ahia
Assoc. of Healthcare Internal Auditors

protiviti®
Global Business Consulting

Healthcare internal auditors prioritize cybersecurity, business performance and technology modernization

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

Table of Contents

Executive Summary

On the heels of the lengthy and exhausting public health emergency (PHE), the healthcare industry has been facing the challenges of the financial downturn and ongoing struggle to return to business as usual. Healthcare providers and payers are working to address a number of unique issues, including some that existed pre-pandemic, while facing the reality of the current landscape.

According to the latest Healthcare Internal Audit Plan Priorities Survey conducted by Protiviti and the Association of Healthcare Internal Auditors (AHIA), the top audit priorities for healthcare organizations in 2023 are encompassed in seven themes which are highlighted below and discussed in further detail in the report that follows.

Cybersecurity, Physical Security and Protecting Sensitive Information

Cybersecurity practices and posture tops the list of internal audit (IA) priorities in our 2023 survey. Healthcare organizations continue to be prime targets for cyber and ransomware attacks, with severe consequences including disruption of essential systems, revenue loss and compromised patient care. Attackers are taking advantage of the healthcare industry's complex organizational structures, outdated technology, and cultural need to protect their patients more than anything else, which drives this as a top priority on IA plans. Other top priorities for IA teams include user access management and physical security.

Human Resources, Benefits and Workforce Challenges

Human resources, benefits and workforce challenges rank as the second highest priority in 2023. Employee time/expense reporting and payroll are critical personnel operations for healthcare organizations as they face rising cost pressures in the post-pandemic environment. Many healthcare organizations have chosen to reduce staff to maintain healthy margins, even as they grapple with meeting and maintaining adequate clinical staffing levels. Workforce issues, including employee retention, succession planning and total rewards, are an ongoing challenge that IA can help address through focused audit efforts.

Financial Integrity

Issues around financial integrity rank high in the list of priorities for internal auditors, with accounts payable (AP) coming in as the fifth highest priority in 2023. Changes to the ecosystem due to emerging technologies, and fragmentation of people and processes due to trends in outsourcing to external parties, add to risks that must be reviewed by IA when auditing AP. Finance and accounting departments must address changing regulations, new or updated payment methods, impacts of inflation, and new technologies to determine their impacts to the organization. Lack of qualified staff and issues accessing data necessary to complete modeling analyses make it difficult for finance and accounting departments to keep up with requests for detailed analysis in addition to their monthly financial reporting duties. As the department grows increasingly busier, valuable IA projects would include validating analysis methods, components of modeling, and internal controls. Capital projects also continue to be an area of significant concern for healthcare IA functions to review within their organizations due to their complex nature, unpredictability, long-term planning requirements, and schedule and budget constraints.

Fraud, Risk and Compliance

U.S. healthcare industry fraud costs tens of billions of dollars each year. Minimizing fraud, waste and abuse, including both employee and third-party threats, is a clear priority for healthcare organizations, ranking as the third highest priority in our survey. Reviewing comprehensive fraud management policies that can help guide organizations and protect themselves from financial losses, reputational damage, legal ramifications and financial penalties should be a priority, as well as looking at common and department-specific fraud scenarios. Pharmacy operations and drug distribution/management are also a priority area for internal auditors, especially as healthcare organizations address recent regulatory changes including those related to drug waste billing, 340B contract pharmacy-related restrictions and the Controlled Substances Act. Noncompliant pharmacy practices should be audited as noncompliance can lead to millions of dollars in lost revenue, hefty fines and lost patient confidence due to reputational harm. Provider compensation continues to remain an area of significant concern for health systems that IA can assist with, especially due to the federal government’s increased regulatory efforts in preventing and prosecuting healthcare fraud through the Anti-Kickback Statute and Stark Law provisions.

Revenue Integrity and Margin Improvement

Revenue integrity and margin improvement are a continuing battleground that is ripe for IA to be able to show some return on investment and be a strategic partner for their organizations. The conclusion of the PHE brought an end to pandemic-related federal funding streams, creating a financial challenge for healthcare organizations as they look for ways to improve revenue cycle and charge capture accuracy and generate a demonstrable return. Compliance with clinical documentation, coding and billing requirements can help organizations ensure accurate revenue and avoid revenue loss due to recoupments, refunds and fines.

Technology Modernization and Leveraging Data

Adoption rates for new cloud-based technologies continue to increase as healthcare organizations update and/or implement new electronic health record (EHR) systems, enterprise resource planning (ERP) systems and more, and see benefits that include streamlined operations, improved efficiency and enhanced care. But cloud-based technology can create additional challenges that IA should focus on to help ensure that these applications are properly secured from the standpoint of sensitive access, segregation of duties, privacy and provisioning.

Additionally, while emerging technologies like artificial intelligence (AI) and machine learning (ML) rely heavily on data, the healthcare industry lacks effective data lifecycle management strategies and foundational data governance practices necessary to optimize data to drive insights and support decision making. Internal audit should be reviewing their organizations' AI and ML strategies and data governance practices. Initiatives to drive data integrity and data-usage guidelines should be included on the IA plan when the organizations are developing roll-out strategies for these technologies.

Third-Party Risk, Supply Chain and Continuity of Operations

Healthcare organizations partner with third parties to outsource services, drive service excellence, increase efficiency, control costs and provide other competitive advantages. But there is tremendous pressure on organizations to ensure third-party vendors maintain compliance with internal policies and evolving regulations. Vendor risk management (VRM) has become a critical routine function; but while healthcare executives recognize its importance, few can credibly report they are doing it effectively. Internal audit is one way organizations can help grasp all of the risks associated with third parties, joint ventures, etc.

Additionally, resilience has been top of mind for supply chain leaders over the last three years and continues to be a priority to be looked at by IA, as capital equipment, supplies and purchased service costs are some of the largest costs for healthcare systems, usually only behind labor. Resilience and visibility into all processes and policies in each supply chain department is an ongoing priority for IA teams to ensure the organization's supply chains facilitate the quality, safety, continuity and lowest possible cost of patient care.

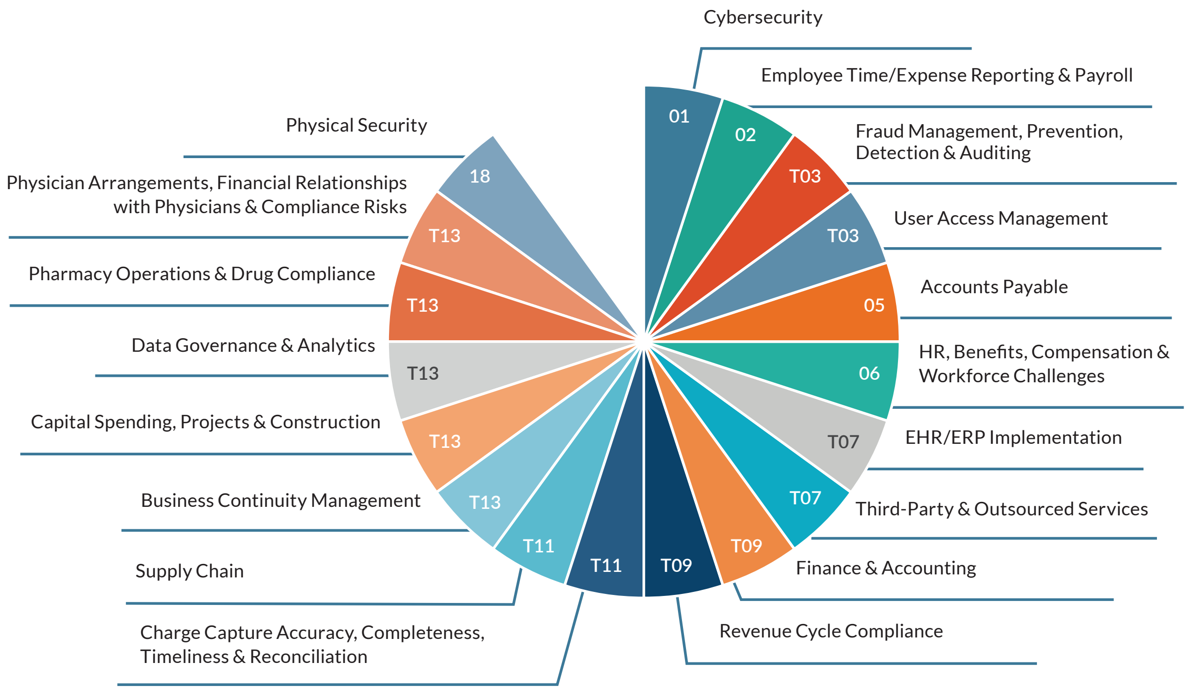
Business Continuity, Emergency Management and Pandemic Preparedness/ Response continue to be among the top priorities for IA teams as they face a daunting risk horizon that includes sophisticated cybersecurity threats; gaps in technology resilience capabilities; enhanced regulatory scrutiny; complex supply (and value) chains informing all aspects of healthcare service delivery; unforeseen climate behavior increasing the risk of widespread geographical disruption; and a global marketplace that is hesitant to lock down again.

In Conclusion

As healthcare organizations continue to recover from the PHE and face disruptions from an uncertain economy, workforce challenges, cyberthreats, changing regulations and the increasing speed of emerging technology, the findings from our latest Healthcare Internal Audit Plan Priorities Survey point to the important role IA plays in helping organizations address their most urgent challenges.

