credentials and overprivileged access.[3] Workforce churn compounds the human side, with frequent turnover of clinicians, locum tenens, agency staff, contractors and offshore call-center workers while AI-driven deepfakes raise the stakes for help-desk resets, remote onboarding and member services.

Key audit areas to consider include:

- **Identity validation for workforce, members and consumers:** Assess processes related to identity proofing at hire, help-desk resets and member-portal registration, defending against deepfake impersonation, credential stuffing and account-takeover fraud.
- **Multifactor authentication (MFA) and phishing-resistant authentication:** Verify MFA across remote, privileged, clinical, broker and provider/member portals, without legacy SMS or bypass exceptions.
- **Least privilege and entitlement governance:** Move beyond assigning broad but basic access that only covers a few systems based solely on job roles by conducting detailed reviews of user permissions, monitoring for segregation-of-duties conflicts, and periodically validating access across key clinical, claims and administrative applications.
- **Nonhuman identity accounts and secrets management:** Audit ownership, vaulting, rotation and decommissioning of service accounts, machine identities, API keys and certificates.
- **Privileged access management (PAM):** Review vaulting, session monitoring and just-in-time elevation, and conduct quarterly reviews of break-glass and privileged human and service accounts.
- **Joiner-mover-leaver and stale-account discipline:** Audit provisioning, acquisition, transfer, termination and dormant-account cleanup for clinicians, locum tenens, contractors, brokers, delegated entities and machine accounts.
- **Third-party, interoperability and agentic AI access:** Evaluate federated access for TPAs, PBMs, partners and CMS API consumers; verify scoped credentials, human-in-the-loop and kill-switch controls for AI agents acting on users' behalf.

* Tie

3 CyberArk, "*Machine Identities Outnumber Humans by More Than 80 to 1*," press release, April 23, 2025.



Cross-Segment Additional Areas of Focus

Accounts payable

A focus on Accounts Payable (AP) is important for audit professionals, given its high transaction volume, vendor diversity and elevated fraud and compliance risk. Healthcare AP encompasses payments to a range of parties (e.g., physicians, medical suppliers, pharmaceutical distributors, contract clinicians, service vendors), each carrying regulatory exposure under the Stark Law, the Federal Anti-Kickback Statute, and Internal Revenue Service (IRS) reporting rules, where improper payments can trigger penalties. Duplicate payments, fictitious vendors and inflated invoices are fraud schemes that thrive in decentralized environments with multiple facilities or lines of business and Enterprise Resource Planning (ERP) instances. AP for healthcare providers and payers also intersects with 340B drug pricing, GPO rebates, capitated arrangements and broker commissions, where payment accuracy directly affects margin. Weak segregation of duties, vendor master file governance, manual invoice approval/ routing, and PHI-adjacent vendor data create operational and cybersecurity vulnerabilities. Rising costs and razor-thin operating margins cause organizations to use AP to preserve cash and optimize payment timing. Focusing on AP allows auditors to surface financial leakage, strengthen working capital and internal controls, and protect the organization from fraud and regulatory, reputational and financial harm.

Focusing on Accounts Payable allows the auditor to surface financial leakage, strengthen working capital and internal controls, and protect the organization from fraud and regulatory, reputational and financial harm.

Business continuity and resiliency

Business continuity and resiliency remain a top internal audit priority within healthcare organizations due to the potential impact operational disruptions can have on patient care, regulatory compliance, financial performance and organizational reputation. Healthcare providers and payers operate in highly interconnected environments that rely on continuous availability of Electronic Health Records (EHRs) that manage clinical and revenue cycle processes, claims systems, other core technology platforms, and external service providers like clearinghouses. As cyber incidents, technology outages, and n^{th}-party disruptions continue to increase across the industry, internal audit plays an important role in evaluating whether resiliency capabilities are adequately designed, governed and operationalized. This includes assessing alignment between business continuity, IT disaster recovery (ITDR), cyber incident response, crisis management and n^{th}-party resiliency programs, as well as evaluating dependency mapping (i.e., potential single points of failure), recovery testing, downtime procedures and escalation protocols to help confirm the organization can sustain critical operations during disruptive events.

Employee, provider and vendor verifications

Verification processes are top of mind as weak controls or insufficient oversight can directly impact patient safety, regulatory compliance, financial integrity and organizational reputation across all healthcare environments. Failures in key verification activities, including employment eligibility, background and exclusion screenings, licensing, credentialing and privileging, and vendor due diligence can result in unqualified or excluded individuals delivering care, administering benefits, accessing sensitive systems, and administering or receiving improper payments to ineligible providers or vendors, increasing exposure to sanctions and fraud, waste and abuse risks. Risks in these areas are amplified by workforce shortages, reliance on third parties and delegated functions, decentralized onboarding and network models, and evolving federal, state and accreditation requirements. Internal audit plays a critical role in providing independent assurance that verification processes are effectively designed, consistently applied, and supported by strong governance to protect patients and members and maintain trust.

Financial planning, integrity, reporting and stewardship

As the central component in safeguarding organizational resources and informing strategic decisions, financial planning, integrity, reporting and stewardship are paramount areas of focus for an internal auditor in a healthcare organization. The healthcare financial environment operates under intense scrutiny from boards, bondholders, CMS, state regulators and tax authorities, where inaccurate forecasts, misstated reserves or flawed financial reporting can jeopardize reimbursement, credit ratings, regulatory compliance, nonprofit tax status, capital access and overall financial sustainability. Budgeting and planning processes drive critical decisions around capital allocation, product and service line performance (e.g., clinical services, health plan offerings), provider reimbursement models, network contracting and operational investments. Errors in underlying assumptions, such as utilization trends, reimbursement rates, medical cost projections or risk adjustment factors, can materially distort financial results and strategic decision-making.

Reporting integrity is further strained by complex revenue and expense recognition models. For providers, this includes net patient revenue, contractual allowances, bad debt, charity care and value-based contract accruals. For payers, complexity arises in areas such as premium revenue recognition, medical cost accruals incurred but not reported (IBNR), risk adjustment estimation, and reconciliation of claims and encounter data. Stewardship responsibilities extend to the proper management of funds subject to regulatory or contractual restrictions. For providers, this includes grants, restricted donations, research funding, and community benefit reporting tied to IRS 501(r) obligations. For payers, this includes premium dollars, reserve adequacy, delegated entity payments, and compliance with medical loss ratio (MLR) requirements and state insurance regulations. Auditing this domain enables internal audit to validate the reliability and integrity of financial information, assess the reasonableness of key assumptions and estimates, strengthen financial governance and oversight, and ensure that resources are deployed in support of organizational strategy, mission and regulatory compliance.

Privacy

Healthcare organizations are managing rapidly expanding volumes of complex data, creating opportunities to enhance care delivery and the member experience while increasing the importance of strong data protection and governance practices. At the same time, evolving threats such as inappropriate access, cyber incidents and vendor-related vulnerabilities require enhanced monitoring, access controls and response capabilities. Organizations are placing greater emphasis on privacy risk management in response to heightened regulatory expectations, increased enforcement and a dynamic regulatory landscape, including growing scrutiny around interoperability and data sharing practices. This includes a focused effort to comply with evolving state requirements and the HIPAA Privacy Rule and Breach Notification Rule, particularly with respect to appropriate access, use and disclosure of protected health information and mitigation of risks related to data minimization and retention failures.

Oversight of user access, including role-based controls and monitoring for unauthorized activity, remains critical, along with strengthened third-party risk management and business associate oversight. As adoption of AI, automation and advanced analytics accelerates, organizations must continuously track the evolving privacy landscape, enhance data governance, and maintain effective incident response processes to support resilience, regulatory alignment and patient trust.

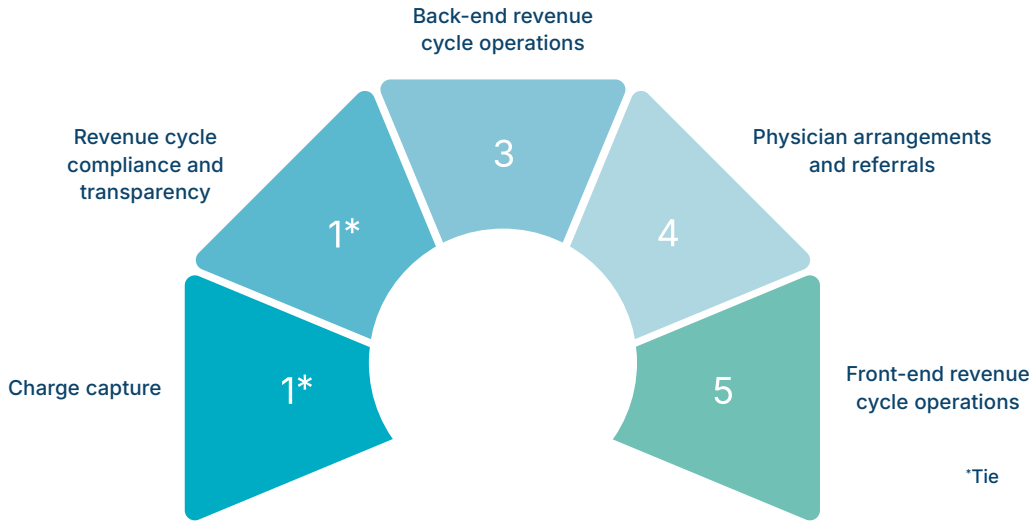
Data governance and enterprise reporting

Healthcare organizations operate across fragmented data ecosystems, where structured systems (e.g., EHRs, billing systems, claims systems and clinical registries) intersect with large volumes of unstructured data that rarely reconcile cleanly. For internal audit, data governance and enterprise reporting risks must be in the plan to address key risk areas. From a provider perspective, patient safety and care quality depend on accurate, complete data flowing to clinical dashboards and quality measures; poor governance can mask gaps that harm patients. From a payer perspective, accurate and tightly governed data is essential to support claims adjudication, encounter submissions, risk adjustment, quality reporting and regulatory filings, where incomplete or inconsistent data can directly impact provider reimbursement, compliance and member experience.

Regulatory exposure is severe. CMS quality reporting, HIPAA, and value-based contracts tie revenue and penalties directly to reported data, while errors may drive fines and clawbacks. Reporting integrity suffers when reporting outputs do not have solid metadata/explainability, leading to misunderstanding and rework. AI and analytics adoption is accelerating, and ungoverned data magnifies bias, misuse and errors. Each of these risks has driven greater investments in data governance within healthcare, which also should be reviewed to ensure proper implementation and return on investment.

Provider Priorities

Top Priorities



Healthcare providers are navigating rapidly evolving care delivery environments while balancing workforce, operational and financial demands. Strengthening governance, enhancing operational effectiveness and providing assurance over key clinical and business processes support the organization.

01* Charge capture

Effective charge capture processes enable healthcare providers to maximize revenue and ensure compliant billing. As operating margins tighten and billing accuracy oversight intensifies, gaps or delays in capturing charges can threaten the organization's financial integrity, as even minor process weaknesses can cause material revenue leakage. Heightened regulatory scrutiny pressures health systems to demonstrate all services provided are accurately and promptly recorded. Incomplete or late charge capture can lead to revenue loss and compliance issues. EHR optimization, AI and automation are streamlining workflows but require robust controls and validation. For these reasons, internal audit functions are prioritizing charge capture audits to safeguard revenue, maintain billing accuracy and ensure billable services are captured and reconciled timely.

Key audit areas to consider include:

- **Charge completeness/reconciliation:** Assess if all patients, services, supplies, implants and pharmaceutical items are captured and reconciled between clinical, supply chain, pharmacy and billing systems.
- **Charge timeliness:** Evaluate whether charges are entered within defined time frames from date of service to support billing and reimbursement cycles.
- **Documentation and coding alignment:** Review whether clinical documentation supports billed charges, medical necessity and coding to reduce rework and denials.
- **Automation and system integration:** Assess effectiveness of automated charge capture tools, system interfaces, and work queues between EHRs, coding and billing.
- **Governance and accountability:** Evaluate oversight structures and role clarity across departments involved in charge capture.
- **Variation and root cause analysis:** Identify variation across service lines, facilities, clinician groups, etc., and analyze drivers of missed or inaccurate charges.

* Tie

01* Revenue cycle compliance and transparency

Revenue cycle compliance and transparency remain a top priority as regulatory expectations continue to expand and directly impact financial performance and operational execution. Two key regulations, the Hospital Price Transparency Rule and the No Surprises Act, along with related state-level transparency and patient-protection requirements that may vary by jurisdiction, are driving increased scrutiny over how organizations disclose pricing information, develop patient estimates and manage billing practices. At the same time, health systems are under pressure to improve revenue realization and reduce administrative burden. Internal audit is playing an expanded role in helping organizations align these regulatory requirements with operational processes and financial outcomes by identifying gaps that impact both compliance and reimbursement. Effective oversight in this area not only reduces regulatory risk but also improves the accuracy, consistency and efficiency of pricing, estimation and billing activities across the revenue cycle.

Key audit areas to consider include:

- **Hospital Price Transparency (HPT):** Assess compliance with CMS and applicable state transparency regulations, including completeness and accessibility of machine-readable files and consumer "shoppable services" disclosures, as well as alignment of pricing data across systems, including recent updated regulations enforceable as of April 1, 2026.
- **No Surprises Act (NSA):** Assess compliance with federal and state surprise billing laws, including timely Good Faith Estimates, controls to prevent prohibited balance billing, and processes for patient consent and dispute resolution.
- **Regulatory monitoring and training:** Evaluate processes to monitor and operationalize federal and state regulatory changes, including HPT and the NSA, and ensure timely policy updates and role-based training across scheduling, registration and billing functions.

Effective oversight in revenue cycle compliance and transparency not only reduces regulatory risk, but also improves the accuracy, consistency and efficiency of pricing, estimation and billing activities across the revenue cycle.

* Tie

03 Back-end revenue cycle operations

Back-end revenue cycle (i.e., billing, accounts receivable (AR) management and denial management) functions are critical for financial stability and remain a focal point due to intensifying industry pressures. Health systems are contending with elevated denial rates and increased payer scrutiny, with rising denial volumes and audit activity underscoring the risk of revenue leakage if processes are not well controlled. At the same time, organizations are deploying automation, predictive analytics and AI-enabled tools to improve collections; these require effective oversight to ensure they operate as intended and do not introduce new risks. Internal audit is increasingly prioritizing this area, expanding beyond traditional audits through continuous monitoring programs that leverage KPIs to shift denials management from a reactive process to a proactive, data-driven prevention model.

By leveraging revenue cycle data, SQL-driven analytics and interactive Power BI dashboards, internal audit can expand beyond native EHR reporting to independently validate performance metrics, uncover insights not readily visible through standard reports, and provide a comprehensive view of denial trends and financial impact. Output of these efforts can be further validated through investigation of patient accounts to identify opportunities for targeted remediation based on process or control gaps. This shift positions internal audit to move beyond traditional assurance by enabling the timely identification of emerging issues and reimbursement trends. Through independent root cause analysis, governance oversight and data-driven insights, internal audit can help drive remediation efforts that enhance revenue integrity and improve cash realization.

Key audit areas to consider include:

- **Billing process integrity:** Evaluate claim accuracy, completeness, compliance and effectiveness of edits prior to submission, while also looking at clean claim rates, first-pass resolution rates and rejection handling.
- **AR performance and KPI monitoring:** Assess collections performance using key metrics (e.g., days in AR, aging), verifying work queue prioritization logic and effectiveness of follow-up strategies.
- **Denial management and root cause identification:** Evaluate identification, tracking, categorization and analysis of denials to drive corrective action and feedback communication, and to help prevent future denials.
- **Denial resolution and recovery:** Using advanced analytics, assess timeliness of follow-up; escalation of high-risk denials, appeals and litigation processes; and underpayment recovery.
- **Technology, automation and AI governance:** Review oversight of tools to ensure effectiveness and reduction of manual effort without added risk, while keeping pace with emerging technologies.
- **Continuous monitoring and insights:** Assess use of KPI-driven monitoring to identify trends, including overpayments and credit balance refunds, and support timely decision-making.

04 Physician arrangements and referrals

Financial relationships with physicians remain a priority for providers due to heightened regulatory scrutiny and complex compensation and referral structures. Federal enforcement agencies, including the OIG and the CMS, continue to focus on arrangements that may create improper financial incentives, particularly where compensation is not supported, exceeds fair market value (FMV), is not commercially reasonable, or lacks clear alignment with services rendered. Gaps are frequently identified in documentation, monitoring and governance practices, including unsupported payments, inaccurate or incomplete data sources, reliance on self-attestation processes, undocumented/outdated policies/procedures, and unclear or undefined ownership of responsibilities. The growing prevalence of layered compensation (e.g., clinical pay, call coverage, research, incentives, administrative) further complicates and heightens compliance and operational risk.

Key audit areas to consider include:

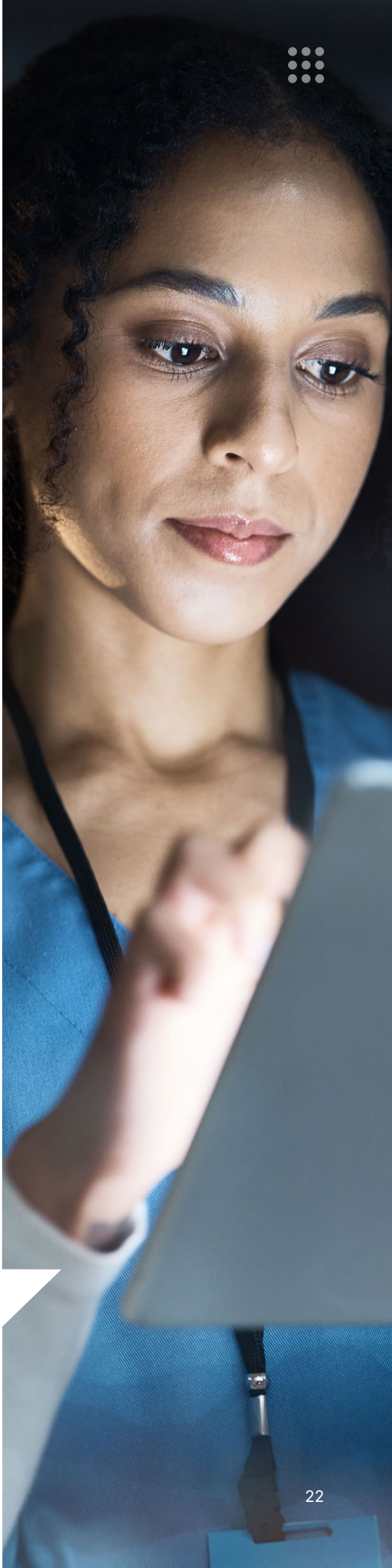
- **Physician contracting lifecycle:** Validate contract existence, execution, scope of services, appropriate approvals, required clauses and alignment of payments with contractual terms. Additionally, perform analytics to compare payment data to the contract management system to help identify payments without a contract or related to terminated contracts.
- **FMV and commercial reasonableness:** Assess completeness, timeliness and documentation supporting FMV and commercial reasonableness evaluations.
- **Payment accuracy and documentation:** Test high-risk compensation samples, identified through advanced analytics of payment and contracting data, for alignment with agreements, including retention of raw data, calculation support, eligibility evidence and documented review. Additionally, assess monitoring to ensure all payments do not exceed contractual or FMV maximums.
- **Stacked and overlapping compensation monitoring:** Assess physician cumulative payments and time allocation through advanced analytics (as data is available) across a physician's arrangement, including responsibilities and applicable departments (e.g., clinical, administrative, research), to identify risks of overlapping services (i.e., dates and times), exceeding maximums, payments outside of approved arrangements and/or duplicate payments.
- **Incentive compensation plan governance:** Evaluate methodology for clarity, support availability, appropriate approval of compensation plan changes and accuracy of metric and payment calculations.
- **Physician-owned distributorships (POD) governance:** Evaluate processes surrounding ownership disclosure, classification, approval workflows, clarity of responsibilities, escalation protocols and oversight.
- **Referral risk and vendor analytics:** Analyze purchasing patterns to identify potential conflicts of interest with PODs and validate ownership disclosures using external data sources.
- **Data integrity and reconciliation:** Assess data flow and reconciliation controls across systems to ensure data completeness and accuracy that support physician compensation calculations.