Internal Audit Plan Priorities and Key Themes

Top healthcare internal audit plan priorities



Note: "T" indicates a tie.

- ■ Cybersecurity, Physical Security and Protecting Sensitive Information
- ■ Human Resources, Benefits and Workforce Challenges
- ■ Financial Integrity
- ■ Fraud, Risk and Compliance
- ■ Revenue Integrity and Margin Improvement
- ■ Technology Modernization and Leveraging Data
- ■ Third-Party Risk, Supply Chain and Continuity of Operations

"Healthcare organizations are experiencing new waves of transformation with the end of the COVID- driven public health emergency and the many process and infrastructure changes that come with the close of related government-funded programs. An uncertain economic climate, ongoing cybersecurity risks and concerns, emerging technologies combined with limited skill sets to leverage them, and talent shortages that are becoming more critical within different healthcare positions all are driving waves of disruptive change that present significant challenges for leadership, including CAEs and their internal audit functions. As the industry continues to transform, internal audit innovation, including use of data analytics and enabling technologies as well as high-impact reporting, should be top priorities for audit groups."

— **Richard Williams**
Managing Director
Global Healthcare Practice Leader, Protiviti

THEME 1 — CYBERSECURITY, PHYSICAL SECURITY AND PROTECTING SENSITIVE INFORMATION

01 Cybersecurity Practices and Posture

Cybersecurity threats, including ransomware incidents, have severe consequences for healthcare organizations, including disrupted essential systems, jeopardized patient treatment, lost revenue capture, regulatory noncompliance, legal implications and brand reputation. As a result, this topic is top of mind for many healthcare leaders and board members and is a constant on internal audit plans. The key consideration: how does internal audit continually refocus these efforts to provide new insights and ongoing value?

Attackers are focused on exploiting their victims in multiple ways, usually to profit directly through ransoms paid to release information back to the organization and/or to keep the attackers from disclosing compromised data to the public. As a result, attackers are encouraged to target organizations that have more to lose if they fall victim to an attack; healthcare providers and payers are high on that list. This financial motivation, combined with the complexity of healthcare organizations, creates additional security challenges with multiple ingress and egress points. Additionally, diverse healthcare user groups, whose members are by nature driven to help and serve, are typically more susceptible to social engineering. Finally, outdated technology systems, commonly used in healthcare, add technical vulnerabilities because some may not be supported with regular security updates.

Healthcare internal audit teams should look at the different cybersecurity program and control aspects that their organizations should have in place to protect their data environment by understanding the typical attack techniques these nefarious actors utilize. They should assess these aspects broadly from a programmatic consideration and do deeper dives on key or critical control aspects to provide the most value in these audit efforts.

- Programmatic considerations include assessing the security risk analysis and associated risk management strategy, reviewing the program maturity using established frameworks (e.g., NIST, HIPAA, CIS, PCI, ISO), reviewing for pervasiveness of assessments across all assets/environments, etc.
- Specific review considerations should include identity and user access management, multifactor authentication (MFA) use, social engineering awareness, incident response planning and preparedness, privileged access management (PAM), third-party risk management, cloud security controls (including SaaS solutions that may be owned by business departments), vulnerability and penetration testing, disaster recovery preparedness, etc.

T03 User Access Management

Consistent and controlled user access management in today's complex and ever-expanding healthcare environments is no easy task. While the aim is to utilize single sign on (SSO) as pervasively as possible, healthcare providers deal with a myriad of applications that makes that goal difficult to achieve. In addition, there is a high level of complexity around the different user profiles that require unique access to perform their job responsibilities. While an individual's background and title may be "nurse," that title does not scratch the surface of all the responsibilities the individual may perform on behalf of the organization. That individual could function as a scheduler, case manager, charge nurse, claims reviewer, etc., and their access must be provisioned to allow for their applicable role.

Additionally, the user base within healthcare organizations is intricate and may include nonemployee users (e.g., contractors, third parties, independent providers) who may need and have access into the organization's systems. Tracking the status of these nonemployees can be a significant challenge for even the most mature entities. Onboarding processes are typically requested at the last minute and rushed to enable a user to perform their job responsibilities when they start. Offboarding processes are often underdeveloped, under communicated and inconsistent, leading to users whose access outlives their relationship with the organization.

Audit teams should:

- Assess user-access-management programs for areas of improvement and determine where procedural breakdowns may occur.
- Test areas that are anticipated to be automatic or have recently been automated to determine whether user access is added and removed as intended, otherwise these may suffer from undiscovered bugs or breaks in the automation logic.
- Assess whether a full list exists of those individuals, departments and teams who are responsible for provisioning access within systems that require a manual interaction. Determine how these groups are communicated with so they are aware of all the employment changes and terminations they need to act upon, what documentation is retained, what processes differ from standard expectations, etc.

User access management is an area that benefits from pervasive testing and continuous monitoring to further help address the risks that individuals are provisioned and retain only that access that is minimally necessary to perform their job responsibilities.

18 Physical Security

Physical safety and security continues to be a top-of-mind issue in 2023, especially for healthcare providers. These organizations need to continue to examine and amend their physical security and emergency management plans to ensure they are mitigating new and existing risks and have plans in place to respond as safety issues arise. This includes:

- Proactively reviewing existing and/or creating physical security policies/ procedures to ensure regulatory compliance and facilitate best practices.
- Performing an annual physical security risk assessment for each facility to ensure site-specific potential risks or issues are identified and evaluated.
- Promoting collaboration among Health and Safety, Security/Police Force, and Operations leadership to foster a strong culture of safety and workplace violence prevention.

- Leveraging design thinking sessions to gather end users' feedback on where they have encountered safety and security concerns.
- Understanding the environment where healthcare providers are delivering care, including the surrounding communities and patient demographics that the organization serves.
- Incorporating enhancements for the safety of staff, patients and visitors to increase overall morale and organizational reputation.
- Establishing plans for preventing, mitigating and responding effectively to identified threats and incidents.
- Periodically drilling the test plans and performing a tabletop exercise to evaluate and determine if the plans mitigate the underlying risk.
- Completing after-action reports following any drills or events to assess the performance of the team involved, including strengths and lessons learned. The effectiveness of communication also should be evaluated to assess the coordination and response to an emergency event.

Additionally, providers should foster and promote a strong culture around physical and environmental safety by implementing protocols, performing ongoing training and maintaining an engaging health and safety management program. By creating a safer environment, providers can potentially reduce worker compensation costs, lost workdays and the risk of fines, as well as improve employee retention, morale and reputation with the community.

Key procedures when auditing include:

- Assessing policies, procedures and practices for physical security and safety to determine alignment with the Occupational Safety and Health Administration (OSHA), Centers for Medicare and Medicaid Services (CMS), associated accreditation organizations' standards, state specific regulations, and industry best practices (e.g., security camera placements, panic buttons, auto-locking doors, metal detectors).
- Evaluating programs for employee training, drills and incident reporting to validate alignment with policies and procedures, regulations and expected practices.
- Assessing the current oversight, monitoring and reporting processes related to physical security and safety, as well as incident reporting.

- Reviewing site-specific physical security risk assessments to ensure assessments are completed routinely and are individualized to identify specific concerns and risks for each facility.
- Reviewing technologies the organization utilizes for physical access control and monitoring functionalities.
- Performing interviews and on-site observations to understand current processes, evaluate the physical environment, and ensure alignment with policies and procedures, leadership expectations and regulatory requirements.
- Assessing management's tabletop exercises and after-action reporting to determine if the results mitigate the underlying risk and if all employees know and perform their required responsibilities.

THEME 2 — HUMAN RESOURCES, BENEFITS AND WORKFORCE CHALLENGES

02 Employee Time/Expense Reporting and Payroll

Employee time and expense reporting and payroll are crucial personnel operations for healthcare organizations as they strive to control costs, provide accurate reporting and produce a seamless employee experience while continuing to deliver high-quality patient care. Healthcare organizations continue to face rising cost pressures in the post-pandemic environment, which only bolsters the need for strong processes and controls.

Because payroll is one of the most significant costs for most healthcare organizations, it is important to regularly conduct thorough reviews of payroll practices. Key risk areas include employee fraud, compliance with U.S. Department of Labor and applicable state regulations, duplicate or inaccurate payroll calculations and/or payments, data integration and integrity to support financial reporting, and segregation of duties.

It is essential for employee time reporting to be as complete and accurate as possible, as it reduces the risk of related fraud and provides key insights into resource management efficiency and appropriate cost allocation through productive and nonproductive labor. Additionally, healthcare organizations must actively manage regulations associated with shift work, mandatory breaks, overtime and hour limitations while also ensuring appropriate staffing levels are in place to provide high-quality care.

It also is important to have effective processes and policies in place related to employee expense reimbursement, including purchases made with corporate credit cards and/or purchasing cards, to help control these expenses and facilitate accurate payment, accounting, and compliance with Internal Revenue Service guidelines. Healthcare organizations also need to report and track physician-related expenses properly to help ensure compliance with contracts and applicable federal and state laws (e.g., Stark Provisions, Medicare and Medicaid Anti-Fraud and Abuse).

Key tasks to perform during audits and assessments include evaluating controls and processes for adherence to regulatory requirements and internal policies, as well as performing analytics to:

- Identify potential employee time- or expense-reporting inaccuracies, missing approvals and/or outliers.
- Determine the integrity of key time-reporting system inputs and payroll outputs such as overtime pay and pay-code categorization.
- Determine compliance with regulatory requirements such as hour limitations.

06 Human Resources, Benefits, Compensation and Workforce Challenges

Workforce challenges continue for healthcare providers, including those related to staffing, employee retention, succession planning and total rewards. Struggling to maintain healthy margins, many organizations have made the difficult decision to reduce staffing while still grappling with the need to meet and maintain adequate clinical staffing levels. The increased competition for clinical staff has made an organization's culture and total rewards more significant than ever. In addition, many healthcare organizations have experienced significant growth without improving or increasing their human resources staffing and processes. This results in the same staff having to do more, often with manual processes that lack key controls.

Key procedures on which internal audit should focus include:

- Evaluating the process design, internal controls and monitoring in place for developing the company's employment brand, new employee recruiting, talent marketing and onboarding.
- Reviewing key performance indicators (KPIs) to determine sufficiency of metrics monitored/reviewed, including data sources utilized for calculating KPIs to determine consistency and reliability.

- Reviewing total rewards packages for employees.
- Assessing whether pay equity and transparency exists as required by law.
- Identifying internal controls for ensuring accuracy and appropriateness of benefits design and opportunities to improve total rewards.
- Evaluating retention metrics and company culture to assess related trends across the organization, understanding factors that may be impacting retention, and providing insights into areas for improvement across talent mobility, employee experience and organizational effectiveness.
- Evaluating processes in place for employee grievances to assess consistency of appropriate resolution.

THEME 3 — FINANCIAL INTEGRITY

05 Accounts Payable

To mitigate key risks within healthcare accounts payable departments, internal audit should focus on continuous implementation of strong internal controls, understanding changes to the ecosystem due to emerging technologies, and fragmentation of people and processes due to trends in outsourcing processes to external parties. In addition, internal audit can play a key role in training accounts payable employees on fraud prevention. Continually monitoring and improving processes such as responsibility for paying bills, vendor setup, invoice processing and invoice payment helps ensure that accounts payable operates efficiently and securely.

Technology is playing a pivotal role in the success of many accounts payable departments. By modernizing accounts payable technology, organizations are better able to integrate with their ERP systems and automate routine tasks, thereby reducing manual work and increasing the bandwidth of the department.

Ensuring segregation of duties (SOD) exist related to the Vendor Master File allows for effective and secure vendor management. To streamline the process of capturing current vendor information, a vendor management portal can be utilized within an organization’s ecosystem. A vendor portal does present some risks, so the process of updating and maintaining the vendor’s email address, which allows them access to update their profile, is critical in preventing fraudulent actors from gaining access to vendor data. Weak controls or lack of awareness can lead to monetary loss to malicious actors. Impostors can convince the company through emails or phone calls that they are working on behalf of the vendor. Accounts payable therefore must perform their due diligence to ensure they are speaking with a legitimate representative from the vendor prior to updating any payment information.

To determine if accounts payable should be in scope for the audit plan, internal audit should:

- Determine if there is a high volume of incoming questions from vendors about invoices.
- Review data analytics and key performance indicators to determine if invoices are processed timely. Identification of backlogs may lead to the discovery of inefficient or ineffective manual processes.

To ensure risks in accounts payable are mitigated, internal audit should determine if:

- Segregation of duties related to vendor creation, invoicing and payment processing are accurate.
- Policies and procedures exist and are current.
- Governance controls around vendor master setup are in place, including vendor maintenance, vendor master integrity for preventing duplicate vendors and payments, and Tax Identification Number (TIN) checks to ensure the TIN and legal name are registered with the Internal Revenue Service (IRS) and not included on any sanctions list, such as that of the Office of Inspector General.
- Non-purchase order (PO) invoice approvals are accurate per delegation of authority (DOA).
- PO approvals are accurate per DOA, the three-way match system is configured accurately, and the percentage of successful three-way matches on the first attempt is in line with industry best practices.
- Cashed checks are processed through a positive pay system to ensure they have not been altered by a fraudulent actor after issuance.
- Check stock is properly secured and accounted for.
- Outstanding payments (e.g., returned ACHs, outstanding checks, and pending credit card transactions) are monitored.
- Statement reconciliations are performed to confirm invoices are properly recorded within the system.
- Third-party confirmations are obtained from the vendor to ensure payments are applied appropriately.
- Accounts payable accrual processes and policies are accurate to ensure the financials reflect the pending liability currently managed by the department.

T09 Accounting, Finance, Integrity of Financial Data, Budgeting, Forecasting, Reserves, Treasury, Investments, Insurance, Grants and Bonds

Finance and accounting departments struggle to keep up with the demands of healthcare organizations. Several key areas need to be modeled to determine their impacts to the organization, including:

- New regulations such as the Financial Accounting Standards Board (FASB) Accounting Standards Update (ASU) No. 2023-02, Investments – Equity Method and Joint Ventures (Topic 323); environmental, social and governance (ESG) sustainability reporting requirements; Committee of Sponsoring Organizations of the Treadway Commission (COSO) supplemental guidance on effective internal controls over sustainability reporting; and more.
- New or updated payment methods, as they are developed, including insurance contract renewals.
- Impacts of inflation and ways to offset them.
- New technologies.

Lack of qualified staff and issues accessing the data necessary to complete the modeling analysis make it difficult for finance and accounting departments to keep up with requests for detailed analysis in addition to their monthly financial reporting duties.

Key areas on which internal audit should focus include:

- Data integrity — Conduct audits aimed at validating the integrity of the data used by finance to prepare journal entries, reconciliations and financial analysis to help the organization gain comfort that financial information is accurate.
- Post-implementation ERP reviews — Review any new system implementations after completion to determine whether internal controls were configured into the new system and processes. Key areas of focus include segregation of duties, data integrity, approval levels and data conversions.
- Budget assumptions — Validate assumptions used in forecasting and budgeting to help the organization gain comfort that forecasts and budgets are representative of future plans.

T13 Capital Spending, Projects and Construction

Capital projects continue to be an area of significant concern for healthcare organizations due to their complex nature, unpredictability, long-term planning requirements, and schedule and budget constraints. There are inherent challenges and risks that must be planned for and managed when undergoing major capital projects, including site conditions, labor shortages, procurement delays, safety issues and weather events. Current market risks continue to be amplified by the expected economic slowdown and rising interest rates and financing costs.

It is critical for healthcare internal audit teams to assess the control environment across the capital project and construction management lifecycle to determine whether strong processes are in place and risks are effectively managed. At a minimum, control assessments should cover procurement, contracting, change management, general cost control processes and payment application reviews. Controls within these processes should be assessed to determine whether they are effective in mitigating the risks for which they were designed. For example, payment applications and change orders should be evaluated against contract terms to determine whether the company being billed (i.e., owner) is inappropriately or inaccurately billed. Key components to test include general conditions, contingency usage, labor rates and burden, bonds and insurance, claims and disputes, project expenses and allowances, contractor fees and payments, proof of payment and final payment requirements. This will enable healthcare organizations to fully execute their capital improvement plans and prevent overspending and deferral of critical projects.

Internal audit also should:

- Evaluate compliance with federally mandated safety regulations, including barrier protection, infection control safety measures, etc.
- Assess whether projects are completed on time with minimal disruption to healthcare operations.
- Verify that the project schedule is reviewed on a consistent basis to determine if it is unencumbered, and that the following considerations are consistently addressed:
  - Advancing procurement of long-lead items such as custom-fabricated items, materials with specific certifications and high-demand specialty equipment.
  - Management of an intensified skilled-labor shortage.
  - Effective sequencing of construction activities.
  - Successful planning and communication of utility shutdowns and switchovers.

THEME 4 — FRAUD, RISK AND COMPLIANCE

T03 Fraud Management, Prevention, Detection and Auditing

Healthcare organizations continue to face challenges to minimize fraud, waste and abuse (FWA). According to the National Health Expenditure Accounts (NHEA), as reported by the Centers for Medicare & Medicaid Services (CMS), total healthcare spending in the United States is more than $4 trillion, which accounts for approximately 18% of the nation's gross domestic product.[1] The National Health Care Anti-Fraud Association reports that U.S. healthcare industry fraud costs amount to tens of billions of dollars each year, likely three to ten percent of total spend.[2] To protect themselves from financial losses, reputational damage, legal ramifications and financial penalties, organizations must implement robust fraud management strategies. This entails a comprehensive approach that encompasses prevention, detection and auditing mechanisms for both employees and third parties.

An effective fraud management program should include a variety of elements, including fraud risk governance policies, fraud risk assessments, preventive and detective internal controls, a counter-fraud analytic ecosystem, fraud awareness training, whistleblower hotlines, vigorous investigative practices, and effective compliance and auditing programs. The Association of Certified Fraud Examiners (ACFE) partnered with COSO to publish its 2023 Fraud Risk Management Guide.[3]

[1] "NHE Fact Sheet," CMS.gov, accessed September 8, 2023, https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/nhe-fact-sheet.

[2] "The Challenge of Health Care Fraud – NHCAA." n.d. National Health Care Anti-Fraud Association, accessed September 19, 2023, https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/.

[3] COSO and the ACFE Publish Fraud Risk Management Guide," afce.com, accessed September 19, 2023, https://www.acfe.com/fraud-resources/fraud-risk-tools---coso.