05 Front-end revenue cycle operations

Front-end revenue cycle processes support downstream financial performance and revenue integrity. Inaccuracies or breakdowns in scheduling, registration, insurance verification and authorization processes drive denials, delays and rework. Many can be traced to front-end errors or omissions. Health systems are adopting online self-scheduling, electronic preregistration and automated insurance eligibility checks to enhance patient experience; these innovations require strong controls to ensure data accuracy and no bypassed steps. This includes leveraging performance metrics and denial trends to identify variations and inefficiencies while providing governance and insight needed to strengthen controls and align front-end execution with compliance requirements and financial outcomes. Strengthening front-end processes supports improved revenue realization, reduced cost-to-collect and a more consistent patient financial experience.

Key audit areas to consider include:

- **Performance monitoring and denial linkage:** Assess use of front-end metrics and analyze denial data to identify trends and drive process improvement.
- **Registration accuracy and data integrity:** Leveraging analytics, assess completeness and accuracy of patient demographic and insurance information captured during scheduling or at intake.
- **Eligibility and benefits verification:** Evaluate processes to confirm coverage status, payer requirements and coordination of benefits details (e.g., copay, deductible) prior to service.
- **Prior authorization management:** Review identification, initiation, expiration and renewals, and completion of authorization requirements to prevent downstream denials.
- **Digital front-door controls:** Assess integration and governance over scheduling, registration and self-service technologies.
- **Point-of-service collections:** Evaluate processes supporting price estimations, upfront collections and financial counseling.
- **Practice variation and process consistency:** Identify inconsistencies across locations or service lines impacting accuracy and efficiency.



Provider Additional Areas of Focus

Hospital and physician clinical coding, documentation and queries

In an environment of expanding AI adoption and persistent margin pressures, the integrity of clinical documentation and coding has become increasingly critical and serves as the foundation for regulatory compliance and financial stability in health systems. As AI-driven clinical documentation integrity (CDI) and coding tools proliferate, audit coverage must verify model accuracy, detect bias and uphold robust governance and compliance standards. Potential risks can come in the form of AI tools pushing leading queries or prompting providers to document conditions that are not fully supported by clinical indicators or deviate from the provider's judgment. Revenue cycle and compliance leaders should actively evaluate the outputs of AI tools, including the queries they prompt. Concurrently, rigorous review of coding accuracy and billing processes remains crucial to support hospital financial performance and safeguard margins. This is especially true as enforcement agencies leverage advanced analytics to identify coding and billing outlier patterns and audit provider organizations and impose civil penalties.

Provider organizations should leverage the same types of analytics to identify potential coding and billing risks and more proactively resolve them before they receive a letter

The integrity of clinical documentation and coding has become increasingly critical, particularly in an environment of expanding AI adoption and persistent margin pressures.

from enforcement agencies. Complete and precise documentation and coding uphold reimbursement integrity, reduce denial risk, and limit regulatory exposure from payers and/or governmental audits. By addressing both AI oversight and traditional coding risks, internal audit can strengthen documentation integrity and compliance and help protect revenue margins.

Pharmacy operations and drug distribution/management

Pharmacy processes encompass significant patient safety, regulatory and financial risks, making noncompliance costly both in fines and reputational harm. Healthcare organizations are challenged with maintaining strict controls over procurement, storage, compounding, dispensing, wasting and administration of medications, particularly controlled substances, all while ensuring compliance with Drug Enforcement Administration (DEA) regulations, state boards of pharmacy, Drug Supply Chain Security Act (DSCSA) requirements and accreditation standards. Increased scrutiny around medication errors, drug diversion (especially controlled substances and other high-cost drugs), and compliance with the ever-changing 340B Drug Pricing Program further elevates risk exposure. Enhancing data integrity between pharmacy inventory systems and billing can help mitigate revenue leakage and compliance risk while supporting safe and efficient medication distribution practices.

Medical management

Health systems continue to face pressure to improve patient throughput, optimize capacity and manage cost of care, elevating the importance of medical and utilization management practices. Decisions related to medical necessity, level of care, length of stay, and observation versus inpatient status drive variation in utilization, denial risk and overall financial performance. In response, internal audit functions are expanding into operational audits focused on clinical performance, evaluating how effectively organizations manage patient flow, discharge and care coordination, and clinical denial and appeal effectiveness. Internal audit supports the enterprise by identifying variation, assessing alignment to payer and regulatory requirements, and highlighting opportunities to improve utilization, reduce delays, and enhance efficiency and financial outcomes.

Chargemaster

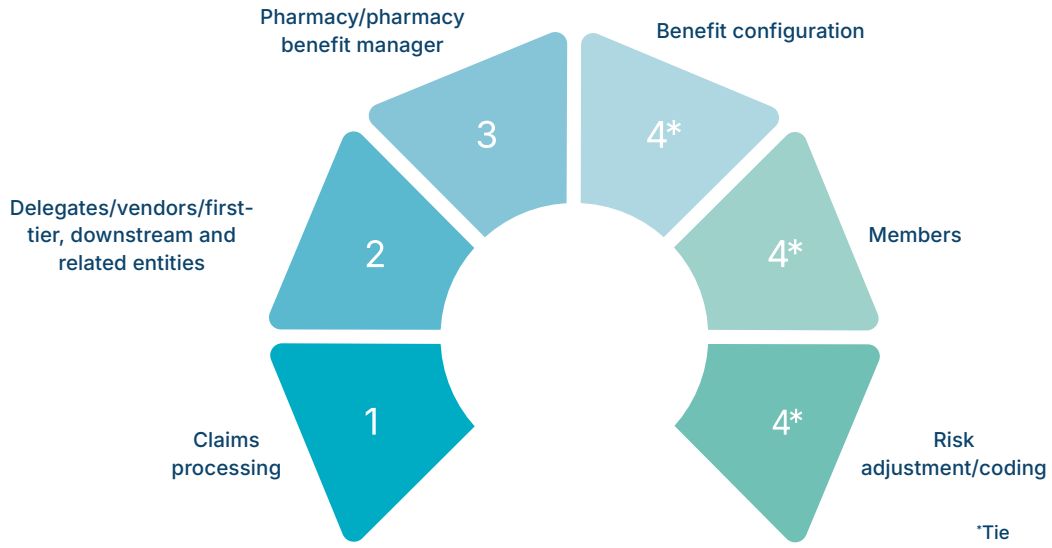
Maintaining an accurate, well-governed chargemaster remains critical due to its role in revenue integrity and financial performance. The chargemaster defines how items, services and procedures are identified across the organization and drives downstream documentation, coding, charge capture, and clean claim submission. Misalignment can create systemic issues affecting billing accuracy, reimbursement and price transparency efforts. These risks are amplified by the need to align with payer requirements, contractual obligations and federal and state regulations. The integrity of the chargemaster depends on effective coordination across clinical, coding, revenue cycle and finance functions. Internal audit evaluates governance, controls and processes supporting data accuracy, consistency and maintenance to reduce variation, rework and compliance risk.

Licensure and accreditation

Licensure, accreditation, CMS Conditions of Participation (CoPs), and state or county surveys represent key requirements and standards that directly influence a provider's ability to operate, deliver patient care and sustain reimbursement, warranting focused attention from internal audit. Variability in requirements, evolving standards and heightened enforcement elevate the risk of noncompliance, which may result in Corrective Action Plans (CAPs), financial repercussions and/or loss of participation status. Internal audit should prioritize assessing governance structures, monitoring processes and enterprisewide regulatory readiness, including survey preparedness, documentation integrity and responsiveness to regulatory inquiries, to support compliance and timely remediation of identified issues. In partnership with Compliance and operational leadership, internal audit should evaluate the effectiveness of regulatory change management, issue escalation protocols and readiness planning efforts to reinforce organizational integrity, mitigate regulatory and operational risk, and safeguard revenue continuity.

Payer Priorities

Top Priorities



Healthcare payers are facing increasing regulatory scrutiny and heightened expectations for accuracy, transparency and member experience. Effective oversight helps manage compliance and operational risks while maintaining trust and supporting organizational objectives.

01 Claims processing

Claims processing remains one of the most critical areas for payers, given the direct impact on financial performance, regulatory compliance and stakeholder trust. Evolving adjudication logic, complex encounters submissions, and coordination of benefits requirements create risk of data inaccuracies and improper payments. These risks are further compounded when core operational functions are delegated to third-party administrators (TPAs) or other third parties, increasing the likelihood of control gaps and inconsistent operations. Regulatory scrutiny, particularly around encounter data accuracy and prompt pay requirements, continues to intensify downstream deliverables. Internal audit is well positioned to evaluate the effectiveness of end-to-end claims processing controls and assess that data is accurately, completely and timely maintained across systems, vendors and processes.

Key audit areas to consider include:

- **End-to-end claims lifecycle:** Assess the design and operating effectiveness of controls across the full continuum, from intake through adjudication, payment and EOB/EOP generation, with an emphasis on configuration, data dependencies, system integrations and process handoffs.
- **Encounters data governance and reporting:** Assess the accuracy, completeness and timeliness of encounter submissions using advanced analytics, including validation of controls, rejection handling, resubmission, and compliance with regulatory reporting requirements.
- **TPA oversight:** Evaluate the governance framework, contractual obligations and performance monitoring processes over delegated entities, with a focus on using data analytics to validate the integrity of claims administration activities, financial accuracy and adherence to SLAs and applicable regulatory requirements.
- **Payment integrity and claim quality:** Evaluate the design and operating effectiveness of pre- and post-payment control frameworks, including analytics-driven audit programs, variance identification and recovery processes, to detect and remediate improper payments while strengthening overall claim accuracy and financial performance.

Claims processing has a direct impact on financial performance, regulatory compliance and stakeholder trust, making it one of the most critical areas for payers.

02 Delegates/vendors/first-tier, downstream and related entities

Oversight of delegates and vendors is a high-risk area for payers, driven by scrutiny from regulators and accreditation bodies. Practices that many payers have historically relied on, such as annual attestations and checklist-driven monitoring, are increasingly viewed by regulators as indicators of insufficient oversight, as plans are being held accountable for the actions and deficiencies of their delegated entities. The delegate ecosystem is also expanding to include AI-enabled vendors and offshore operations as payers and providers increasingly utilize third-party partners to support cost-containment efforts. Internal audit plays a critical role in validating that the processes and controls around delegation oversight are designed effectively, operating as intended, and appropriately documented.

Key audit areas to consider include:

- **Delegation inventory tracking and governance:** Evaluate whether the delegate population is being comprehensively identified and tracked, including downstream entities and their subcontractors; appropriately risk stratified; and subject to oversight activities aligned with the level of assessed risk.
- **Pre-delegation due diligence:** Assess exclusion screening processes, solvency, System and Organization Controls (SOC) reports, and information security validation prior to go-live of new vendors.
- **Contractual flow-down:** Review whether required flow-down clauses, audit rights, training requirements, code-of-conduct acknowledgement, offshore restrictions, performance guarantees and data protection provisions are operationalized.
- **Ongoing performance and compliance monitoring:** Evaluate the effectiveness of delegation oversight committees and the monitoring of KPIs, SLAs and incentives.
- **Data privacy and cybersecurity:** Review controls over PHI and personally identifiable information (PII), data access protocols, HIPAA breach notification processes, as well as AI and model risk for vendor tools, including subcontractors used by delegates.
- **Issue management and termination readiness:** Assess CAP closure quality, repeat-finding trends, contingency planning effectiveness, and the ability to transition out or insource high-risk delegates, through the use of advanced analytics that enhance risk monitoring, trend analysis and decision-making.

03 Pharmacy/pharmacy benefit manager

Pharmacy benefit management is high-risk for payers given its impact on cost, member experience and regulatory compliance. With complex arrangements that often involve pricing guarantees, rebate structures and delegated responsibilities, financial transparency and accountability can be obscured. As drug costs rise, regulators increasingly scrutinize formulary decisions, coverage determinations and utilization management, particularly regarding member access. Lack of oversight can cause financial leakage, regulatory noncompliance and member abrasion. Given the reliance on Pharmacy Benefit Managers (PBMs) and benefit design complexity, internal audit should evaluate if PBM relationships are effectively governed, contractual obligations are enforced, and coverage decisions are consistently applied in accordance with regulatory expectations, including through the use of advanced analytics.

Key audit areas to consider include:

- **Payment accuracy and rebate validation:** Assess the accuracy and completeness of pharmacy claims payments, manufacturer rebates and reconciliation processes, including delinked compensation and pass-through requirements.
- **PBM oversight and contract compliance:** Assess governance over PBM relationships, including adherence to contractual terms, pricing guarantees, transparency and rebate arrangements. Ensure KPIs are documented and monitored.
- **Fraud, waste and abuse monitoring:** Evaluate controls and analytics used to identify inappropriate prescribing patterns, pharmacy billing anomalies and potential misuse of benefits.
- **Formulary management and governance:** Evaluate processes for formulary development, approval and ongoing maintenance, including alignment with clinical guidelines, prior authorization and utilization management criteria, and regulatory requirements.
- **Specialty pharmacy oversight:** Assess governance over specialty drug programs, including pricing, utilization controls and coordination with care management functions.

04* Benefit configuration

Benefit configuration represents a critical control point within payer operations, directly impacting claims accuracy, regulatory compliance and the member experience. Errors in translating approved benefit designs into core claims processing systems can result in inappropriate denials, payment inaccuracies and misapplication of member cost share across high volumes of claims, collectively driving financial leakage and member abrasion. This is an area well suited for advanced analytics to identify configuration anomalies and quantify downstream financial impact. In response, regulatory scrutiny surrounding utilization management continues to intensify, particularly with respect to prior authorization practices that influence access to care, requiring payers to substantiate that determinations are clinically appropriate, consistently applied and supported by robust documentation. As payer operations continue to evolve, the increasing use of AI embedded within prior authorization workflows further elevates risk by raising questions around governance, bias and transparency.

Key audit areas to consider include:

- **Benefit configuration accuracy:** Evaluate whether approved benefit designs are accurately translated into claim systems, including coverage parameters, exclusions, limitations, in- and out-of-network classification, and service eligibility criteria.
- **Cost share integrity:** Assess whether member financial responsibility, including copayments, coinsurance, deductibles and out-of-pocket maximums, is consistently calculated and applied in accordance with plan design and applicable regulatory requirements.
- **Prior authorization governance:** Evaluate the design and execution of prior authorization processes, including the application of medical necessity criteria, consistency of determinations, sufficiency of documentation, and oversight of AI-enabled decision-making, with focus on model governance, human review, and monitoring for potential bias or inappropriate denials.
- **Referral validation:** Review the accuracy and enforcement of referral requirements, including alignment to benefit design and evidence of appropriate validation during claims adjudication.

Practices that many payers have historically relied on, such as annual attestations and checklist-driven monitoring, are increasingly viewed by regulators as indicators of insufficient oversight, as plans are being held accountable for the actions and deficiencies of their delegated entities.

* Tie

04* Members

Member-related processes are foundational to payer operations, directly influencing revenue, regulatory compliance and member satisfaction. Consequently, inaccuracies in the eligibility and enrollment processes cascade downstream, potentially resulting in misstated financials, improper claim payments and associated administrative remediation efforts. In parallel, appeals and grievances processes sit at the cross section of quality, compliance and the member experience. Regulators continue to place emphasis on timeliness, transparency and fairness of determinations. These processes have a direct impact on quality performance measures (e.g., star ratings), which can materially impact the reimbursement and competitive positioning of the payer.

The complex operations and regulatory sensitivity of processes affecting members position internal audit to play a central role in evaluating the integrity of membership data. Internal audit can leverage advanced analytics as a core audit technique to identify trends and anomalies across the member lifecycle. In addition, internal audit can assess the organization's ability to identify and remediate systemic control deficiencies. Through data-driven procedures, it can also evaluate the timeliness, consistency and outcomes of appeals and grievance activities, enhancing root cause identification and risk stratification.

Key audit areas to consider include:

- **Enrollment and eligibility data quality:** Evaluate the completeness, accuracy and timeliness of enrollment transactions, including member eligibility status, effective dates, coverage requests misclassified or dismissed inappropriately, and alignment with source systems and regulatory requirements.
- **Membership data integrity:** Assess the reconciliation of membership data across administrative, financial, care management and regulatory reporting systems, including controls to identify and resolve discrepancies impacting Primary Care Provider (PCP) assignment and attribution, revenue, claims processing and more.
- **Member material accuracy:** Evaluate the accuracy, completeness and timeliness of materials sent to members.
- **Appeals and grievances trends:** Assess processes for monitoring appeals and grievance trends, identifying root causes and implementing corrective actions to address systemic issues and improve member experience.
- **Appeal decisions:** Review medical and prescription drug appeal determinations for appropriateness, including adherence to medical necessity criteria, timeliness requirements and evidence of appropriate clinical involvement in decision-making.
- **Grievances classification:** Evaluate whether complaints are accurately classified, investigated and resolved within required time frames, with responses that meet regulatory standards for clarity and completeness.