Employee fraud, insider threats and third-party fraud continue to cause significant problems in the healthcare industry. Common fraud types include billing for services never provided, upcoding and/or unbundling services, performing medically unnecessary services for the purpose of generating insurance payments, falsifying patient diagnoses and medical records, pharmaceutical fraud, and accepting kickbacks and/or bribes. In the post-pandemic environment, the continued proliferation of remote health care (i.e., increase in telehealth, telemedicine and telecare services) also leaves the healthcare industry exposed to additional fraud risks that must be proactively mitigated in order to prevent FWA. On June 28, 2023, the Department of Justice, along with state and federal law enforcement and the Department of Health and Human Services (HHS) Office of the Inspector General (OIG), announced a national health care fraud enforcement action, demonstrating the government's commitment to fight and prosecute health care fraud. This action resulted in criminal charges for 78 individuals for $2.5 billion in health care fraud.[4]

Prevention is the first line of defense against FWA. Organizations should foster a strong ethical culture that promotes transparency, integrity and accountability at all levels. Implementing a code of conduct and mandatory ethics training programs helps employees and third parties alike understand the organization's expectations and consequences of fraudulent activities. Additionally, implementing effective preventive internal controls, including segregation of duties and access controls, can significantly reduce opportunities for fraud to occur.

Detection mechanisms also play a crucial role in identifying potential FWA. The use of tools such as data analytics, automation and fraud detection software help organizations monitor and analyze copious amounts of data to identify patterns, anomalies and suspicious transactions. Regular internal and external audits also provide an independent assessment of the organization's financial records, operational processes and compliance with policies, procedures and regulatory requirements.

Key ways in which IA can contribute to the organization's fight against fraud include:

- Implementing continuous monitoring to quickly identify and detect potential red flags, outliers and program vulnerabilities with the utilization of advanced data analytics and automation.
- Leveraging data and open-source intelligence to create models that proactively assess and detect vulnerabilities.

[4] "National Enforcement Action Results in 78 Individuals Charged for $2.5B in Health Care Fraud," U.S. Department of Justice press release, accessed September 19, 2023, https://www.justice.gov/opa/pr/national-enforcement-action-results-78-individuals-charged-25b-health-care-fraud

- Performing regular risk assessments and implementing (and iterating as necessary) fraud prevention and detection policies and controls.
- Assessing the extent to which ethical standards, codes of conduct and values around FWA are formally documented, publicized and enforced.
- Assessing the extent to which mandatory trainings and ongoing education on relevant laws and regulations are provided effectively, as well as the sufficiency and effectiveness of processes to prevent, identify and/or report FWA.

Internal audit plays a pivotal role in assessing the efficacy of fraud prevention measures and identifying potential vulnerabilities. Its objective and independent perspective helps organizations strengthen their fraud management strategies and mitigate risks.

T13 Pharmacy Operations and Drug Distribution/Management

Noncompliant pharmacy practices can lead to millions of dollars in lost revenue, hefty fines and lost patient confidence due to reputational harm. Recent regulatory changes for drug waste billing, restrictions surrounding 340B contract pharmacies, and fines for noncompliance with the Controlled Substances Act have pharmacy, compliance and revenue-cycle leaders racing to implement system and process changes to keep up with data analytics, modifier application, inventory requirements and compliance.

Key areas on which internal audit should focus include:

- JW/JZ Modifier usage — Effective January 1, 2023, CMS requires the use of the JW modifier to report all separately payable single-use drug waste. And as of July 1, 2023, CMS requires providers to use the JZ modifier on claims to certify that there has been no drug waste on single-dose containers or single-use packages. When the reimbursement of a single dose of some drugs can run more than $1 million, documenting wasted portions can enable providers to capture significant revenue.[5] When hospitals discard leftover drugs from single-use vials and do not report the waste, they lose revenue. EMR systems today have processes to auto calculate and apply the appropriate modifier; however, errors are common in the EMR configurations, which leads to incorrect calculations and failure to apply the appropriate modifiers. This often results in noncompliant billing and/or the potential for lost revenue, so procedures to review and confirm accuracy of these claims are still needed.

[5] "Providers Could Gain Revenue as CMS Drug Claim Rules Change to Require JW and JZ Modifiers," Protiviti, accessed September 19, 2023, https://blog.protiviti.com/2023/06/28/providers-could-gain-revenue-as-cms-drug-claim-rules-change-to-require-jw-and-jz-modifiers/

- 340B Drug Pricing Program compliance and optimization — Many health systems rely on the millions of dollars in savings from 340B drug discounts to offer additional programs needed in their communities. Significant scrutiny exists around the extent to which 340B savings are used in accordance with program expectations. The ability to respond to how benefits are realized should be included in audits by reviewing calculated savings and usage documents (sometimes documented in a community benefit program). Additionally, contract pharmacy restrictions from manufacturers have resulted in lower revenue compared with previous years, making it as important as ever to assess compliance and optimization of 340B drug accumulations through audits. Human Resources and Services Administration (HRSA) audits approximately 200 covered entities annually and commonly find errors related to registration, diversion and duplicate discounts. The most egregious penalties for violating the group purchasing organization (GPO) prohibition (i.e., inappropriately purchasing 340B drugs on GPOs) can result in removal from the 340B program and millions of dollars in lost savings.
- Drug Diversion and Opioid Prescribing — United States drug overdose deaths have started to flatten from 2022 to 2023, but they are still at an all-time high.[6] With enhancements in data analytic capabilities, most health systems have the information available to detect patterns and high-risk behaviors to help promptly identify whether diversion or inappropriate prescribing is occurring in their facilities. Audits should be performed to help ensure that all theft and significant loss of controlled substances are reported and controlled substances and other highly diverted drugs have proper inventory controls and accurate record keeping in place and are properly monitored.
- Audits should focus on:
  - Proper utilization of monitoring tools (beyond accuracy of documentation), including what constitutes an outlier, and responsibility for review and documentation.
  - Detailed investigation and reporting protocols for all staff, contracted workers, students and volunteers.
  - Program oversight and involvement of all key parties (e.g., pharmacy, compliance, anesthesia and human resources departments, at minimum).
  - Annual training for all individuals (e.g., employees, contractors, providers) who come in contact with providers and patients to help them identify impairment or diversion signs and teach them how to report it.

[6] "Products — Vital Statistics Rapid Release — Provisional Drug Overdose Death Counts," Centers for Disease Control and Prevention, accessed September 19, 2023, https://www.cdc.gov/nchs/nvss/vsrr/drug-overdose-data.htm.

T13 Physician Arrangements, Financial Relationships with Physician/Other Referral Sources, Associated Compliance Risks and Physician Owned Distributorships (PODs)

Provider compensation continues to remain an area of significant concern for health systems due to the federal government's increased regulatory efforts in preventing and prosecuting healthcare fraud through the Anti-Kickback Statute and Stark Law provisions. Internal audit should work closely with legal and compliance departments to understand their organization's position on arrangements using the new safe harbors and/or exceptions.

One of the main areas of focus for regulators is physician-owned distributorships (PODs) that derive revenue from selling, or arranging for the sale of, implantable medical devices. While not all PODs are inherently problematic, there are certain risks and ethical concerns associated with relationships with these entities. One of the primary concerns with PODs is the potential for conflicts of interest. Physicians may be motivated to use and promote the products of their PODs over other alternatives, even if their products are not the most appropriate or cost-effective for patients. This can compromise the quality of patient care and raise ethical questions about whether decisions are truly made in the best interest of the patient. An additional concern associated with PODs is the increased risk of improper arrangements or kickback schemes which could lead to legal repercussions for hospitals, physicians and PODs.

Key procedures internal audit should perform include:

- Assessing controls designed to identify and prevent improper provider arrangements, including processes such as independent fair-market valuations and extended contract approval and contracting checklists. Also, the routine review of existing contracts and arrangements can help validate the overall effectiveness of those controls.
- Reviewing controls to identify and prevent improper provider compensation, such as clearly defined metrics, traceable funds and appropriate documentation for payments to providers.
- Assessing adherence to internal processes for determining whether a provider's approved total compensation is within established guidelines and fair market value (FMV).

- Analyzing the Open Payments database to identify payments which may have been unreported on conflict of interest (COI) disclosure forms.
- Validating processes used to verify and document the business need for all payments (internal and external).
- Determining whether appropriate approvals were received from all required individuals and committees while building out the conflict management remediation plans.

THEME 5 — REVENUE INTEGRITY AND MARGIN IMPROVEMENT

T09 Revenue Cycle Compliance

Compliant clinical documentation to support medical necessity, medical diagnosis and procedure code assignment, and claims management processing are critical attributes of the revenue cycle that serve as a hospital’s first line of defense against issues related to compliance and financial risk. It is essential to assess compliance with clinical documentation, coding and billing requirements to not only ensure accurate revenue but also to avoid revenue loss due to recoupments, refunds and fines.

Key activities that should be considered when reviewing these areas include:

- Auditing claims for documentation integrity of items/services billed and proper coding, including use of modifiers and diagnoses to improve accuracy and specificity.
- Assessing adherence to recent and evolving transparency regulations such as the No Surprises Act balance billing prohibitions and good faith estimate requirements, and the Hospital Price Transparency Rule.
- Assessing the patient access department’s ability to identify and communicate cost-sharing obligations without impeding access to care.
- Assessing compliance with federal and state billing requirements such as combining items/services into a single claim based on timing and locations of services provided.
- Assessing the charge description master (CDM) for complete and accurate charge-level detail by comparing to available reference pricing and published pricing from peers.

T11 Charge Capture Accuracy, Completeness, Timeliness and Reconciliation

Hospitals can identify opportunities to improve their revenue cycle and generate a demonstrable return by emphasizing compliance and accuracy in the identification, capture, reporting and reconciliation of chargeable items and services. Without standard and reliable processes, poor charge entry and missed charges can affect healthcare organizations significantly. Charge capture errors can represent millions of dollars to a provider organization, and overcharging is equally, if not more, detrimental than undercharging. To help mitigate risks associated with the various charge capture processes, routine audits should be performed to assess the effectiveness and adequacy of key controls.

Although charge capture and reconciliation efforts should reflect a more comprehensive approach, healthcare providers may choose to conduct focused audits on specific departments and/or service lines that typically have the most risk for charge capture noncompliance. These may include areas that are often dependent upon manual interpretation and charge entry, which pose an increased risk for human error. Manual intervention is inherent to services that are soft coded (i.e., manually assigned) by coding or clerical staff referencing clinical documentation and/or department charge sheets. The departments/service lines to consider including in scope (those that typically provide the best return on investment and/or opportunities for improvement) are operating rooms, interventional cardiology and radiology, pain management, outpatient provider clinics and emergency services.

Providers should ensure there are audit procedures in place to review areas where charge-interfacing errors may occur. Internal audit can help support and lead charge capture audits using data analytics to identify charge entry delays and potential charge discrepancies or exceptions, such as:

- Missing high-dollar surgical supplies and implants
- Missing or invalid fluoroscopy or medications utilized in pain management procedures
- Inconsistencies between facility and professional procedural coding
- Incorrect emergency department visit level assignment.
- Missing or invalid bedside procedures, as well as delays with charge entry.

Leveraging analytics allows internal audit to determine which departments and/or facilities to include in scope and helps determine a targeted sample to test. Testing evaluates supporting clinical documentation to determine if charges are captured inaccurately or untimely. The scope of a charge capture audit should be adapted to key stakeholder needs and targeted around existing or emerging governmental or industry risks and suspected operational gaps that can lead to lost revenue.

Inaccurate and untimely charge entry can lead to potential financial and compliance risks that jeopardize a hospital's finances and reputation. Implementing policy, governance, and comprehensive revenue reconciliation and monitoring processes will help ensure compliance, reduce rework and ultimately improve net revenue.

THEME 6 — TECHNOLOGY MODERNIZATION AND LEVERAGING DATA

T07 EHR/ERP/Other System Implementation, Conversion and Upgrade Practices

Healthcare providers recognize the benefits of new systems, which can streamline operations, improve efficiency, enhance patient care, and/or enable alternative delivery methods and mechanisms. New electronic health record (EHR) systems, ERP systems and other systems significantly benefit and impact core operations, processes and related controls. The adoption rate for new cloud-based technologies continues to increase throughout the industry, which represents additional challenges over on-premise systems. As such, internal audit functions not only should embrace new and evolving technologies, but also should adequately plan and prepare for their adoption.

The two key areas for internal audit to evaluate and optimize related to system initiatives are business process controls and application security controls. At a high level, business process controls consist of detective/monitoring controls, mitigating manual controls, enhancing configurable control components, and data validation and governance controls. A few important audit considerations include:

- Deciding how to optimize and secure the enhanced workflow capabilities of these new systems.
- Determining the configurable components of workflows, such as triggering events, sequence, validation rules, tolerance settings and approval levels.

- Evaluating controls across systems holistically and from an end-to-end process perspective.
- Identifying necessary detective controls and applicable alerting functions.

Obviously, employees can do more because of the enhanced features of these new systems. More functions can be performed, more transactions can be processed, and more data is available and potentially accessible. But while these enhanced features contribute to optimizing operations and processes, the application capabilities must be properly secured from an architecture, sensitive access, segregation of duties, privacy and provisioning perspective. Key audit items to consider and evaluate typically include:

- Addressing the inherent security concerns with the out-of-the-box security roles that come standard with most systems.
- Getting a comprehensive understanding of the security architecture of new systems, which are often extraordinarily complex.
- Evaluating out-of-the-box administrator roles that can provide access to business transactions.
- Understanding that cloud-based systems are blurring the lines between business and IT, and it is common for business personnel to have configuration access.

There are many audit considerations related to new and evolving IT systems. Well-executed audits of new systems provide the opportunity for internal audit to provide value and help confirm that the systems are sound and secure and that controls are optimized.

T13 Data Governance, Data Analytics, Business Intelligence and Other Data Monitoring/Reporting

The overall payment model change in healthcare reimbursement and the continued shift to value-based care, as well as increasing regulatory scrutiny and transparency requirements, continue to increase the importance of effectively managing organizational data throughout its lifecycle. In addition, the rise of data commercialization, interoperability, and the continued evolution of emerging technologies (e.g., artificial intelligence) have made it crucial for organizations to continuously enhance their data strategies.

Strategies are being revised to consider how to use data more effectively to improve patient care, member and provider engagement, population health management and decision making. As these strategies are being rolled out, they should include initiatives to drive data integrity and data-usage guidelines. Population health initiatives, including advanced practices that use artificial intelligence and machine learning to drive preemptive intervention, remain heavily reliant upon a data-rich environment frequently plagued with issues. Furthermore, while new opportunities have materialized for organizations to commercialize their data through sales, licensing, partnerships and/or entirely new data-driven products or services, a new set of risks related to data privacy, consent and security have also emerged.

Effective data lifecycle management strategies and supporting foundational data governance practices are significantly lacking across much of the industry, resulting in disjointed efforts to aggregate, maintain and ensure the integrity of data, the inability to effectively use data to drive insights, and a perceived lack of value in the data itself.

Key areas on which internal audit should focus include:

- Data governance — Reviewing data quality, data lineage, sourcing, security, utilization, transformation and other aspects of managing data as an asset.
- Continuous monitoring — Implementing monitoring capabilities that leverage near real-time data insights to drive audit focus (e.g., revenue adjustment codes that exceed one standard deviation in one month over a 12-month average).
- Technology and/or cloud strategy and architecture — Assessing current data and analytics strategy/capabilities against organizational goals and any corresponding roadmaps to ensure alignment.
- Data commercialization — Evaluating existence of, and compliance with, policies related to data access, data identification, standardized consent and other applicable legal and regulatory requirements.
- Audit analytics — Identifying ways that internal audit can leverage analytics in the planning, delivery and monitoring of all audits to expand the breadth and depth of its capabilities.

THEME 7 — THIRD-PARTY RISK, SUPPLY CHAIN AND CONTINUITY OF OPERATIONS

T07 Third-Party and Outsourced Services

Healthcare providers partner with third parties, including through the formation of joint ventures, to outsource services, drive service excellence, increase efficiency, control costs and gain other competitive advantages. With increasingly complex third-party ecosystems, rising customer demands, disruptions in the supply chain, a rapidly changing regulatory environment and ever-looming cybersecurity threats, there is tremendous pressure on organizations to ensure their vendors maintain consistent compliance with internal policies and evolving regulations. While many processes can be outsourced, it is rare that all associated risks can be shifted to the outsource partner.

Vendor risk management (VRM) is the practice of evaluating third parties before a business relationship is established, monitoring vendors over the duration of a contract, and ensuring appropriate protections are in place upon contract termination. Over the last decade plus, VRM has advanced from an annual-checklist exercise to a critical routine function. The circumstances or nature of any of the relationships may change at any point, or vendors may have a change in business operations, so detecting and managing these changes are critical to an organizations' success. In fact, many organizations report that they have recently experienced a third-party security incident and/or data breach.

In general, healthcare executives recognize the importance of third-party risk management; however, few organizations can credibly say they are doing it effectively. Often, vendor risk management functions do not have a defined owner and/or may be focused on one specific risk type, be that cybersecurity, contractual or regulatory risks. Most organizations have not established a comprehensive VRM function aligned with overall Enterprise Risk Management (ERM) identified risks and goals. Shared Assessments' Vendor Risk Management Maturity Model (VRMMM)[7] provides a framework for holistically identifying, assessing and managing an organization's vendor-related risks throughout the vendor lifecycle. The framework consists of the following eight program categories: (1) program governance, (2) policies, standards and procedures, (3) contracts, (4) vendor risk identification and analysis, (5) skills and expertise, (6) communication and information sharing, (7) tools, measurements and analysis, and (8) monitoring and review. This publicly available framework provides organizations with the ability to determine their current maturity and benchmark against others within the industry.

Healthcare organizations are increasingly using the internal audit function as a resource to assist with third-party vendor risk management. Internal audit is often tasked with evaluating the program that management has developed and implemented and with providing value-added feedback.

Key procedures for internal audit to perform when conducting VRM assessments include:

- Determining whether there is a well-defined vendor governance framework.
- Reviewing appropriate governance documents.
- Confirming whether there are established contractual standards, including any that a provider might be responsible for in a joint venture relationship.
- Assisting with periodic due diligence and continued oversight.
- Understanding if there are established, robust vendor inventory and performance monitoring processes.
- Developing an internal vendor-risk assessment or scoring process.
- Determining whether there are effective termination and offboarding processes.
- Evaluating the VRM lifecycle to determine how effectively the organization uses ongoing assessments and performance monitoring mechanisms (e.g., scorecards, questionnaires, standards for service-level agreements (SLAs), automation) to manage their overall portfolio of vendor risk.