* Tie

04* Risk adjustment/coding

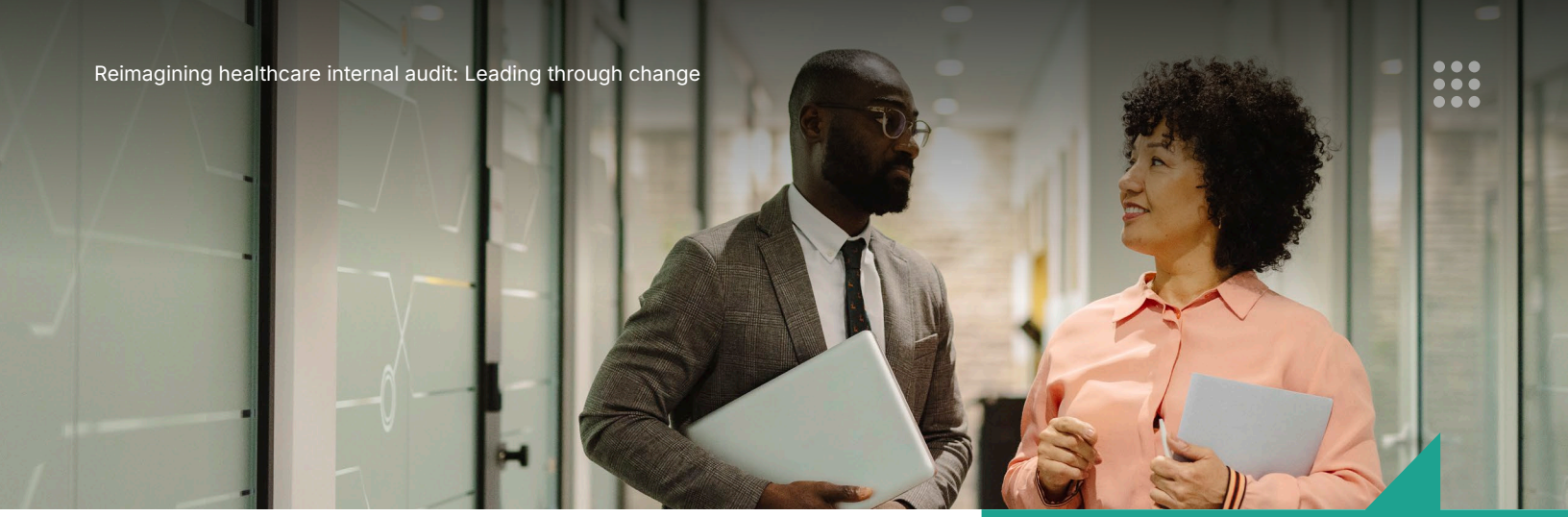
Risk adjustment remains a critical focus for payers due to its direct impact on regulatory compliance, financial integrity and reputational risk. Under Medicare Advantage (MA) and Affordable Care Act (ACA) programs, risk-adjusted payments are designed to align reimbursement with member acuity and resource utilization, supporting appropriate funding for clinically complex populations. While this model promotes equitable care delivery, it introduces compliance and financial risk when diagnoses are unsupported or inaccurately reported.

Regulators continue enforcement actions related to unsupported diagnoses, one-way chart reviews, and failure to correct known errors. CMS has also expanded Risk Adjustment Data Validation (RADV) audits, creating significant financial and regulatory exposure for MA payers. Additionally, the rapid adoption of AI-enabled tools may introduce risks related to documentation misinterpretation, coding inaccuracies and bias. Without effective governance and human oversight, these tools may heighten, rather than mitigate, compliance risk.

Key audit areas to consider include:

- **Governance and end-to-end controls:** Evaluate the completeness of the risk adjustment control framework, including accountability across compliance, risk adjustment and coding teams. Assess controls over diagnosis capture, validation, submission and deletion, including adherence to CMS overpayment requirements.
- **Accuracy and documentation support:** Test submitted diagnoses against medical records, using AI and advanced analytics to identify high-risk conditions; diagnoses originating from Health Risk Assessments, chart reviews and in-home assessments lacking additional support; and one-time conditions without ongoing management.
- **Two-way chart reviews:** Assess whether retrospective reviews identify both missed and unsupported diagnoses, and whether correction processes are timely and effective.
- **Technology and incentive oversight:** Evaluate AI governance, including validation, human review, and monitoring for bias, as well as alignment of incentives with accuracy and compliance.
- **Audit readiness and remediation:** Assess preparedness for RADV and OIG audits, including documentation retrieval, issue tracking and timely identification, investigation and repayment of overpayments.

* Tie



Payer Additional Areas of Focus

Coverage decisions/utilization management

Coverage decisions and utilization management continue to represent elevated risk areas for payers, driven by increasing regulatory, legal and reputational considerations and the expanding use of delegates. External pressure is intensifying from multiple fronts, including the CMS Interoperability and Prior Authorization Final Rule, expanding state-level prior authorization reform requirements, strengthened parity enforcement under the Mental Health Parity and Addiction Equity Act (MHPAEA), and ongoing class-action litigation related to algorithm-driven denial practices. Collectively, these developments have raised expectations for the transparency, timeliness and clinical supportability of coverage decisions. Internal audit should prioritize evaluating whether controls are designed and operating effectively to support the consistent application of medical necessity criteria, adherence to regulatory requirements, and parity between medical and behavioral health coverage. Additionally, internal audit should assess governance structures and validation practices for the use of AI and algorithmic tools, including oversight of model performance, appropriate human-in-the-loop processes and clinician involvement in decision-making.

The growing use of AI and algorithmic decision-making is raising the bar for oversight, requiring stronger governance, validation and clinician involvement.

Medical loss ratio

Medical loss ratio (MLR) has a direct impact on regulatory compliance, financial performance and the reputational risk of a payer. As a KPI, there is significant pressure across payers to reduce MLR, as it reflects the percentage of premium revenue spent on quality improvements and clinical services relative to administrative costs and is central to demonstrating compliance with federal and state requirements. Inaccuracies in timing, classification, and the completeness of underlying data may result in regulatory scrutiny stemming from misstatements and inappropriate rebate obligations. Given that MLR calculations require complex aggregation of data from actuarial, claims and finance functions, the risk of error is inherently elevated. The judgmental categorization of expenses further elevates the risk profile. Internal audit should provide assurance over the integrity of MLR calculations, challenge underlying methodologies and assumptions, expense classifications and eligibility, and identify control gaps that may expose the organization to financial misstatement, regulatory noncompliance and reputational risk.

Increasing regulatory scrutiny is placing greater emphasis on the accuracy, transparency and governance of actuarial models and commission practices.

Financial/Actuarial

Placing a heavy reliance on complex data sets, assumptions and methodologies, the areas of sales commissions, actuarial modeling and IBNR estimates are inherently subject to risk of misstatements and regulatory exposure. Complex contractual terms coupled with evolving regulatory requirements highlight the increasing scrutiny on sales commissions, notably within government programs. Additionally, actuarial models and IBNR estimates require the application of significant judgment; when assumptions or underlying data are flawed, the impact on financial reporting and reserve adequacy can be material. In this environment, internal audit should independently validate key financial assumptions, assess the completeness and accuracy of underlying data, and evaluate the effectiveness of controls around agent and broker sales commissions to limit financial misstatement and regulatory exposure.

Provider network operations

Provider-centric processes influence quality of care, regulatory compliance, member access and cost containment. As value-based care models expand, the complexity of provider contracting and associated reimbursement methodologies increases, heightening the risk of misalignment between contractual terms and operational execution. Regulators are intensifying scrutiny over provider directory accuracy and credentialing practices, where deficiencies can cause compliance violations, member abrasion and reputational harm. Ineffective network management and contract configuration errors drive payment inaccuracies and can erode provider relationships. Given the interdependencies across provider data, claims adjudication and member experience, and the reliance on robust internal controls and high-quality data, internal audit is well positioned to provide assurance over control effectiveness, validate alignment across systems and provider contract terms, and identify vulnerabilities that may expose the organization to financial, regulatory and operational risk.

Behavioral health

Behavioral health faces heightened regulatory scrutiny, sustained member demand, and evolving care delivery models, making it a top risk area for payers. Enforcement under the MHPAEA Final Rule, comparative analysis requirements for nonquantitative treatment limitations, and continued focus on network adequacy, restrictive prior authorizations and “ghost networks” have meaningfully raised compliance expectations. Member demand for telehealth-based behavioral care has surged with virtual therapy and digital platforms now serving as primary access channels, creating new risks around licensure, fraud and quality of care. Providers are accelerating their use of AI for clinical intake, symptom screening, virtual therapy, crisis triage and treatment planning, introducing concerns around accuracy, bias, privacy and member safety. Internal audit should evaluate processes and controls around parity compliance, access and timeliness of services, oversight of delegated vendors, claims and authorization integrity, and the governance of AI-enabled tools.

In Closing

“

As healthcare organizations adapt to a rapidly changing risk environment, internal audit must continue to evolve alongside them. This year’s results highlight both the accelerating pace of change and the expanding expectations placed on internal audit leaders. With 65% of respondents identifying technology-enabled change adoption as a significant organizational risk and 63% reporting that they are already performing AI governance engagements, the profession is increasingly being called upon to provide assurance over emerging technologies while helping organizations balance innovation with accountability. This perspective is consistent with Protiviti’s The Next Phase: AI and Human Collaboration Powering Internal Audit Transformation, which frames AI enablement as an increasingly important part of internal audit’s next evolutionary phase and emphasizes that technology must be paired with the right experience, skills, innovation orientation and human judgment[4]. AI is both a subject for assurance and a capability healthcare internal audit functions are expected to use responsibly.

The most effective internal audit functions will move beyond traditional assurance by leveraging data, analytics and advanced technologies to deliver timely, risk-focused insights that anticipate challenges before they emerge. As healthcare organizations navigate evolving risks, regulatory expectations and strategic priorities, internal audit has a unique opportunity to strengthen its role as a trusted advisor while helping leadership build resilience, enable transformation and make informed decisions with confidence.

Matt Jackson
Managing Director
Healthcare Internal Audit Practice Leader
Protiviti

[4] Protiviti, “*The Next Phase: AI and Human Collaboration Powering Internal Audit Transformation*,” July 2025.

Appendix A — Innovation in healthcare internal audit

AI, automation and advanced analytics

Technology is changing what healthcare internal auditors can cover, how quickly they can respond and the value they can deliver. AI, analytics, automation and continuous monitoring are reducing manual effort, expanding coverage and catching issues earlier, freeing more time for auditors to focus on analysis, judgment and stakeholder engagement.

AI and analytics use in internal audit is now widespread. Protiviti and AHIA's 2026 survey found 94% of respondents currently use AI, most commonly for interview note summarization (59%), business and risk research (55%), workpaper and report drafting (47%) and data analysis (45%). Analytics are most often applied to dynamic risk assessment and engagement planning (53%), exception identification and review (49%), and dashboards or visual reporting (45%). Microsoft Copilot (80%), Excel-based analytics (57%) and Power BI (55%) were the most commonly used tools, while 57% reported using a dedicated governance, risk and compliance (GRC) platform and 45% reported using additional automation or process intelligence tools. Adoption of AI and analytics remains uneven though, and most teams are still working through how to apply these tools in a repeatable way.

For AI specifically, Protiviti's AI Pulse Survey found only 1 in 10 organizations has embedded it in repeatable workflows alongside analytics, automation and monitoring.[5] A few recurring obstacles help explain why more teams have not reached that point. The most commonly reported hurdles were time constraints and competing priorities (39%), staff skill gaps or limited AI experience (37%), data privacy or confidentiality concerns (33%), and reliability or auditability of AI outputs (31%). What often separates the teams that get past these hurdles is the quality of their data. In Protiviti's AI Pulse Survey, 97% of organizations whose AI returns significantly exceeded expectations were confident in their data, while limited or unreliable data narrows analysis and makes it harder to identify patterns or understand the full extent of risk.[6]

[5] Protiviti, *AI in Internal Audit: Turning Momentum into Impact, From Pilot to Practice Webinar,* May 2026.

[6] Protiviti, *From Data Confusion to AI Confidence: Data Is the Foundation of Trustworthy AI,* AI Pulse Survey, Vol. 2, 2025.

These concerns are not unique to internal audit. Leadership is wrestling with the same issues at the enterprise level, and AI is climbing the list of healthcare executives' top concerns. Risk tied to adopting new and emerging technologies (including AI) and the need to upskill the workforce rose from the ninth to the fifth highest rated near-term risk between Protiviti's 2025 and 2026 Executive Perspectives on Healthcare Top Risks surveys. Concerns are especially tied to:

- Managing the risks tied to the data required for AI use and the heightened cybersecurity exposure that comes with it
- Integrating AI with existing technologies, business processes, and the workforce
- Equipping the workforce to realize AI's value proposition[7]

In addition to optimizing its own AI use, internal audit is also well positioned to provide assurance around AI use across the enterprise. The most common AI-related engagements reported in this survey were AI governance (63%), responsible AI principles or policy compliance reviews (37%), AI model risk or validation reviews (22%), AI vendor or third-party risk reviews (20%), and AI value realization reviews (14%).

Ambient listening tools, which transcribe patient-provider conversations to ease documentation burdens on providers, are one common and high-risk example that merits audit's attention. In an audit of a health system's AI rollout, internal audit found that diagnoses coded by providers were often not fully supported by documentation captured through ambient listening, resulting in high error rates and highlighting material compliance and billing risks that may have otherwise remained undetected. Additionally, autonomous coding codes most records in high volume areas like the Emergency Department, without a human coder reviewing. In one audit, internal audit identified issues with diagnoses and procedures being incorrectly coded on thousands of accounts due to the technology misinterpreting information in the medical record.

The teams getting the most from AI and analytics are the ones applying them consistently rather than occasionally. The capabilities below show where internal audit functions are focused.

[7] Protiviti and NC State University's ERM Initiative, *Executive Perspectives on Top Risks and Opportunities: Healthcare Industry*, 2026.

How leading internal audit functions are applying innovation

Capability	Use case example	Value driven
Dynamic risk assessment and engagement planning	Combine interviews, prior findings, regulatory developments, operational metrics and external information to refresh audit priorities, and draft risk and control matrices from limited inputs	Focuses resources on changing, higher-impact risks
Resource scheduling and staffing	Match auditor skills and availability to the audit schedule, suggest assignments and auto-adjust for timing shifts and turnover	Aligns the right people on audits and adapts staffing as schedules and teams change
Full-population analytics	Analyze complete populations, reconcile data across systems, identify outliers and quantify exposure	Expands coverage and supports conclusions in total dollars, days, denials or defects
Continuous monitoring and auditing	Automate recurring data feeds and monitor key risk indicators (KRIs), control thresholds and exception trends	Identifies emerging risks and control deterioration earlier
Walkthroughs and documentation	Record a single walkthrough and convert it into process narratives, flow charts, and standard operating procedures with steps and screenshots, without stopping the meeting to take notes	Speeds documentation while keeping the auditor in control of the final product
Intelligent testing workflows and automation	Use AI agents to automate control testing, evaluate samples and evidence across files and various file types, document exceptions, and generate first-draft audit reports	Extends capacity while maintaining review and escalation points
AI-enabled exception analysis	Group exceptions, identify patterns, summarize likely drivers and prioritize higher-risk items for review	Reduces manual review and focuses auditors on significance and root causes
Audit knowledge and benchmarking	Make prior plans, reports, work programs and benchmarks searchable across audits and facilities	Reduces duplicated effort and improves consistency

Where healthcare provider and payer internal audit teams are focusing

In addition to the more common uses noted above, healthcare provider and payer teams are applying AI and analytics to risks specific to their segments. The examples below reflect some successful use cases in each segment based on observed practices and survey responses.

Provider

Risk area	Where internal audit is applying AI and analytics
Revenue cycle and denials management	Full-population analysis of claims, remittance, write-offs and open receivables to identify leakage and recovery opportunities
Vendor and third-party spend	Continuous monitoring of payments for duplicate, off-contract or erroneous spend, with exceptions grouped and prioritized for review
Physician arrangements	Extract key terms from provider contracts and test payments against contract and fair market value thresholds to flag arrangements outside policy

Payer

Risk area	Where internal audit is applying AI and analytics
Claims payment integrity	Full or expanded population testing for overpayments, duplicate payments and authorization gaps
Provider contract management	Extract key contract language and compare terms across the full contract portfolio to flag outliers, noncompliance and negotiation or recovery opportunities
Premium billing and enrollment accuracy	Testing of member enrollment, eligibility and premium billing data to identify discrepancies, retroactive adjustments and revenue leakage

What this looks like in practice

Internal audit can use AI-enabled innovation to move beyond point-in-time testing and identify operational breakdowns that create measurable financial exposure. Across the industry, internal audit's use of AI and advanced analytics for full-population analysis and payer behavior analysis is resulting in millions of dollars from overturned denials and recaptured revenue. At a large, multi-state integrated delivery system, internal audit analyzed more than $100 billion in patient charges quarterly and performed root cause analysis on weaknesses revealed as part of a broader enterprise-wide

margin improvement initiative. The continuous monitoring resulted in significant financial returns and has surfaced control improvement opportunities across the revenue cycle that can be addressed more proactively, giving leadership a clearer view of where revenue is at risk. This work also strengthened internal audit's role as a strategic partner by establishing a foundation for ongoing monitoring, targeted recovery and transparency into how and when AI will be introduced by key vendors, including Epic, to further drive improvements in margin, quality and compliance.

This illustrates how internal audit can use AI and analytics to quantify risk, prioritize strategic attention and support sustained improvement while management retains responsibility for remediation. The same model, connecting risk assessment, analytics, monitoring and AI-enabled review, can be applied across other key enterprise risk areas, from procurement and payroll to physician arrangements, coding and beyond.

Internal audit innovation outside of healthcare

Across industries, leading internal audit functions are pushing past basic AI assistance into higher-value applications. Some key examples from Protiviti's work with internal audit teams in other industries include:

Industry	What internal audit teams are doing with AI	Value driven
Financial services	Reviewing large control libraries to remove duplicates and standardize the rest, so teams test a smaller, higher-quality set	Reviewed thousands of controls at once to cut redundancy and improve consistency
Private equity	Tracking the financial health of portfolio companies and flagging early signs of trouble, with AI explaining what is driving the risk	Turned a point-in-time review into ongoing, portfolio-wide monitoring with transparent, supportable calculations
Manufacturing and distribution	Checking products against complex export rules to spot items requiring a license or extra review	Screened ~10,000 products against multiple regulatory frameworks that previously required time-consuming manual review

Moving from individual use to a repeatable operating model

Organizations that scale AI strategically are three times more likely to exceed return on investment (ROI) expectations than those stuck in perpetual pilots.[8] Leading internal audit functions are embedding innovation across the lifecycle, especially early in planning, rather than relying on isolated use cases. Executive leadership perceives the greatest value when advanced analytics and AI are applied in

[8] Protiviti, *When AI Readiness Meets ROI Reckoning: Findings from Yearlong Research on AI Adoption, ROI and Optimization Issues,* February 2026.

engagement-level risk assessment and planning processes to direct additional audit activity, rather than when the quantified exposure becomes the issue itself. Practical steps include:

- Target procedures that are manual, data-intensive or repeated across engagements
- Use analytics and AI in planning and risk assessment to scope engagements and direct fieldwork toward root cause
- Select the right mix of AI, analytics, automation and monitoring for the audit objective
- Require human judgment at each key decision gate and establish clear expectations for output oversight
- Standardize successful approaches in work programs, templates and training
- Use reputable data sources and repeatable logic for recurring analysis
- Define thresholds, escalation criteria, review responsibilities and documentation expectations
- Measure value through coverage, time saved, earlier detection, quality and quantified outcomes
- Feed monitoring results into risk assessment and audit plan updates

As routine work shifts further to AI, teams should also be intentional about developing and strengthening the judgment, skepticism and stakeholder engagement skills that AI cannot replicate.

Balancing AI value and spend

As AI pricing shifts toward consumption-based models (e.g., usage-based pricing), where cost is tied to actual usage and processing volume rather than a flat license fee, internal audit functions need to understand what each use case costs and whether the value justifies the spend. Match the model and tool to the task, use lower-cost analytics or automation when AI does not add meaningful value, and compare spend to time saved, coverage expanded or losses avoided. CAEs should also understand where AI is used across the internal audit function, what it costs, who owns the spend, and whether the benefits support continued use.

The bottom line

Healthcare internal audit is at a turning point. The organizations pulling ahead are not the ones with the most tools, but the ones applying them consistently, on a foundation of reliable data and sound judgment. As AI moves from individual experiments to how the work actually gets done, the teams that treat it as a core capability will expand what they can cover, surface risks earlier and strengthen their standing as a strategic partner to the organization.

Appendix B – Benchmarking insights

Following are key takeaways from the data, followed by the full results categorized in these sections:

- Internal audit budgets and resourcing
- Internal audit's use of AI, analytics and other enabling technologies
- Internal audit structure and reporting
- Risk assessment practices
- Internal audit's collaboration with compliance and ERM

Key takeaways

Artificial intelligence and analytics:

1. AI is now widely used by internal audit, as only 6% of respondents reported not using AI tools today.
2. Internal Audit is primarily leveraging AI to support auditor efficiency and analysis, with the most common use cases including interview note summarization (59%), business and risk research (55%), workpaper and report drafting (47%), and data analysis (45%).
3. Time constraints and competing priorities (39%), staff skill gaps or limited AI experience (37%), data privacy or confidentiality concerns (33%), and reliability or auditability of AI outputs (31%) were the most commonly reported hurdles to using or scaling AI tools.
4. AI governance was the most commonly reported AI-related engagement area performed by internal audit (63%), followed by responsible AI or policy compliance reviews (37%), AI model risk or validation reviews (22%), AI vendor or third-party risk reviews (20%), and AI value realization reviews (14%).
5. Analytics are most commonly used to support dynamic risk assessment and engagement planning (53%), exception identification and review (49%), and dashboards or visual reporting (45%), indicating continued focus on using data to support auditor judgment and decision-making activities.
6. Microsoft Copilot (80%), Excel-based analytics (57%) and Power BI (55%) were the most commonly reported AI and analytics tools leveraged by internal audit. At the same time, 43% of respondents reported not using a dedicated governance, risk and compliance (GRC) platform, and 55% reported not using additional automation or process intelligence tools.

Organizational transformation pressures:

7. Technology-enabled change adoption (65%); workforce capacity, culture and change fatigue (63%); and leadership, governance and strategic alignment (51%) were the most frequently identified organizational-change risk areas, underscoring the significant transformation pressures facing healthcare organizations.

Internal audit and other risk management functions:

8. Outside of internal audit, the most commonly reported areas that audit committees have responsibility for and/or receive reports from include compliance (84%), external audit (76%), information security (63%) and ERM (63%). Compared to 2025, respondents reported increased audit committee involvement across each of these areas, including a 16% increase in ERM oversight.
9. Internal audit continues to support ERM activities through risk assessment, monitoring, reporting and assurance. However, among organizations without a formal ERM program, 57% cited a lack of board or executive sponsorship as a key barrier, while 43% identified budget, funding and resource constraints. These results suggest that successful ERM programs depend on strong leadership commitment and organizational investment, with internal audit most effective in an independent advisory and assurance role rather than as the owner of the ERM program.
10. Internal audit most commonly supports fraud risk management by incorporating fraud considerations into audit activities (43%) and assisting other departments' fraud management efforts (27%). Only 18% of respondents reported that internal audit leads the organization's fraud risk management program, reinforcing internal audit's role as an independent assurance and monitoring function rather than the primary owner of fraud risk management activities.
11. Interviews (84%), discussions with peers at other organizations (78%), published industry studies (76%) and input from outsourced or co-sourced partners (75%) were the most commonly reported inputs used to inform internal audit risk assessments, while less than half of respondents (49%) reported leveraging data feeds or analytics. Additionally, 70% of respondents perform their risk assessment annually, while 20% refresh their risk assessments two or more times per year.

Internal audit budgets and resourcing

Exhibit 1: Annual internal audit function's budget by organizational revenue

Survey Respondents %		14%	39%	23%	12%	4%	8%
Size (revenue in USD)		Less than $1 billion	$1 billion to less than $5 billion	$5 billion to less than $10 billion	$10 billion to less than $15 billion	$15 billion to less than $20 billion	$20 billion or more
Annual Internal Audit Budget (millions)	$3+	14%	10%	24%	33%	100%	75%
	$2.5–$2.999			9%	33%		25%
	$2–$2.499		5%		17%		
	$1.5–$1.999			9%			
	$1.25-$1.499						
	$1–$1.249		30%	24%			
	$.75–$0.999		15%	9%			
	$.5–$0.749		15%	16%	17%		
	$.25–$0.499	29%	25%				
	<$.25	57%		9%			

Exhibit 2: Internal audit function's annual hours by organizational revenue

Survey Respondents %		14%	39%	23%	12%	4%	8%
Size (revenue in USD)		Less than $1 billion	$1 billion to less than $5 billion	$5 billion to less than $10 billion	$10 billion to less than $15 billion	$15 billion to less than $20 billion	$20 billion or more
Annual Internal Audit Hours Budget	15,000+		10%	17%	49%	50%	75%
	10,000-14,999				17%		25%
	7,500-9,999						
	4,000-7,499		45%	42%	17%		
	2,000-3,999		20%	8%			
	1,000-1,999	71%	15%	8%	17%		
	<1,000	29%	10%	25%		50%	

Exhibit 3: Internal audit function's staff size by organizational revenue

Survey Respondents %		14%	39%	23%	12%	4%	8%
Size (revenue in USD)		Less than $1 billion	$1 billion to less than $5 billion	$5 billion to less than $10 billion	$10 billion to less than $15 billion	$15 billion to less than $20 billion	$20 billion or more
Internal Audit Staff Size	20+	14%	5%	17%		100%	75%
	15-19			8%	17%		
	10-14		15%	25%	49%		25%
	6-9			33%			
	3-5	29%	50%	17%	17%		
	1-2	43%	20%				
	0 or fully outsourced	14%	10%		17%		

Internal audit's use of AI, analytics and other enabling technologies

Exhibit 4: Internal audit's current use of AI tools

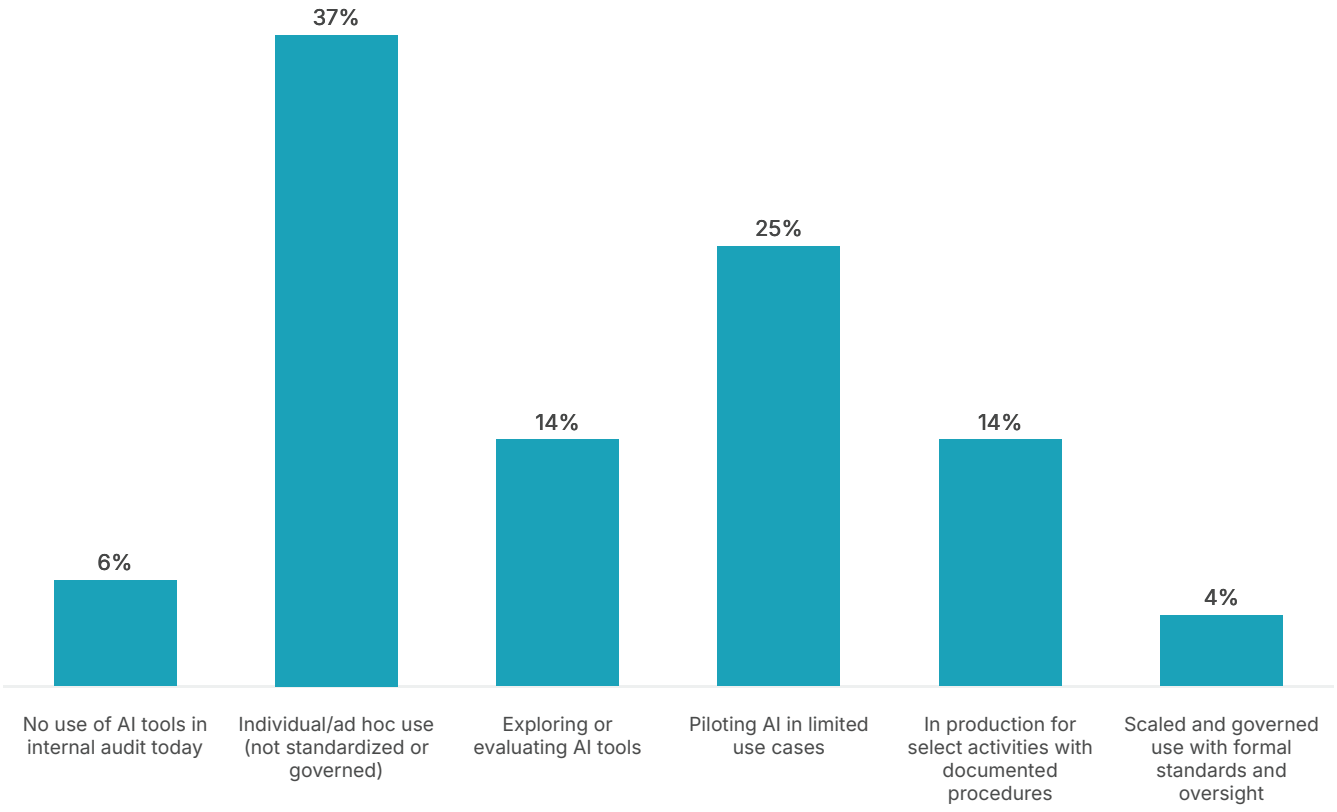


Exhibit 5: Areas in which internal audit is using AI (multiple responses permitted)

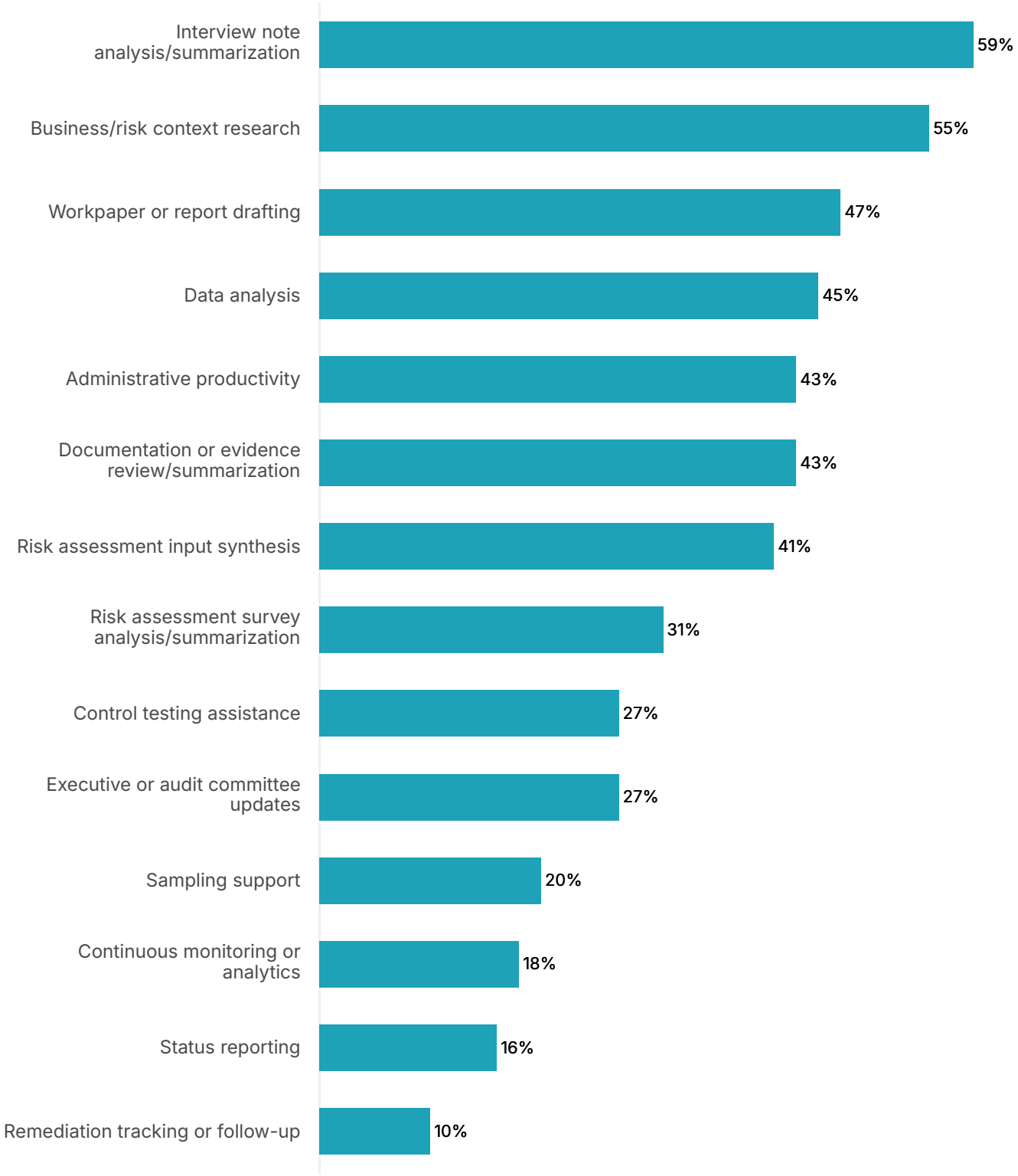


Exhibit 6: AI-related engagements internal audit has performed or plans to perform (multiple responses permitted)

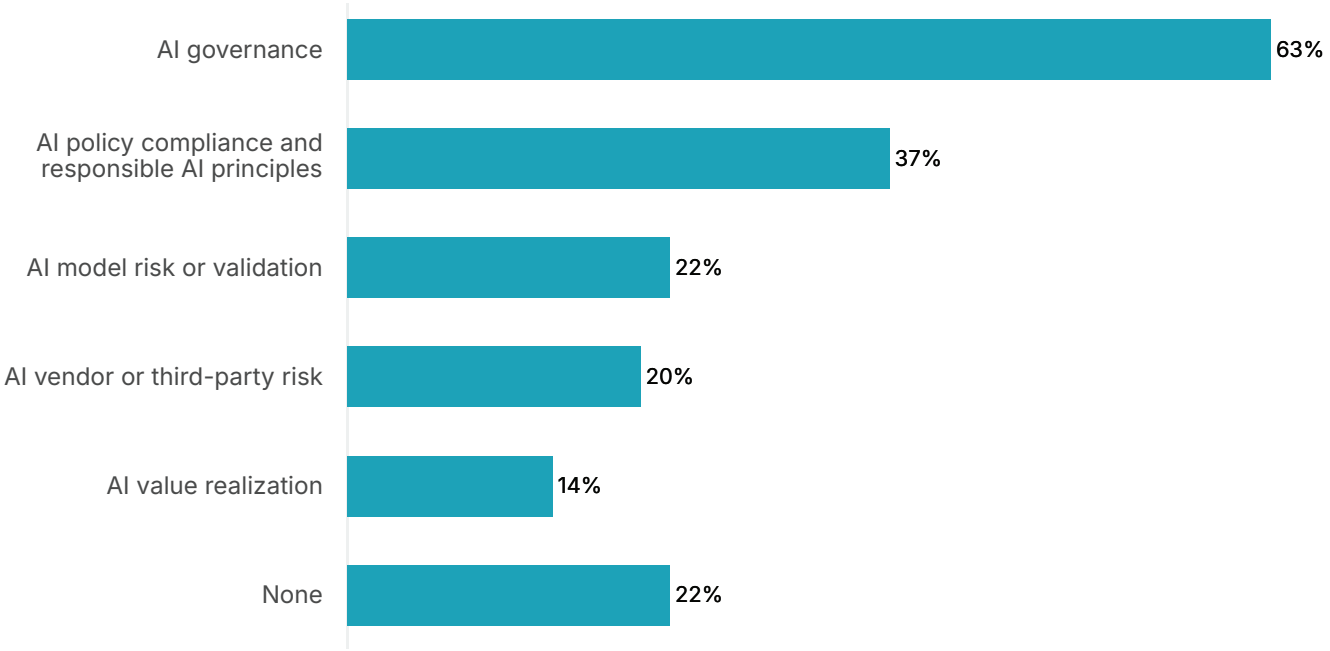


Exhibit 7: Primary hurdles internal audit faces in using/scaling AI tools (multiple responses permitted)