Also, internal audit should assess compliance with business associate agreements (BAAs), evaluate changes to third-party relationships since the execution of the original agreement that involve the exchange of patient information, and review business associates' controls (where feasible).

[7] "VRMMM — Shared Assessments — Third Party Risk Management," n.d. Shared Assessments, accessed August 15, 2023, https://sharedassessments.org/vrmmm/.

T11 Supply Chain

Internal audit departments should continue to perform supply chain audits to ensure that their organization's supply chain facilitates the quality, safety, continuity and lowest possible cost of patient care. As capital equipment, supplies and purchased services are some of the largest costs for healthcare systems, IA teams need to evaluate the resilience and visibility of all processes and policies in each supply chain department.

Resilience has been top of mind for supply chain leaders over the last three years and should now be integrated into every aspect of supply chain decisions and developments. To help ensure that the correct product gets to the correct patient at the correct time, IA teams should be prepared to audit vendor management, procure-to-pay, inventory and statutory requirement aspects of the entire supply chain for all critical items.

While visibility into the various supply chain processes, policies and data is an integral part of a resilient supply chain, the IA team will need to develop a way to derive meaningful insights from multiple disparate internal and external systems. Fragmented architecture will add cost to each supply chain transaction and will necessitate techniques to map the entire process flow from clinical vendor and item selection through item requisition and into the chargemaster and accounts receivable functions. It is imperative that IA teams seek out the areas in which there are opportunities to manage costs or mitigate financial leakage through advanced spend and transaction management analysis. Some areas ripe for review include supplier and contract lifecycle management, item master/chargemaster reconciliations and other assessments tracking the lifecycle of a specific product request all the way through to its financial revenue capture.

Partnerships are key to driving the above-mentioned goals of resilience and visibility. Most health systems' biggest partnership is with their group purchasing organizations (GPOs). Most of these partnerships have built-in audit mechanisms, but IA teams should be prepared to investigate all aspects of the relationship, including contract utilization, cost tracking and any other ancillary services offered to ensure the organization is making the most out of the relationship.

T13 Business Continuity, Emergency Management and Pandemic Preparedness/Response

An effective business continuity management (BCM) program should be in place at all organizations. Organizations should first determine if a business impact analysis (BIA) has been performed. A BIA is the foundational effort that allows for the determination of recovery requirements for any aspect of an organization that may suffer an unplanned disruption to normal business operations. It explores multiple impacts, including financial, operational, legal and regulatory/compliance. Based on the potential impacts uncovered, subsequent recovery strategies and corresponding plans should then be developed. The key output of a BIA is the determination of recovery time objectives (RTOs) and recovery point objectives (RPOs).

After understanding the BIA, internal audit should confirm that recovery strategies (e.g., work from home, transferring workload from a disrupted workplace to an alternate team or location, planned deferral of specific processes or tasks) have been validated. Strategies and plans should consider the three core BCM interrelated disciplines: crisis management and communications, business resumption, and IT disaster recovery (ITDR). Walkthroughs of recovery plans and procedures for each of these disciplines should verify relevant team members are able to respond to an event and recover respective processes and operations within the established recovery objectives. Additionally, key personnel should be identified in each plan to allow for effective communication, clear designation of roles and responsibilities, and coordination protocols between functions and team members. Internal audit also should verify that all strategies and plans are maintained and tested/validated regularly.

For healthcare provider organizations, it is critical to have a comprehensive emergency management program that is clinically focused. In this way, the emergency management and business continuity programs are complementary.

When auditing BCM and ITDR programs, IA should review and assess the following:

- Program management and governance: Policies, frameworks, standards, charters, roles, responsibilities, etc.
- Business impact analysis (BIA): Potential impacts of disruption, recovery time objectives, recovery point objectives, identification of dependencies, etc.
- Development of response and recovery artifacts: Business continuity plan(s), IT disaster recovery plan(s), crisis management plan(s), pandemic preparedness plan(s), and relevant intersections with the emergency operations (or management) programs.
- Testing strategies and plans: Exercises of teams, strategies, technology and plans.
- Training and awareness: Roles, responsibilities, documentation and procedures.

ADDITIONAL OBSERVATIONS

Areas that are not included in the 2023 audit plan but appear to be priorities for 2024 include:

- Employee, Provider and Vendor Verifications (Employee Eligibility, Background, Exclusion Checks, Licensing, Credentialing and Privileging)
- Environmental, Social and Governance (ESG) Reporting
- IT Asset Management (Laptops, Desktops, Servers and Mobile Devices)
- Billing Accuracy and Accounts Receivable (Collections, HOPD, Cash Application, Charity Care Determinations/Reporting and Bad Debt/Write-Offs)
- IT Disaster Recovery
- IT Governance (Oversight, Innovation and Spend)
- Medical Devices

Areas that are not on any audit plan due to lack of skills and competencies include:

- Digital/Innovation Initiatives
- Medical Management, Medical Necessity, Length of Stay Management, Observation/ Short Stays, and Related Compliance Risks (Documentation, Transfers, Discharges and 30-Day Readmissions)
- Changing Delivery Model Across the Care Continuum (Population Health, Aging Patient Population, Accountable Care Organizations (ACO) and Value-Based Contracting)
- Emerging Technologies (Automation, Artificial Intelligence and Predictive Analytics)
- Licensure, Accreditation, CMS Conditions of Participation, and State or County Surveys

Conclusion

As healthcare organizations shift to recovery mode and focus their attention on returning to business as usual and providing quality patient care following the end of the PHE, they face an increasingly broad risk landscape that includes cyber threats, talent shortages and workforce issues, business performance expectations, new and ongoing risk and compliance issues, and the need to modernize and optimize their technology structure. The findings from our latest Healthcare Internal Audit Plan Priorities Survey underscore the pivotal role that internal audit will play in helping organizations address these pressing concerns.

Internal audit functions must remain agile and forward-looking, embracing new technologies, methodologies and data analytics that will help them advance their efforts and provide innovative, proactive and strategic guidance to help their organizations address these issues successfully.

Now, more than ever, internal audit is a critical ally to healthcare leadership, providing fresh insights, data-driven recommendations and enhanced risk mitigation strategies throughout the organization. As leaders navigate the continuing complexities of the post-pandemic era, harnessing the power of internal audit remains pivotal for fostering adaptability, resilience and growth in the evolving healthcare landscape.

Appendix A: Provider-Specific Priorities and Other Observations

Top Provider Internal Audit Plan Priorities

	2023 Ranking	Yes, on 2023 audit plan
Cybersecurity Practices and Posture	1	72%
Employee Time/Expense Reporting and Payroll	2	70%
Fraud Management, Prevention, Detection and Auditing	T3	65%
User Access Management	T3	65%
Accounts Payable	5	56%
Human Resources, Benefits, Compensation and Workforce Challenges	6	54%
Revenue Cycle Compliance	T7	50%
Third-Party and Outsourced Services	T7	50%
Charge Capture Accuracy, Completeness, Timeliness and Reconciliation	T9	48%
EHR/ERP/Other System Implementation, Conversion and Upgrade Practices	T9	48%
Supply Chain	T9	48%

Other observations: Providers

Areas that are not included in the 2023 audit plan but appear to be priorities for providers for 2024 include:

- Data Governance, Data Analytics, Business Intelligence and Other Data Monitoring/Reporting
- Employee, Provider and Vendor Verifications (Employee Eligibility, Background, Exclusion Checks, Licensing, Credentialing and Privileging)
- Environmental, Social and Governance (ESG) Reporting
- IT Asset Management (Laptops, Desktops, Servers and Mobile Devices)
- Billing Accuracy and Accounts Receivable (Collections, HOPD, Cash Application, Charity Care Determinations/Reporting and Bad Debt/Write-Offs)
- IT Disaster Recovery
- IT Governance (Oversight, Innovation and Spend)
- Medical Devices

Areas that are not on any provider audit plans due to lack of skills and competencies include:

- Digital/Innovation Initiatives
- Medical Management, Medical Necessity, Length of Stay Management, Observation/ Short Stays and Related Compliance Risks (Documentation, Transfers, Discharges and 30-Day Readmissions)
- Changing Delivery Model Across the Care Continuum (Population Health, Aging Patient Population, Accountable Care Organizations (ACO) and Value- Based Contracting)
- Emerging Technologies (Automation, Artificial Intelligence and Predictive Analytics)
- Licensure, Accreditation, CMS Conditions of Participation, and State or County Surveys

Appendix B: Payer-Specific Priorities, Other Observations, and Key Risks to Consider

Top Payer Internal Audit Plan Priorities

	2023 Ranking	Yes, on 2023 audit plan
User Access Management	1	89%
Cybersecurity Practices and Posture	2	79%
Employee Time/Expense Reporting and Payroll	3	68%
Finance and Accounting	T4	63%
Fraud Management, Prevention, Detection and Auditing	T4	63%
Accounting, Finance, Integrity of Financial Data, Budgeting, Forecasting, Reserves, Treasury, Investments, Insurance, Grants and Bonds	T6	58%
Accounts Payable	T6	58%
Business Continuity, Emergency Management and Pandemic Preparedness/Response	T6	58%
Data Governance, Data Analytics, Business Intelligence and Other Data Monitoring/Reporting	T6	58%
Human Resources, Benefits, Compensation and Workforce Challenges	T6	58%