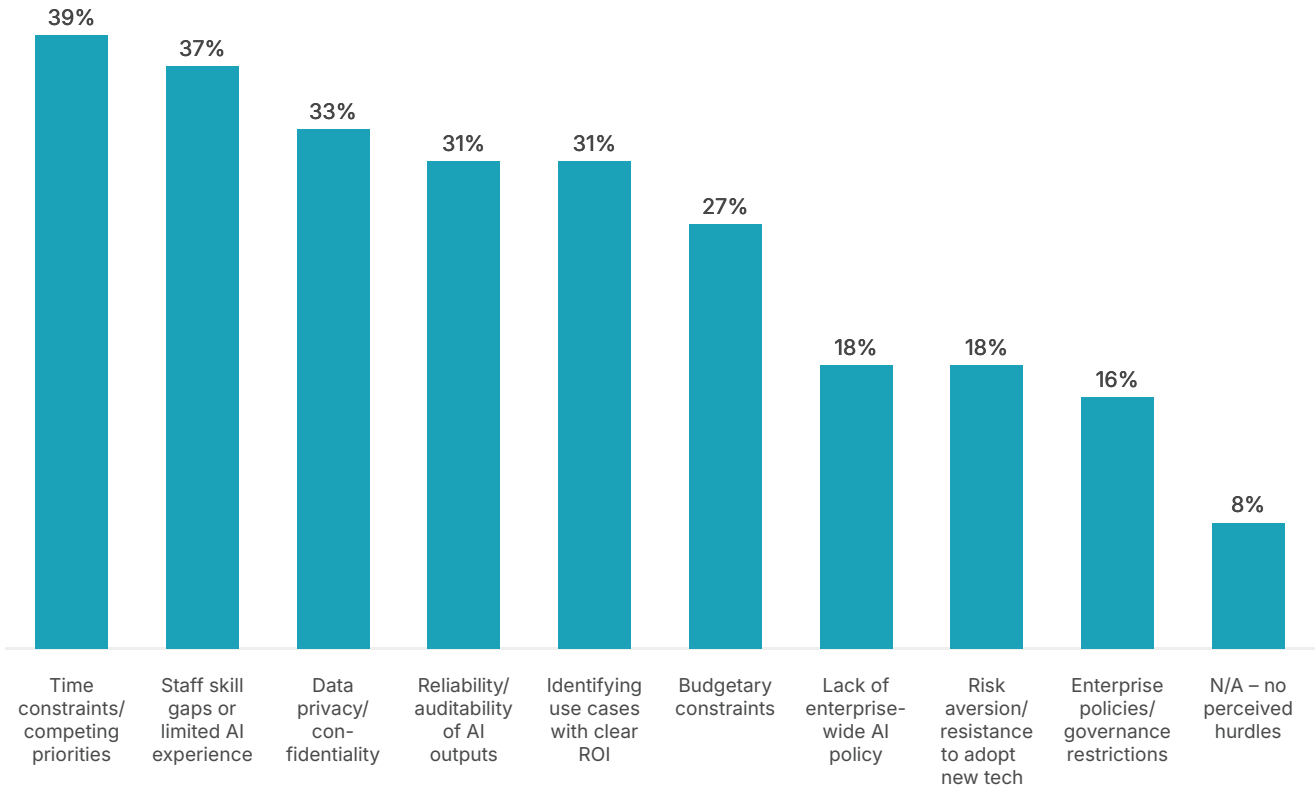


Exhibit 8: AI tools used by internal audit (multiple responses permitted)

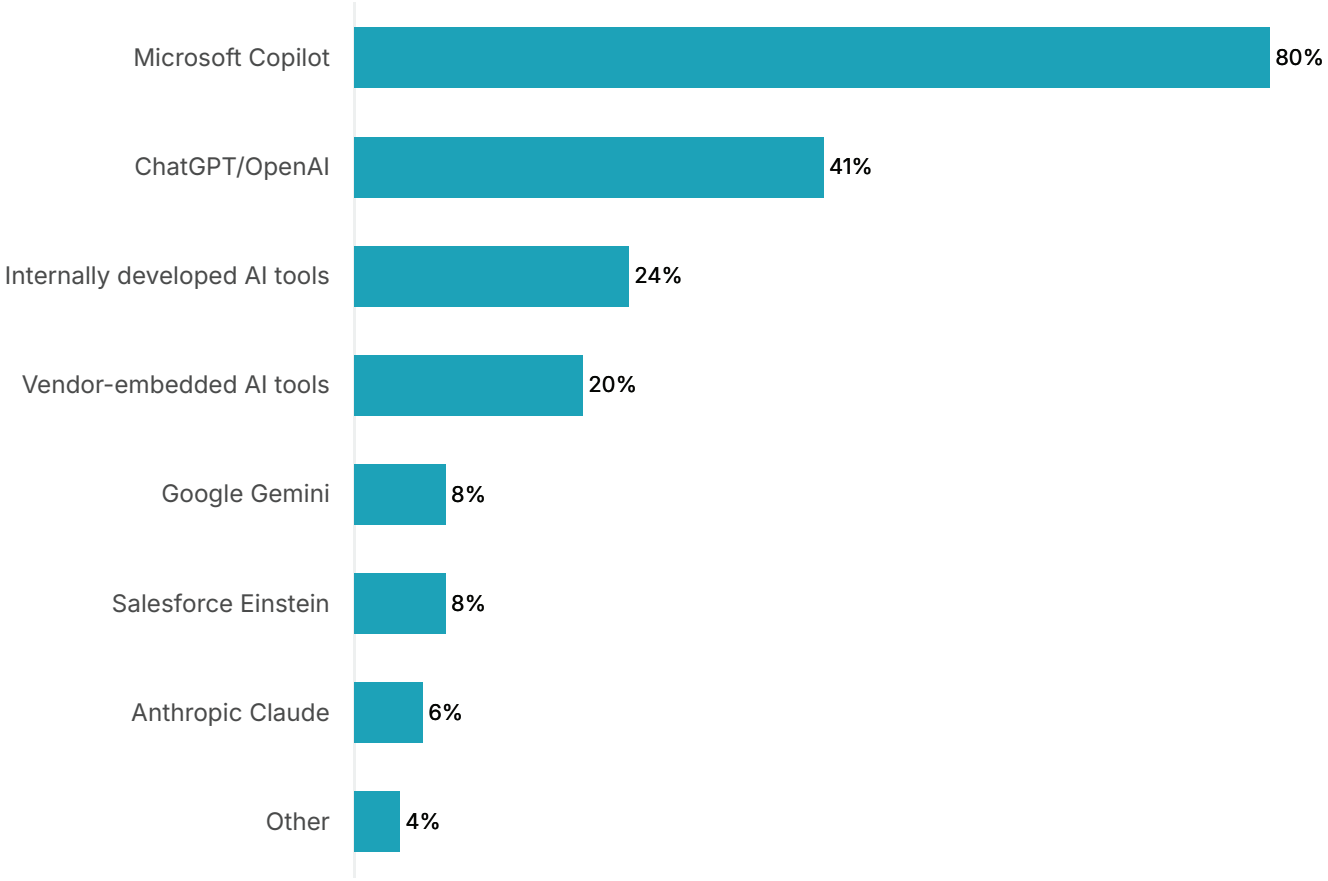


Exhibit 9: Internal audit coverage areas using analytics (multiple responses permitted)

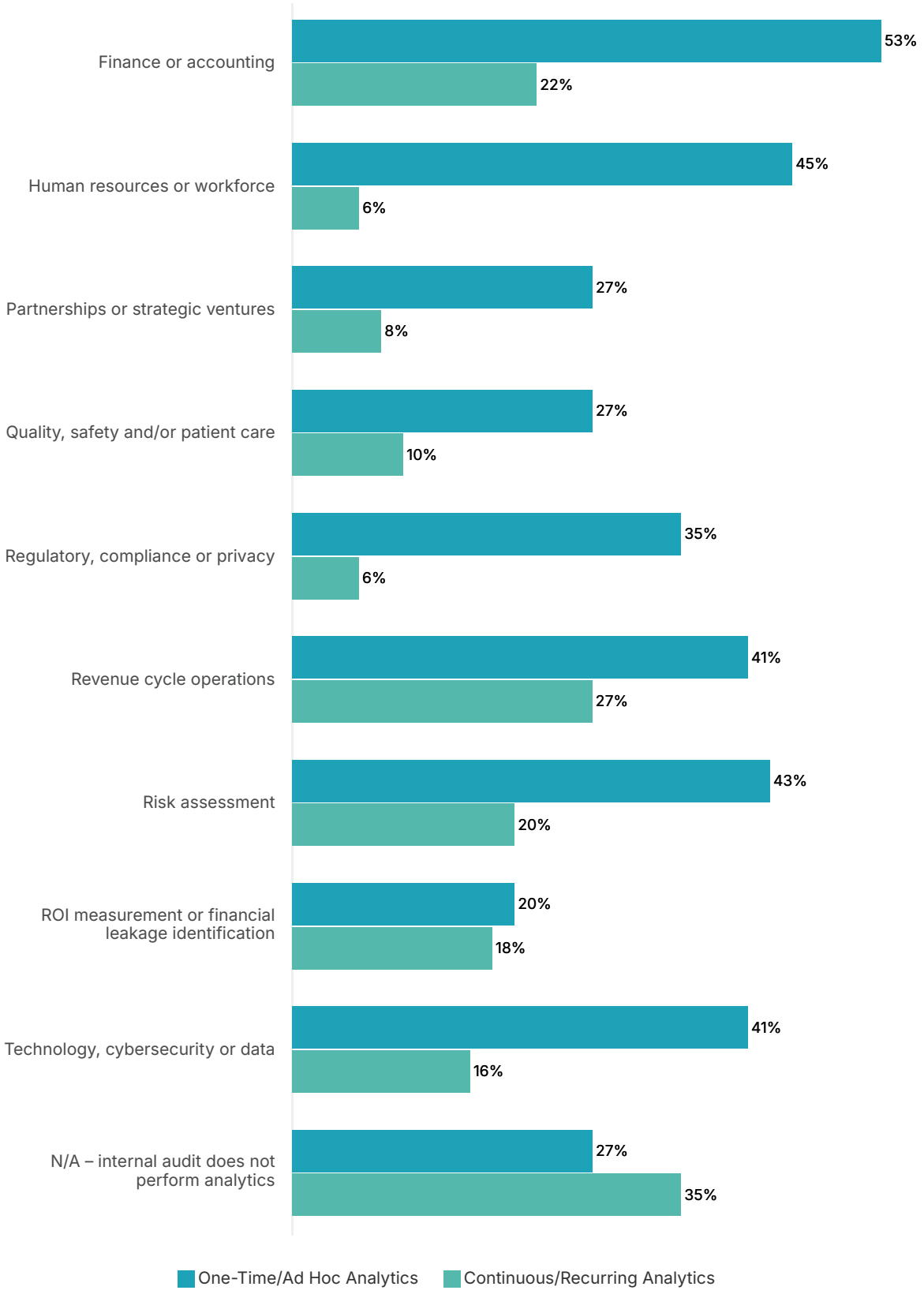


Exhibit 10: Frequency with which internal audit's continuous/recurring analytics are refreshed (multiple responses permitted)

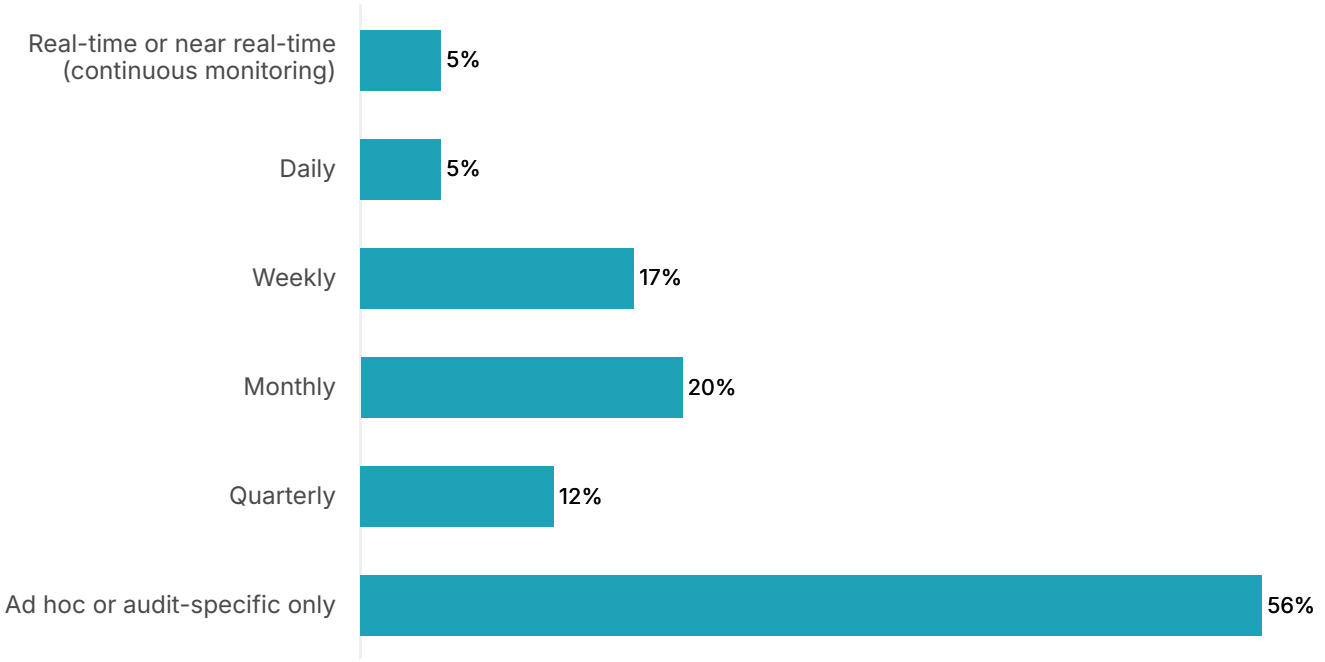


Exhibit 11: Primary outputs generated from internal audit analytics (multiple responses permitted)

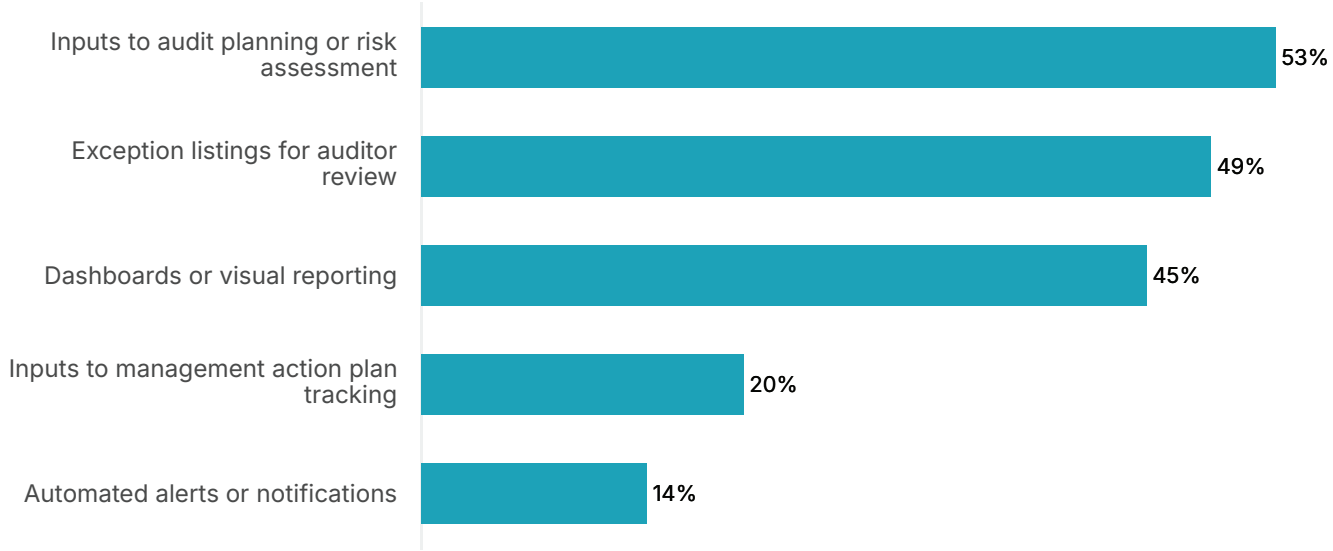


Exhibit 12: Data analytics tools used by internal audit (multiple responses permitted)

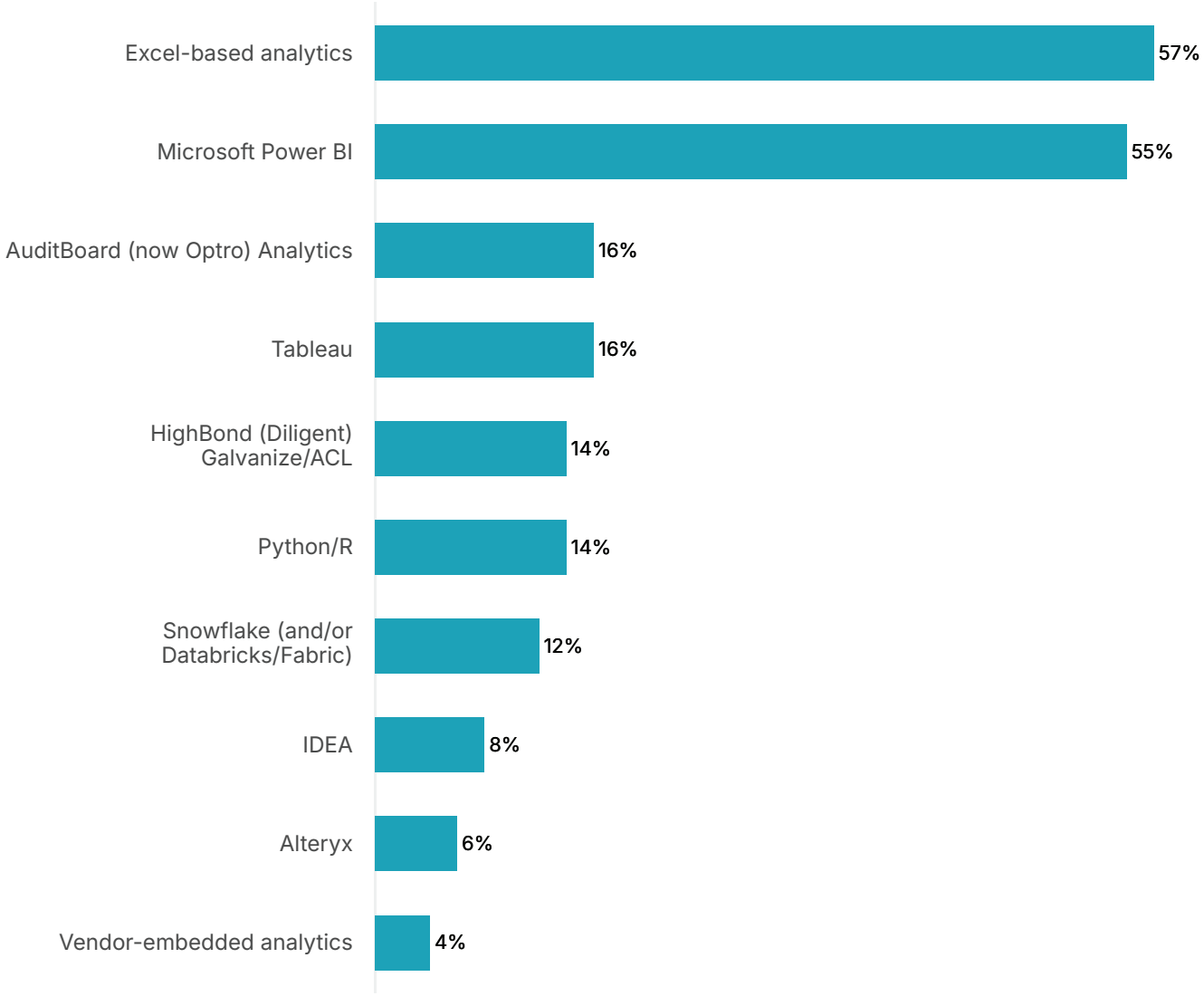


Exhibit 13: GRC tools used by internal audit (multiple responses permitted)