	2023 Ranking	Yes, on 2023 audit plan
Claims Processing	T6	58%
Members	T6	58%

Other observations: Payers

Areas that are not included in the 2023 audit plan but appear to be priorities for payers for 2024 include:

- Third-Party and Outsourced Services (Vendor Selection, Management and Contract Compliance [Payment Terms, SLAs and BAA Requirements])
- Emerging Technologies (Automation, Artificial Intelligence and Predictive Analytics)
- IT Governance (Oversight, Innovation and Spend)
- Temporary Staffing, Recruitment and Unions
- Employee, Provider and Vendor Verifications (Employee Eligibility, Background, Exclusion Checks, Licensing, Credentialing and Privileging)

Areas that are not on any payer audit plans due to lack of skills and competencies include:

- Changing Delivery Model Across the Care Continuum (Population Health, Aging Patient Population, Accountable Care Organizations (ACO) and Value-Based Contracting)
- Consumerism and Patient Experience
- Digital/Innovation Initiatives
- Licensure, Accreditation, CMS Conditions of Participation, and State or County Surveys
- Medical Management, Medical Necessity, Length of Stay Management, Observation/ Short Stays, and Related Compliance Risks (Documentation, Transfers, Discharges and 30-Day Readmissions)

Key Payer-Specific Risks to Consider

Similar to other types of healthcare organizations, internal audit functions across the payer landscape are grappling with the challenge of doing more with less while facing increasing risks that include regulatory pressures, margin compression, data governance, quality concerns, labor shortages, provider reimbursement model changes, payment integrity, member and provider satisfaction, and more. While the risks below did not make the top 10 list for payers and providers combined, here are some of the top payer-specific priorities and why they should be top of mind for payers and their audit teams.

01 Claims Configuration, Adjudication and Payment

Healthcare payers view claims processing as a top risk due to the criticality of accurate and timely claims payment and the minimization of overpayments and revenue leakage. Effective claims processing also helps prevent provider and member complaints by streamlining reimbursement processes. Further, robust claims processing contributes to compliance with regulations and conformance to industry standards, leading to increased quality in healthcare payer services and financial operations.

02 Member Experience

Star Rating changes introduced in the 2024 Final Rule, coupled with the increased popularity of submitting an online review, help drive member experience to the top of the list for health plans this year. In the current market, more members than ever are driving their purchasing decisions based on satisfaction scores. The enrollment, care coordination, customer service and appeals and grievances departments are the primary interfaces between the plan and its beneficiaries, making it critical for these business units to provide accurate and timely resolution of issues. Poor interactions lead to reputational damage, increased disenrollment and complaints, reduced Star Ratings, and scrutiny from CMS. Plans should be sure to incorporate these areas into their audit plans, especially appeals and grievances, as they continue to be a target for CMS audits.

03 Provider Services

Given the continued market consolidation and shifts in provider networks, the OIG has placed added oversight of providers as a priority for FY23. The OIG has prioritized patient access, patient safety and reducing critical incidents involving Medicaid beneficiaries, while increasing efforts to monitor fraud hotspots and reduce improper payments from public health plans. Payers should ensure that they have the mechanisms in place to provide regular monitoring of and oversight to their contracted providers. Failure to properly verify credentials, perform exclusions checks or regularly monitor provider performance can result in noncompliance with applicable laws and regulations, place the health plan at financial and reputational risk, and expose members to poor quality of care.

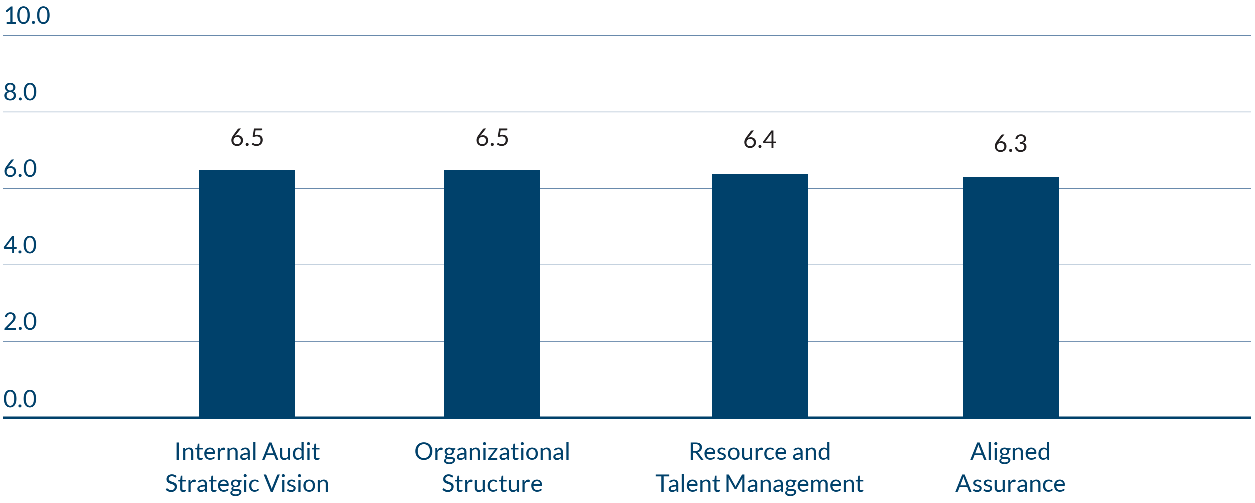
04 Compliance and Regulatory Scrutiny

Compliance and regulatory requirements are a top risk for healthcare payers due to the evolving regulatory landscape and increased scrutiny by regulators. Health plans should ensure that they have established a robust delegation oversight strategy for First-Tier, Downstream, and Related Entities (FDRs) and employ vigorous fraud, waste and abuse (FWA) strategies, including an effective special investigations unit (SIU), to remain compliant with regulatory requirements and help ensure readiness for state and federal audits like CMS program audits. Regulatory changes, including the unwinding of the COVID-19 PHE (e.g., Medicaid continuous coverage requirements), changes to risk adjustment methodologies, and enforcement of the No Surprises Act and price transparency requirements are impacting many plans' bottom lines and presenting additional compliance and reputational risks. Furthermore, regulatory enforcement continues on the data privacy front. As healthcare organizations expand and collect more information from patients and members and share that information with vendors and third parties, data privacy compliance will continue to be a key risk area. These data privacy concerns require ongoing monitoring to keep up with the ever-changing laws and regulations, as well as to understand how they apply to the current and planned future state of operations.

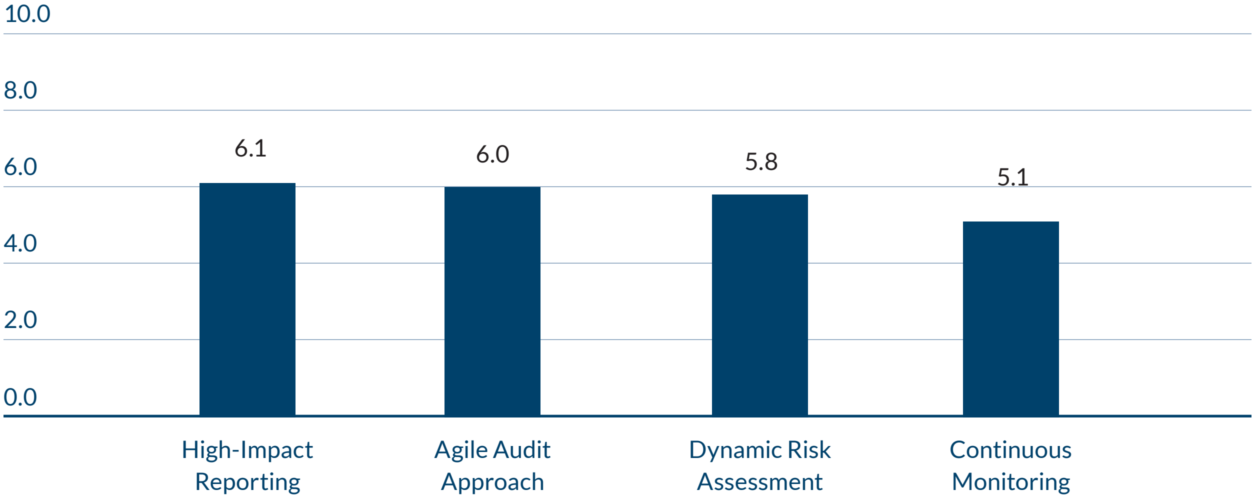
Appendix C: Additional Healthcare Survey Insights

Please rate the current level of maturity of each of the following components within your internal audit organization.
Respondents measured their maturity from 1 (low level of maturity) to 10 (high level of maturity). The scores shown are the average scores across all respondents.
(Base: All respondents)