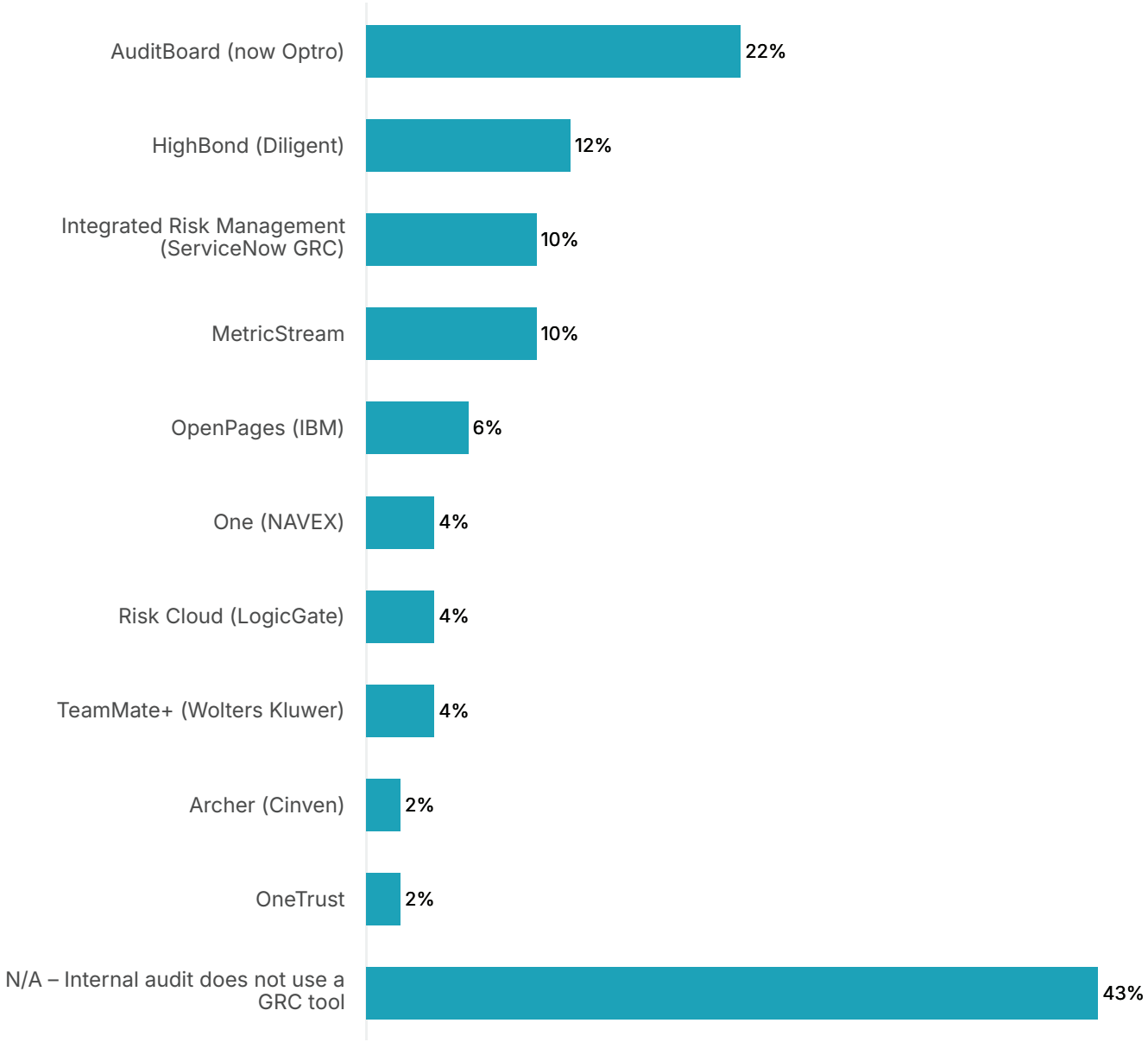
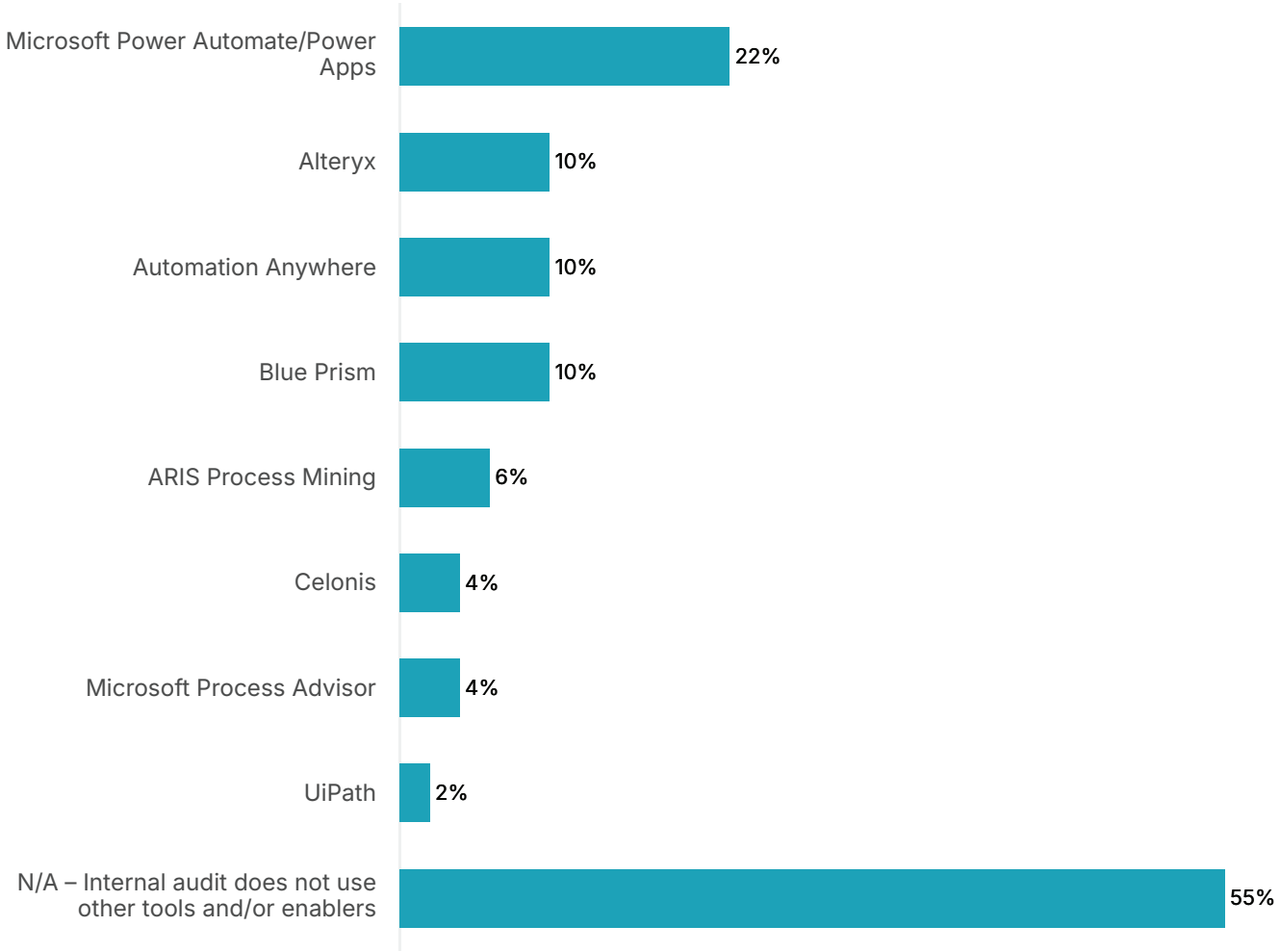


Exhibit 14: Additional tools/enablers used by internal audit (multiple responses permitted)



Internal audit structure and reporting

Exhibit 15: Count of assurance engagements on an annual internal audit plan by organizational revenue

Survey Respondents %		14%	39%	23%	12%	4%	8%
Size (revenue in USD)		Less than $1 billion	$1 billion to less than $5 billion	$5 billion to less than $10 billion	$10 billion to less than $15 billion	$15 billion to less than $20 billion	$20 billion or more
Count of Assurance Engagements	35+	14%	15%		16%	50%	50%
	30-34			8%			
	25-29			8%	17%		25%
	20-24		10%	17%	17%		25%
	15-19		10%	8%	17%		
	10-14	14%	25%	17%	17%		
	<10	72%	40%	42%	16%	50%	

Exhibit 16: Average number of hours per assurance engagement on an annual internal audit plan by organizational revenue

Survey Respondents %		14%	39%	23%	12%	4%	8%
Size (revenue in USD)		Less than $1 billion	$1 billion to less than $5 billion	$5 billion to less than $10 billion	$10 billion to less than $15 billion	$15 billion to less than $20 billion	$20 billion or more
Assurance Engagement Hours	400+		30%	18%	49%		50%
	350-399	33%	15%		17%		25%
	300-349	33%	5%	18%	17%		
	250-299	17%			17%		25%
	200-249	17%	25%				
	100-199		15%	9%			
	<100		10%	55%		100%	

Exhibit 17: Count of advisory engagements on an annual internal audit plan by organizational revenue

Survey Respondents %		14%	39%	23%	12%	4%	8%
Size (revenue in USD)		Less than $1 billion	$1 billion to less than $5 billion	$5 billion to less than $10 billion	$10 billion to less than $15 billion	$15 billion to less than $20 billion	$20 billion or more
Count of Advisory Engagements	35+		15%				
	30-34						
	25-29						
	20-24		5%				
	15-19			9%		50%	50%
	10-14		5%	18%	17%		
	<10	100%	75%	73%	83%	50%	50%

Exhibit 18: Average number of hours per advisory engagement on an annual internal audit plan by organizational revenue

Survey Respondents %		14%	39%	23%	12%	4%	8%
Size (revenue in USD)		Less than $1 billion	$1 billion to less than $5 billion	$5 billion to less than $10 billion	$10 billion to less than $15 billion	$15 billion to less than $20 billion	$20 billion or more
Advisory Engagement Hours	400+		20%		50%		50%
	350-399	29%	10%				
	300-349	14%		8%			
	250-299		5%	8%			
	200-249	14%	10%	17%	33%		25%
	100-199	14%	35%				25%
	<100	29%	20%	67%	17%	100%	

Exhibit 19: Top organizational change/change management risk areas (multiple responses permitted)

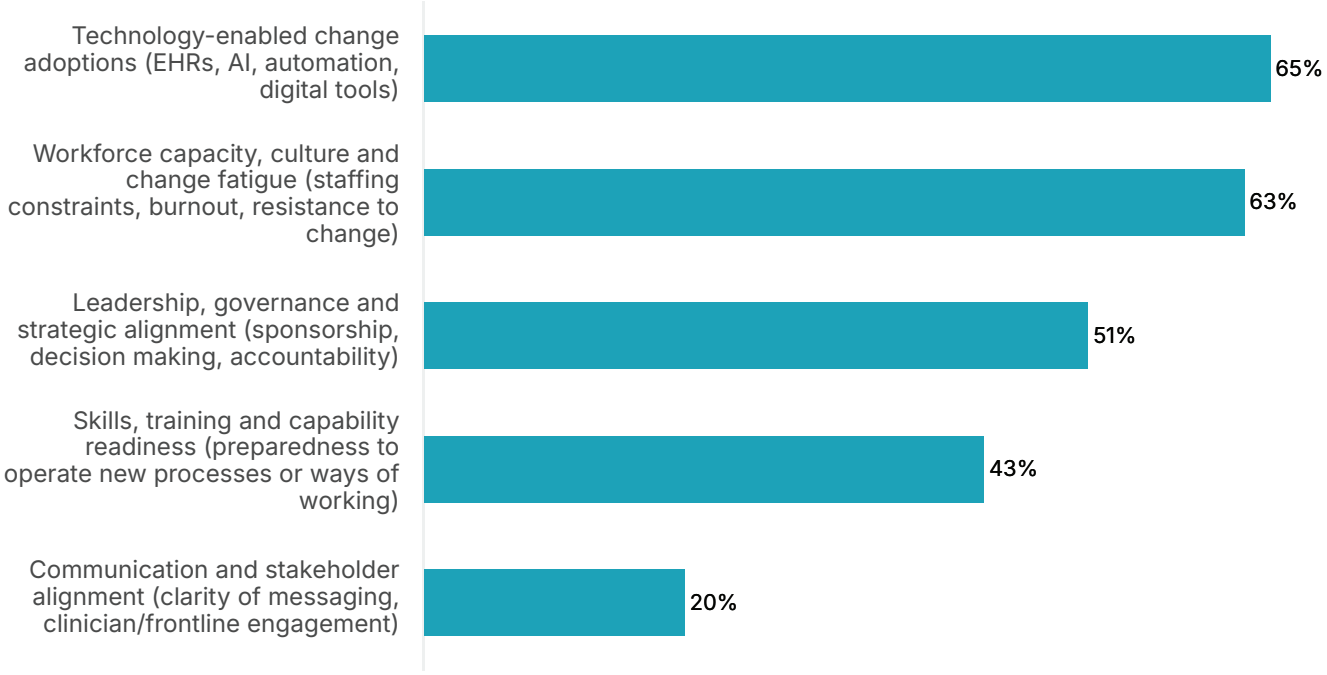


Exhibit 20: Internal audit reporting lines (administratively vs. functionally)

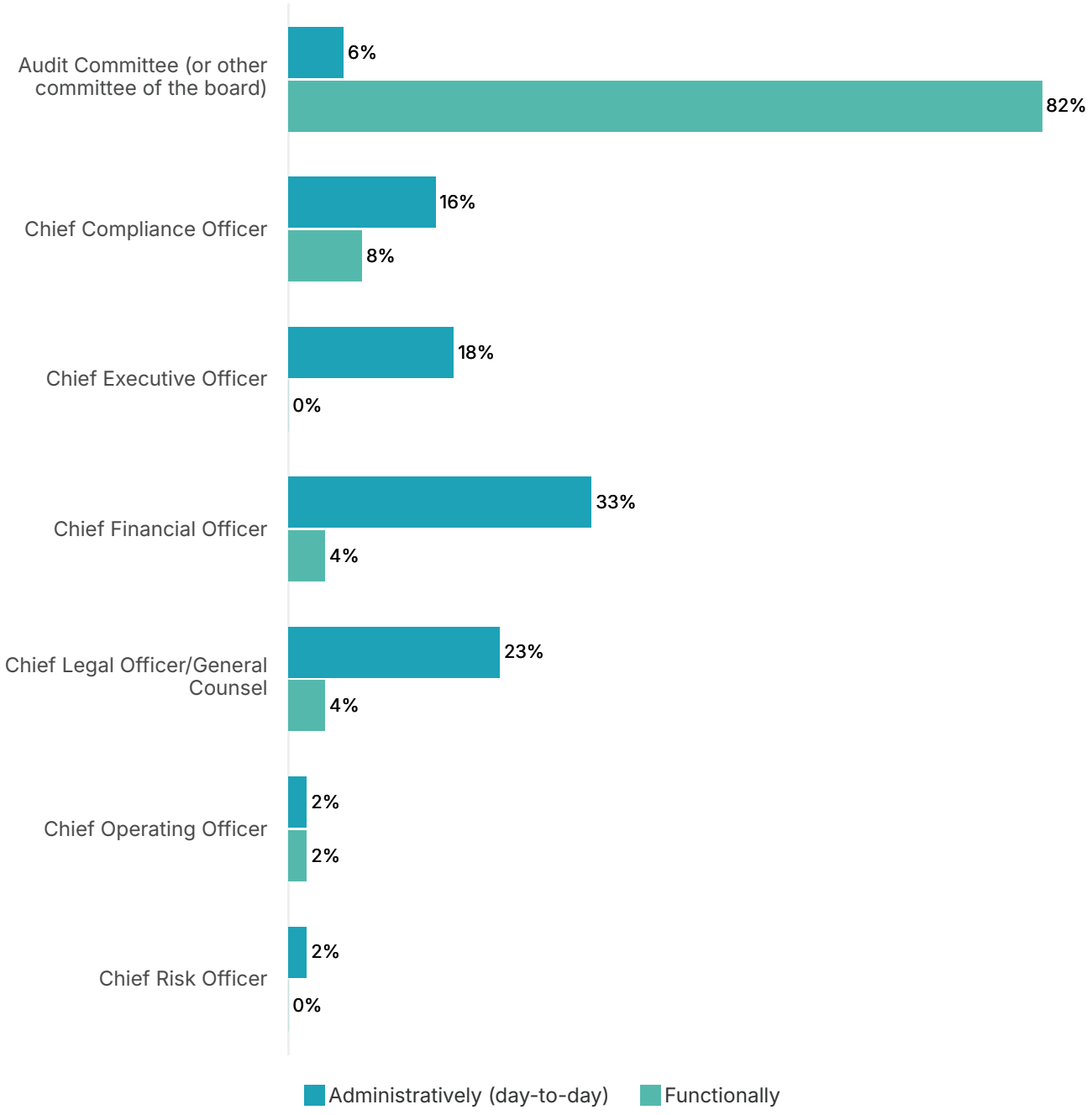


Exhibit 21: Other functions which the audit committee has responsibility for and/or receives reports from (multiple responses permitted)

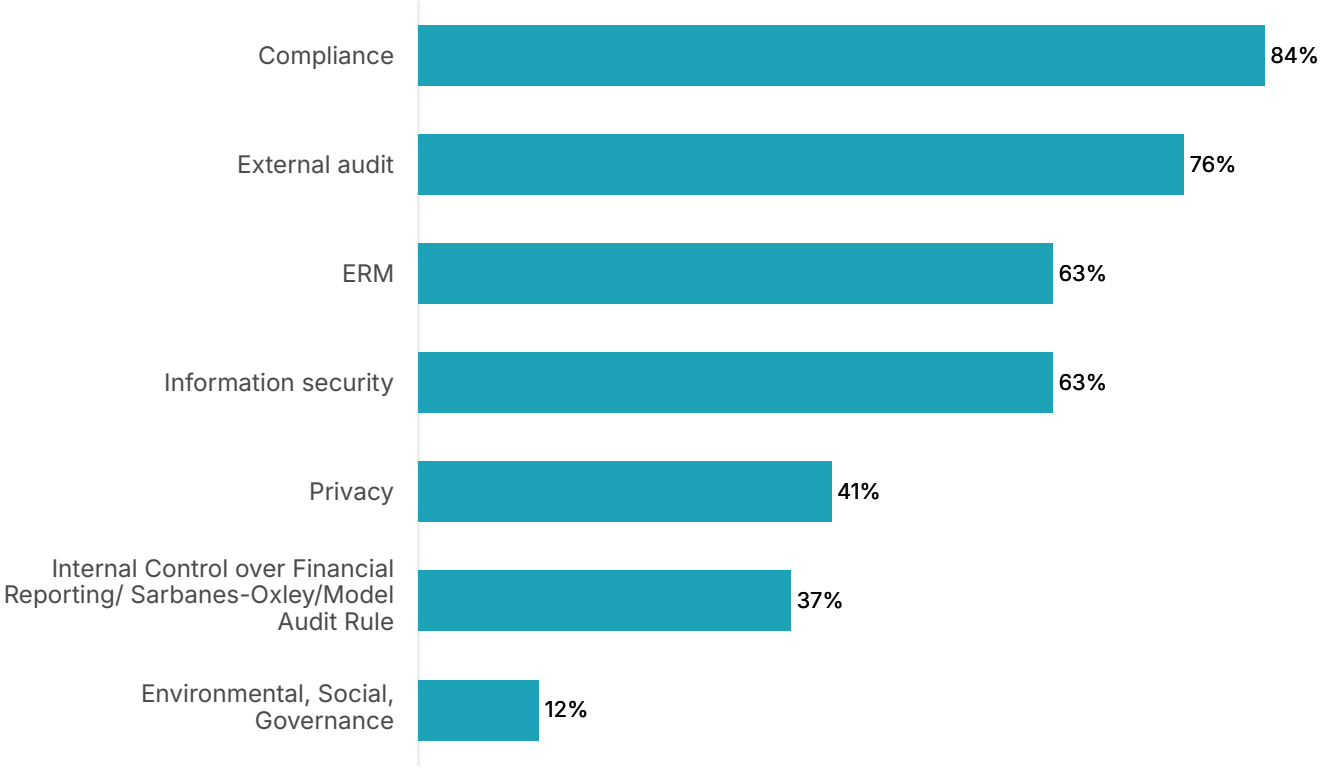


Exhibit 22: Allocation of time budgeted by audit area

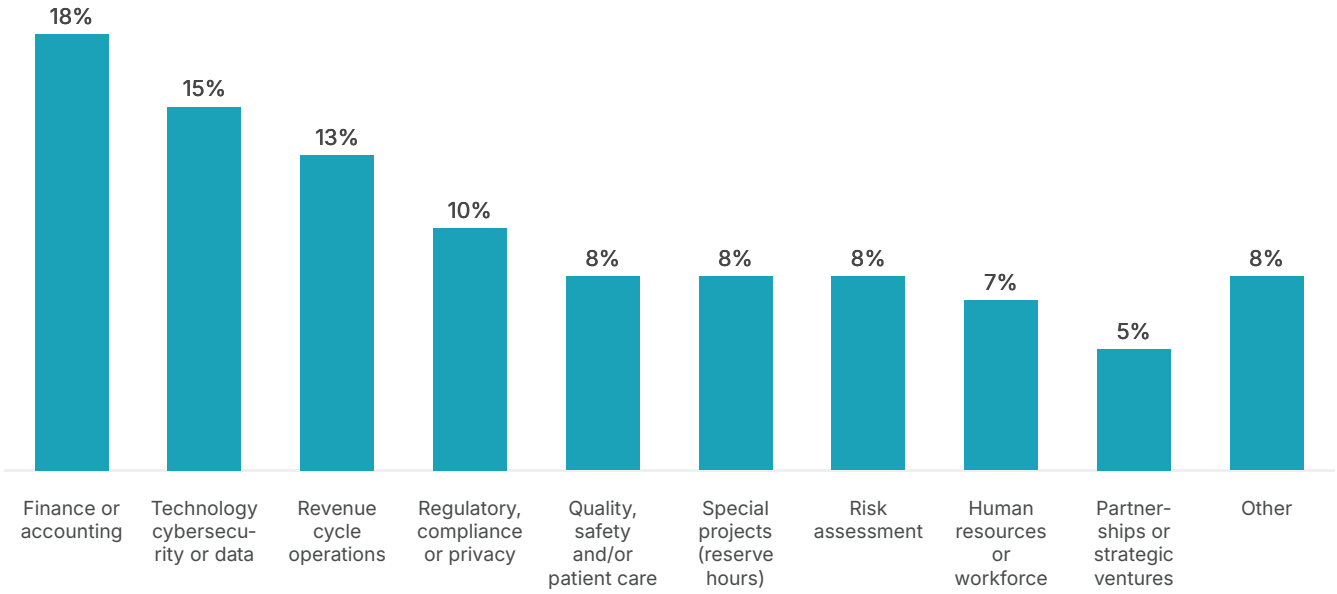


Exhibit 23: Audit areas where organizations co-source with a strategic partner/third-party vendor (multiple responses permitted)

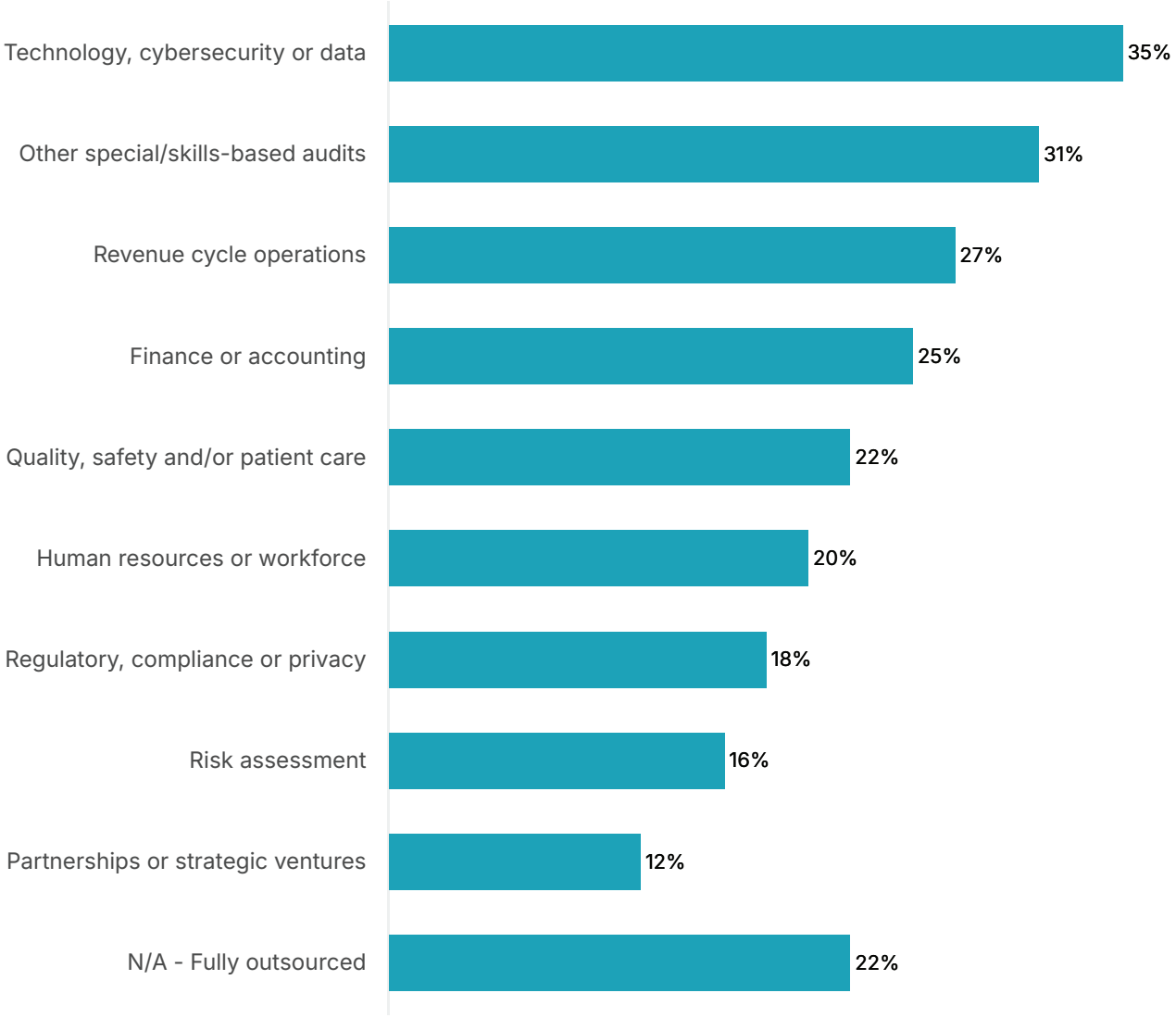


Exhibit 24: Organization's compliance philosophy with Sarbanes-Oxley Act (SOX)

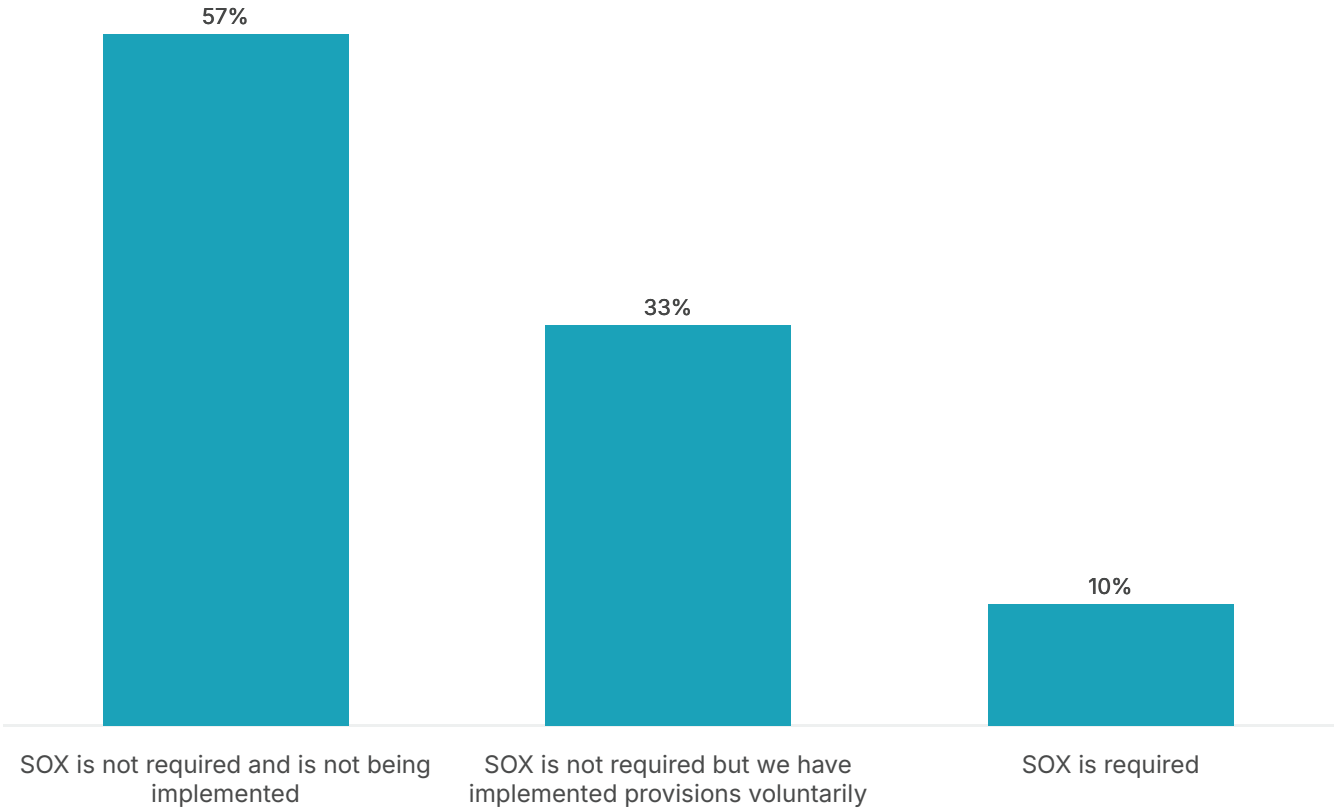
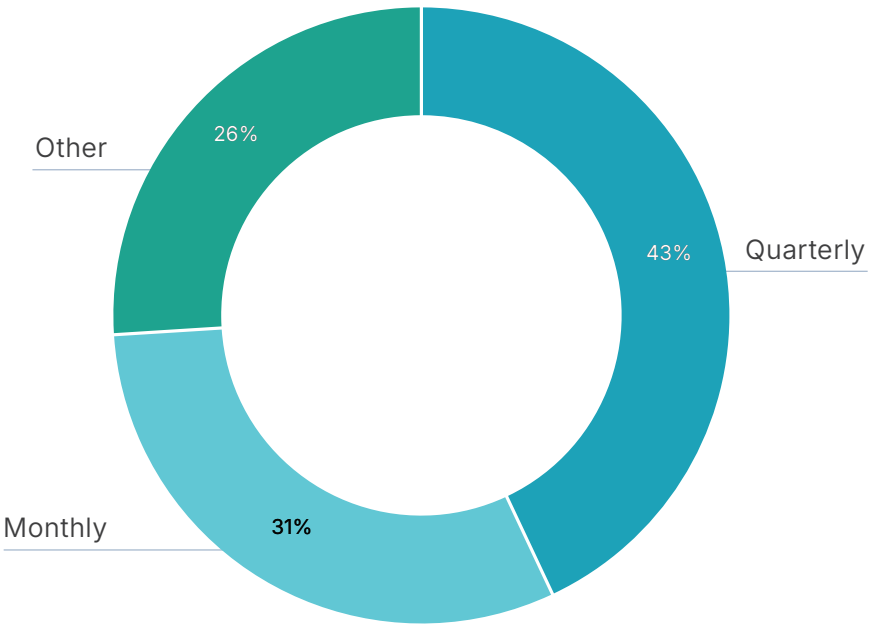


Exhibit 25: Frequency of following up on outstanding action plans



Risk assessment practices

Exhibit 26: Frequency of internal audit risk assessment process

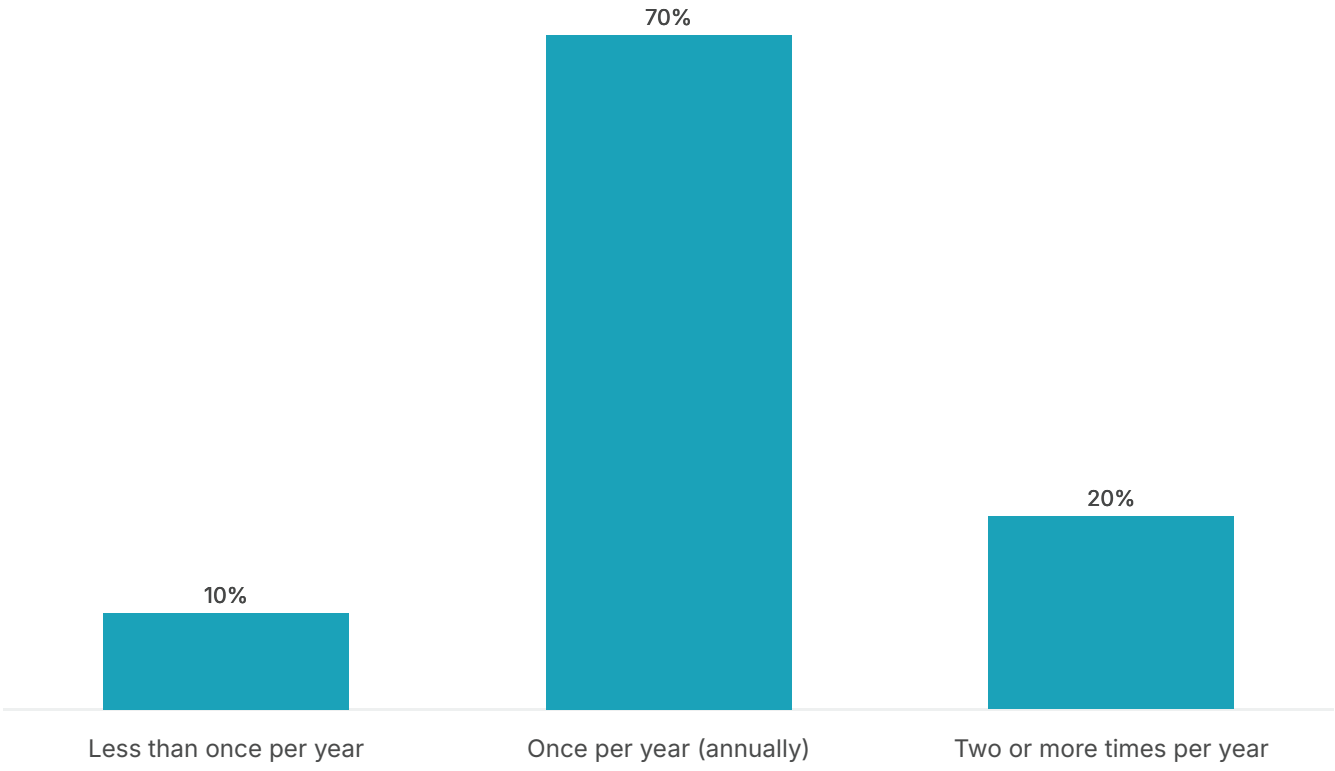
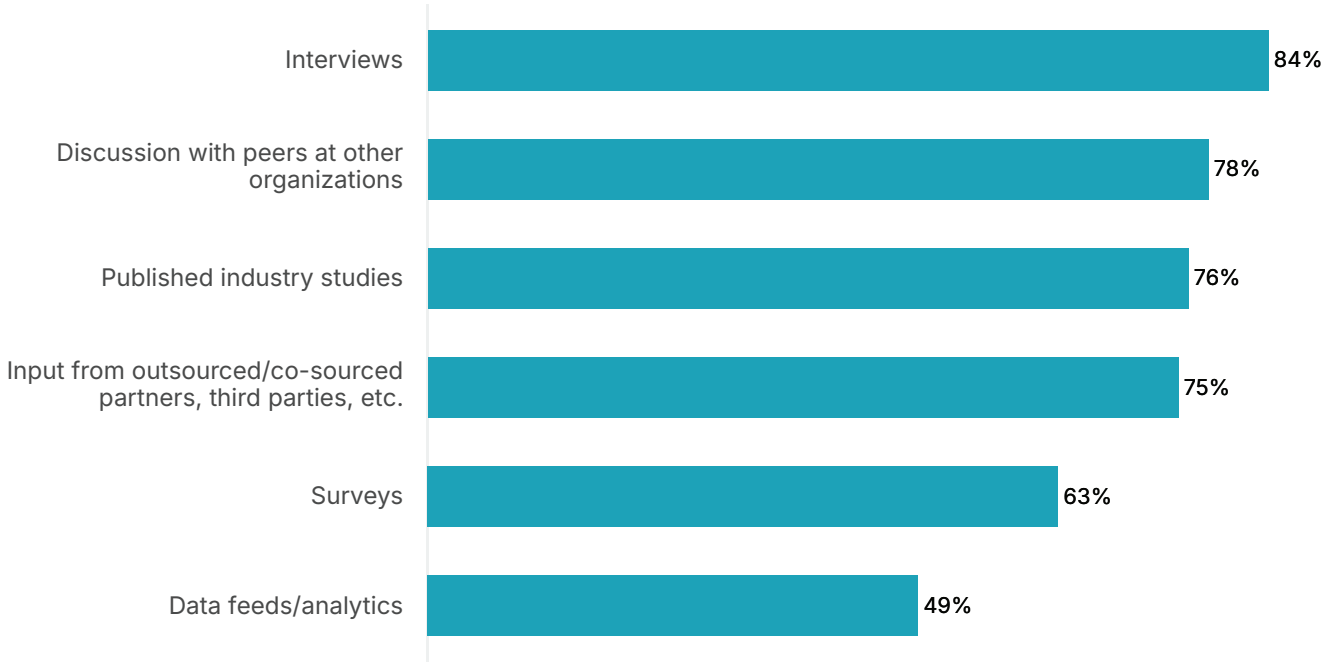


Exhibit 27: Inputs informing the internal audit risk assessment process (multiple responses permitted)



Internal audit's collaboration with compliance and ERM

Exhibit 28: Audits are performed at the request/on behalf of the compliance function

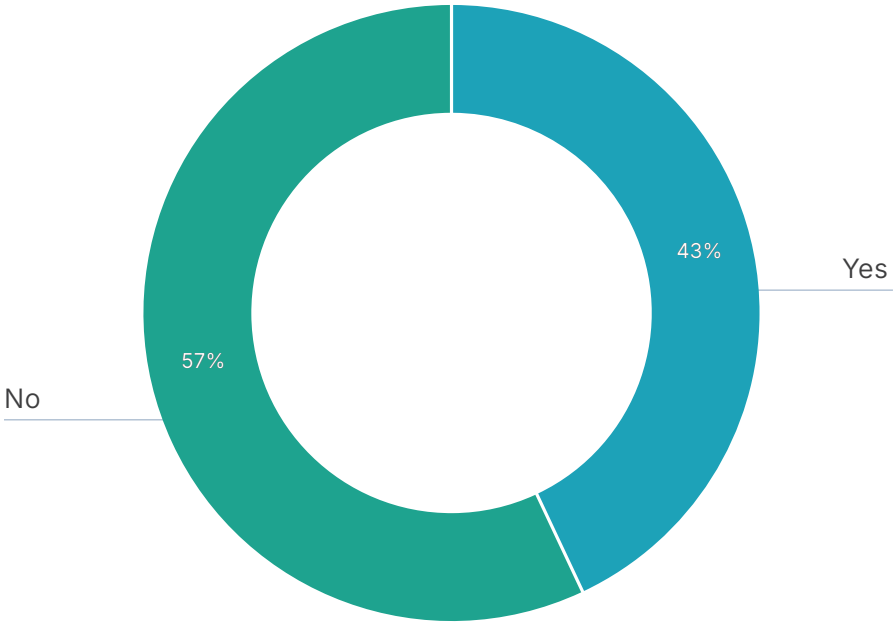


Exhibit 29: The compliance leader (e.g., CCO) and internal audit leader roles are held by the same individual within the organization

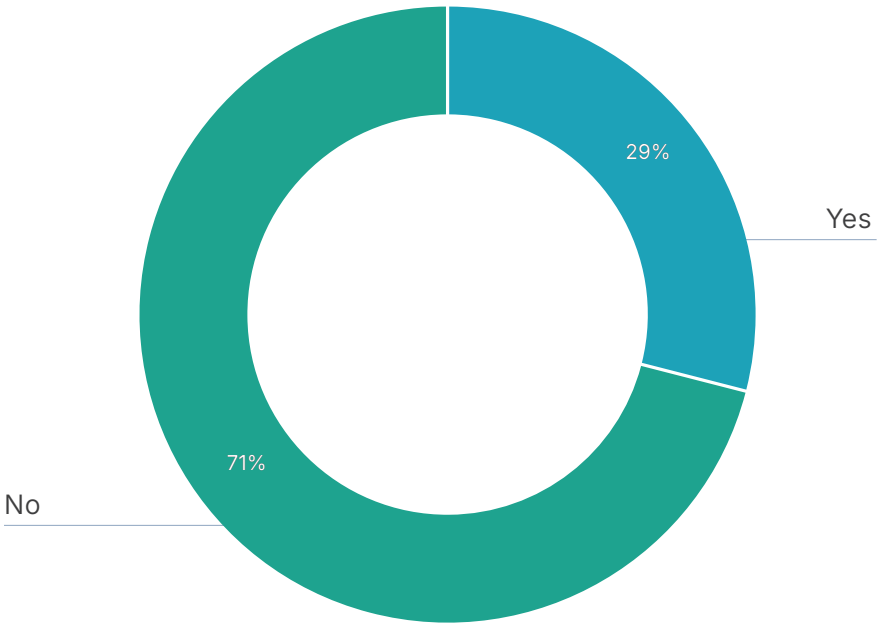


Exhibit 30: Role of internal audit as it relates to fraud risk management (multiple responses permitted)

Exhibit 31: Executive sponsor leading the fraud risk management program

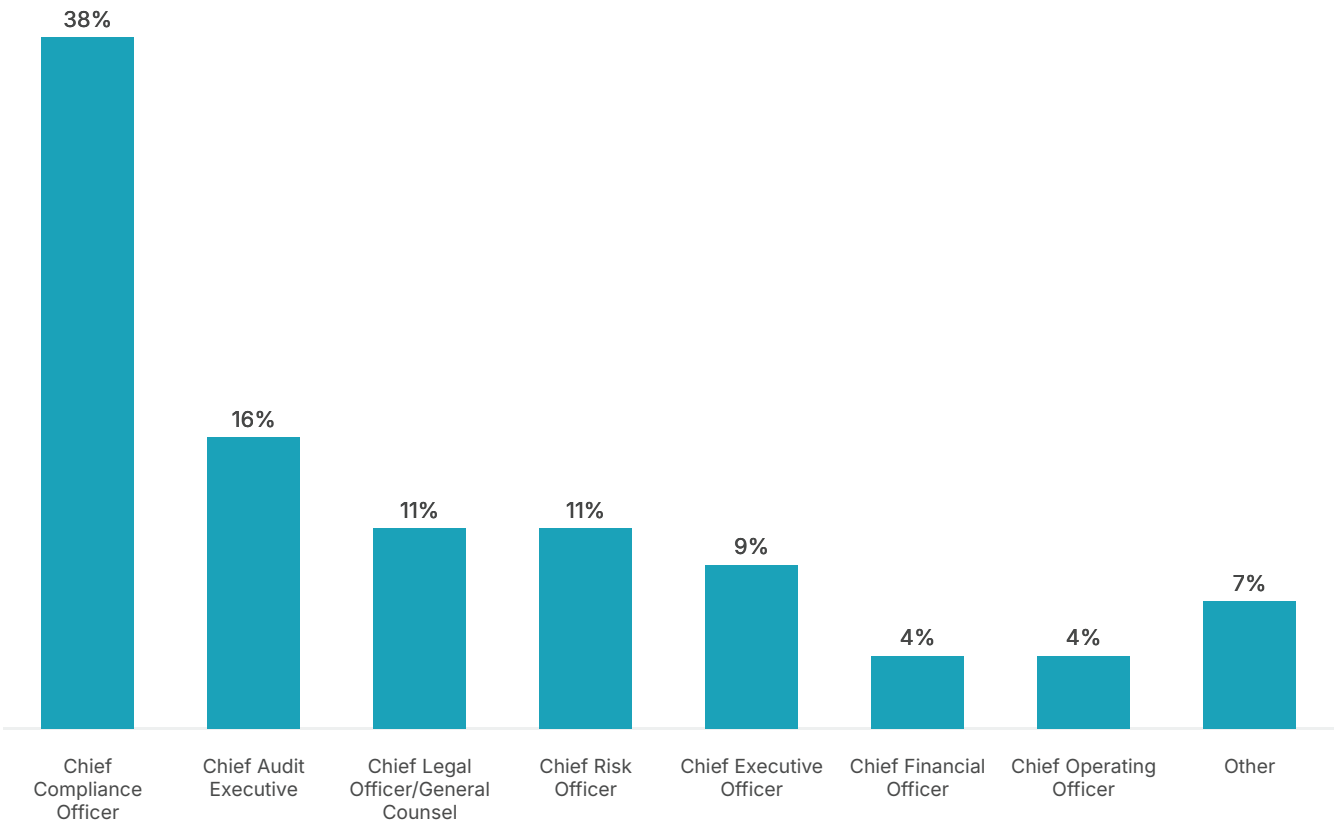


Exhibit 32: Role of internal audit as it relates to enterprise risk management (ERM)

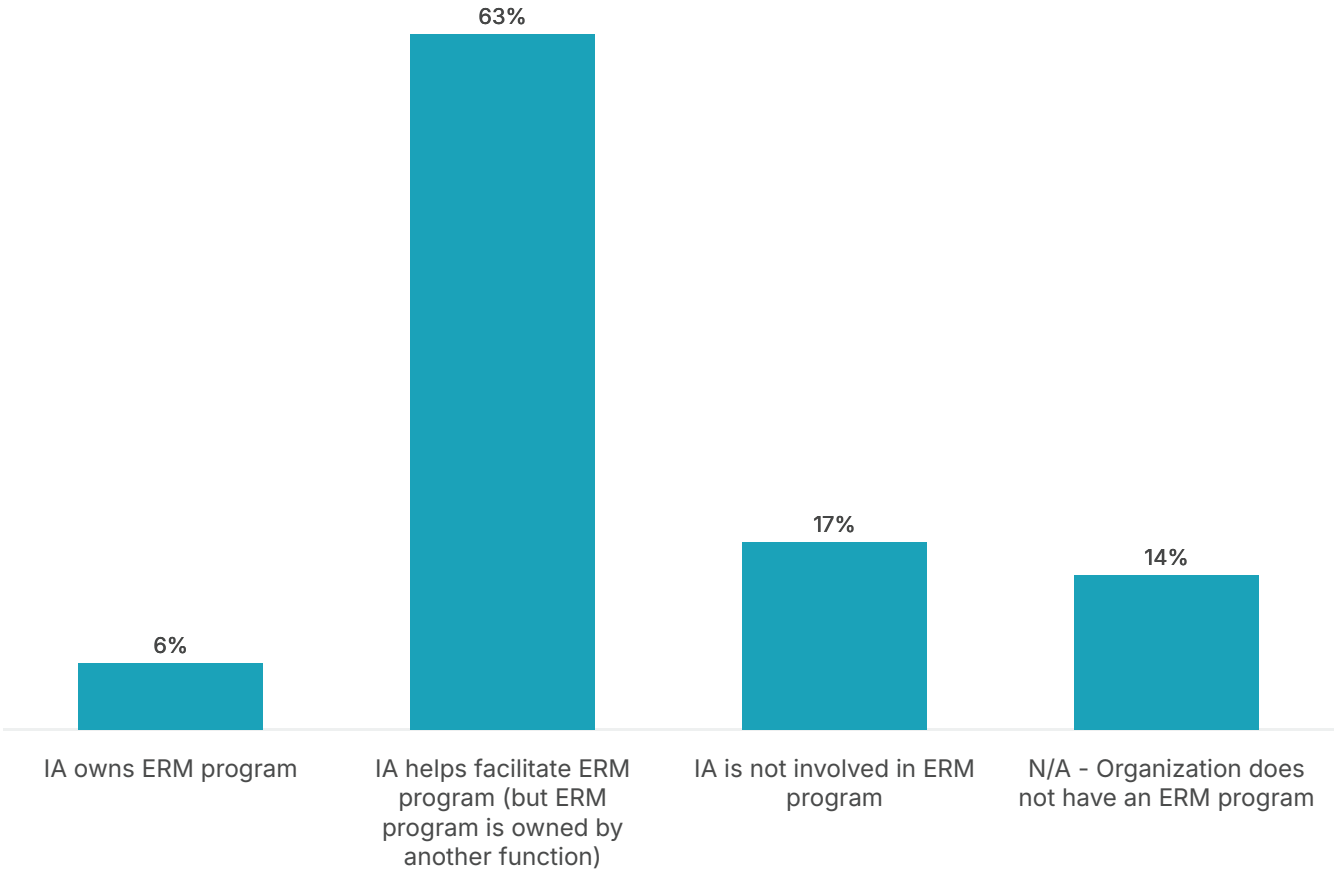


Exhibit 33: Executive sponsor leading the organization's ERM program

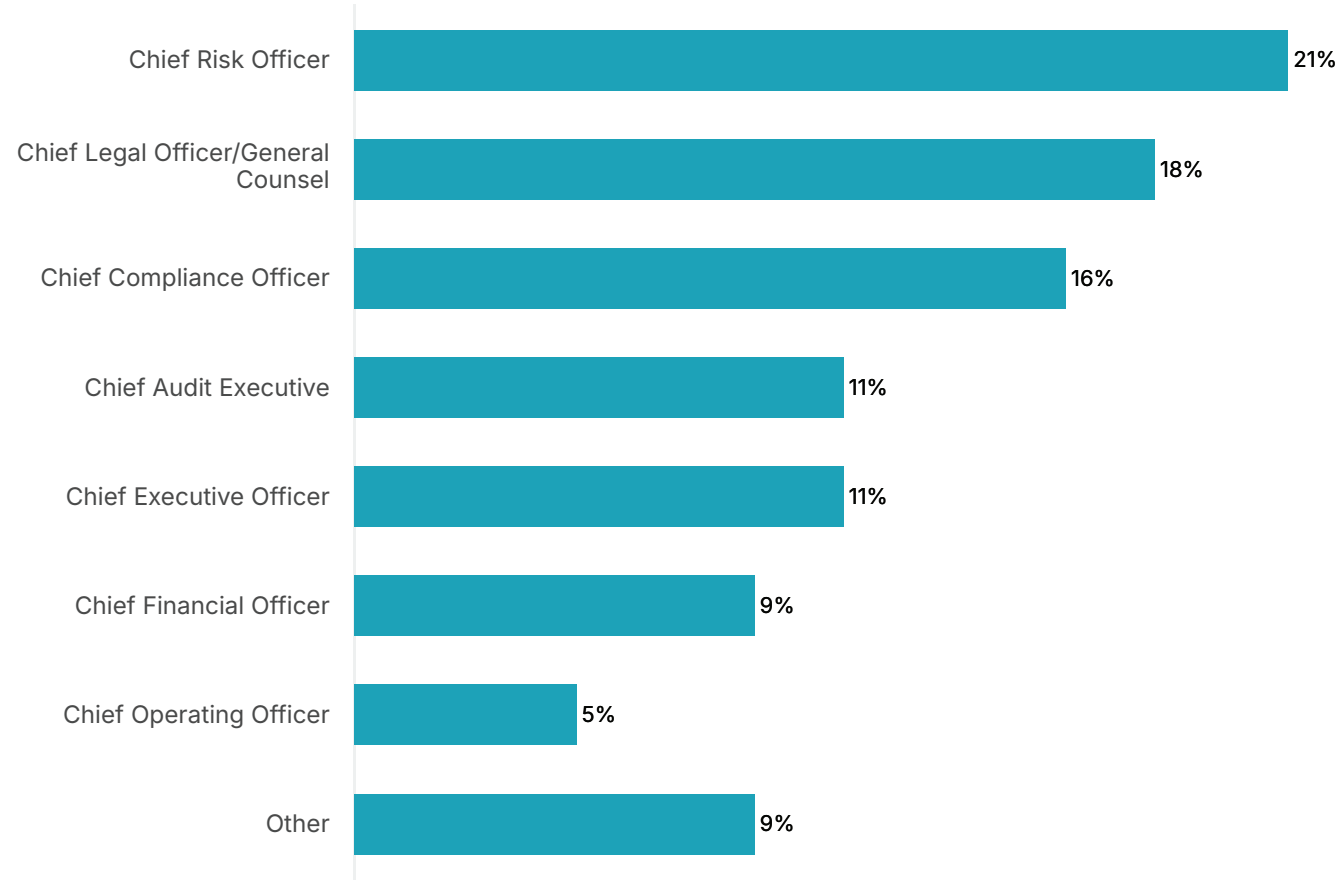


Exhibit 34: Reason why an ERM program does not exist in the organization (multiple responses permitted)

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organizations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the *Fortune* 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Our Healthcare Internal Audit Solutions

Healthcare organizations today are faced with myriad challenges and many are underutilizing one of their greatest assets: internal audit. Leading internal audit functions have moved well beyond checking the box on policy compliance and serve as a strategic partner to help ensure their organizations become more innovative and explore new technologies, identify and mitigate emerging risks, develop creative solutions to complex business challenges, and encourage best practices to enhance business functions. Protiviti's industry-leading healthcare internal audit solutions are flexible with proven methodologies, provide access to a vast array of skills, are value-added and collaborative, incorporate tools and techniques such as RPA and advanced analytics, and allow us to be a strategic partner in helping your organization confidently face the future.

To learn more about Protiviti's Healthcare Internal Audit practice, please watch the following video: Protiviti Healthcare — Internal Audit Solution.

Contacts

Richard Williams
Global Practice Leader, Healthcare Industry
+1.214.395.1662
richard.williams@protiviti.com

Matt Jackson
Healthcare Internal Audit Practice Leader
+1.214.284.3588
matthew.jackson@protiviti.com

11,000+	90+	25+	$2 BN
Protiviti professionals*	office locations worldwide	countries	in revenue*

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®