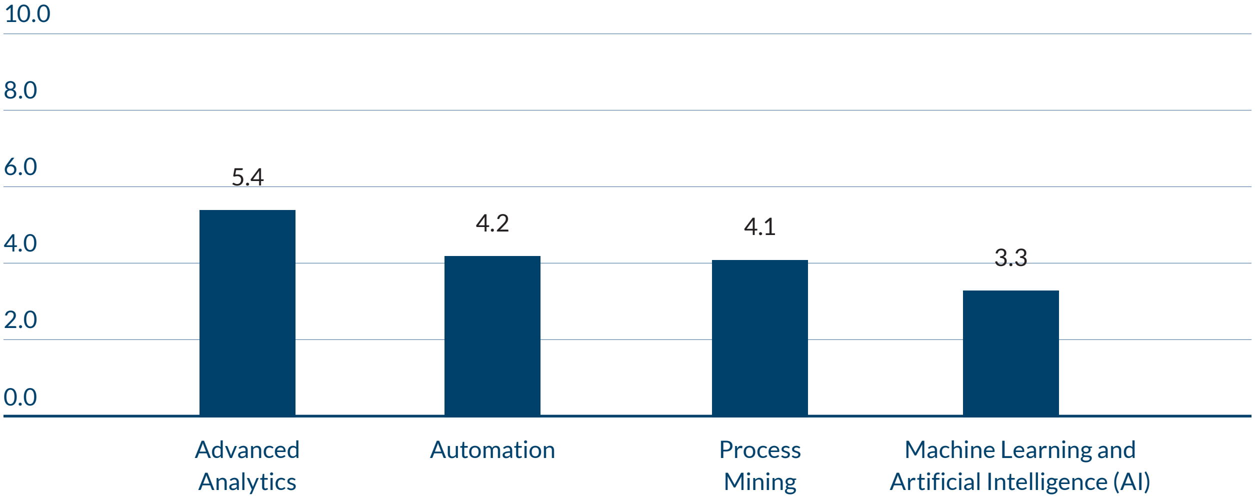
GOVERNANCE



METHODOLOGY

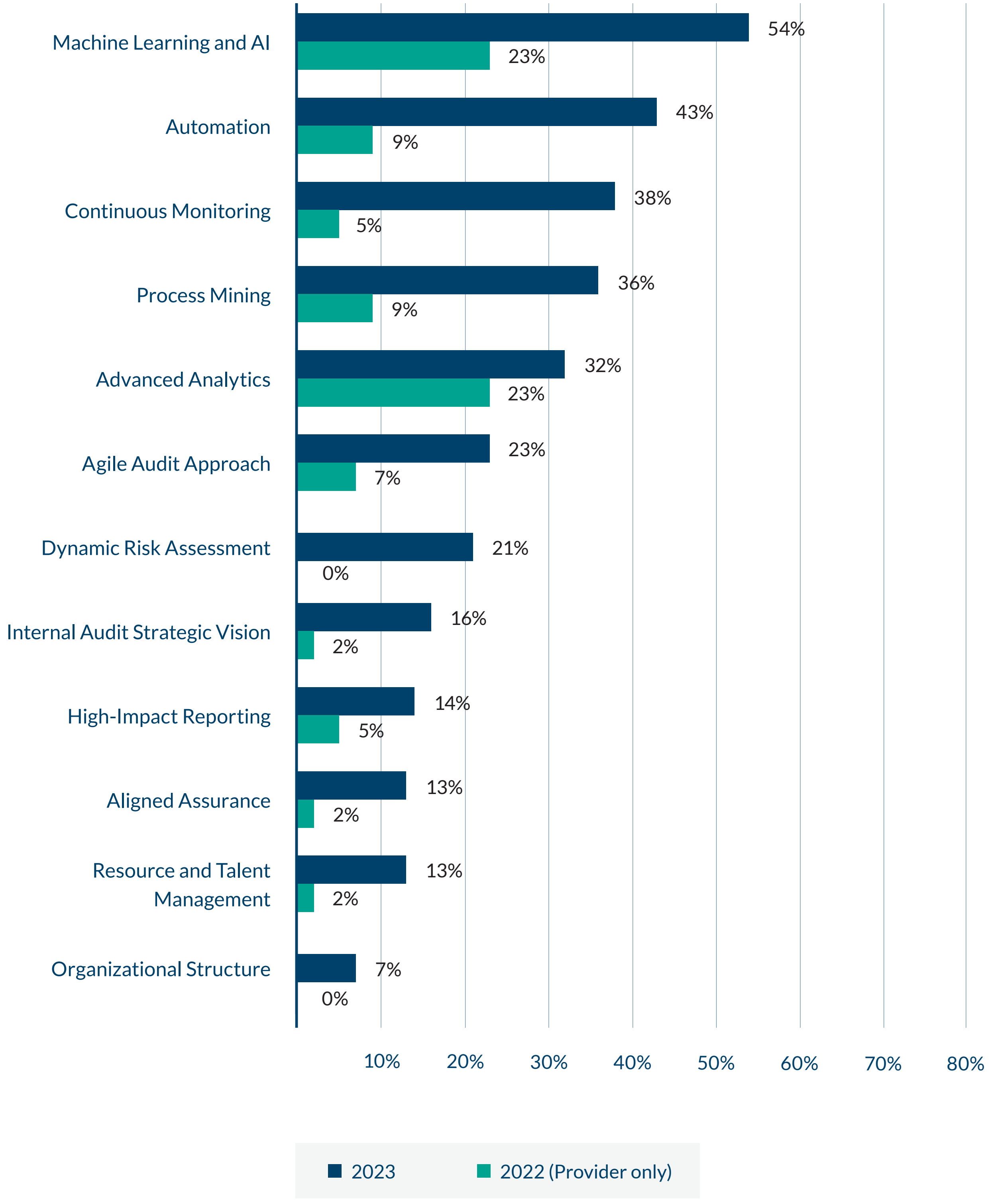


ENABLING TECHNOLOGY



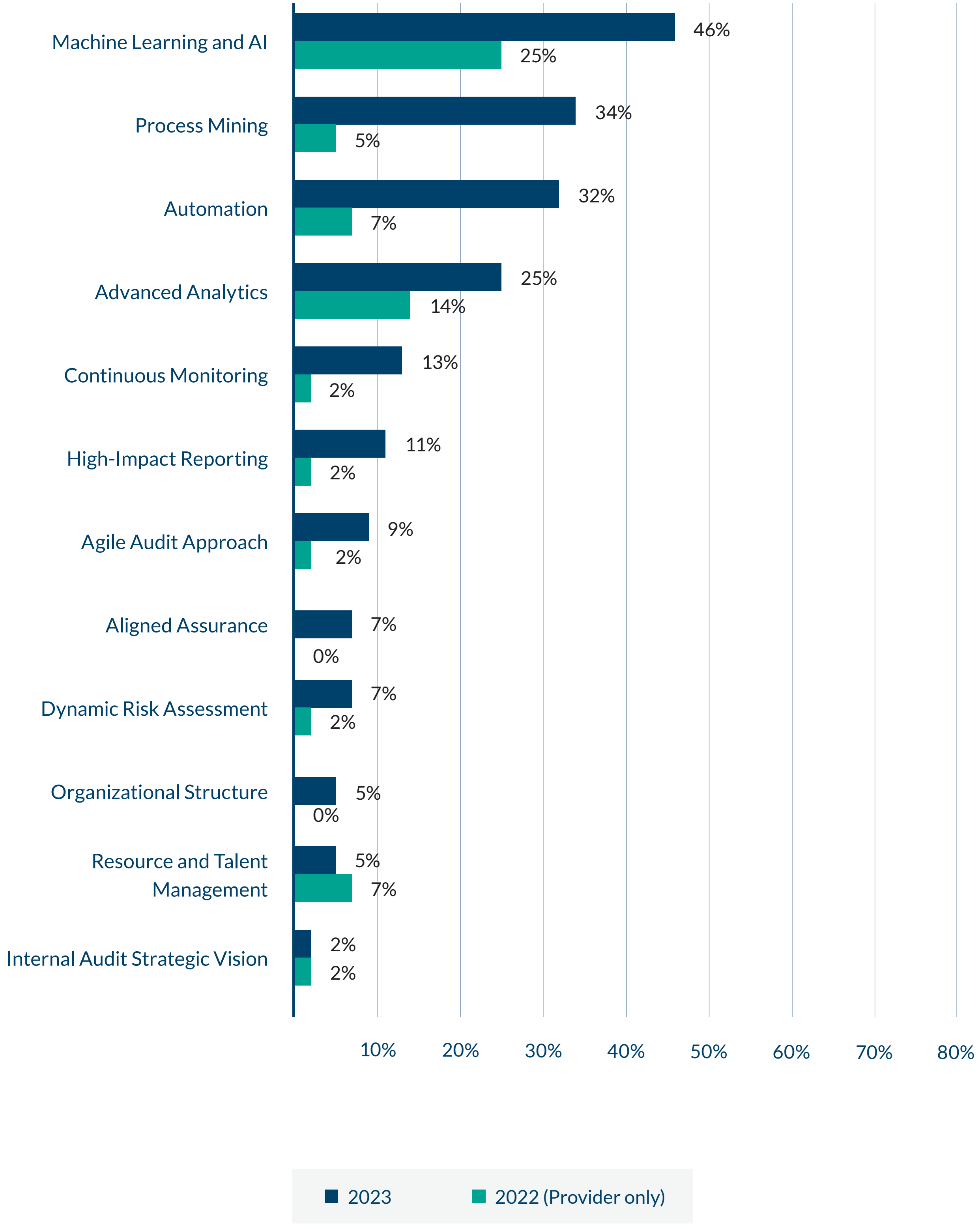
What next-generation areas, if any, are you interested in implementing but doubtful that you will be able to procure the resources to do so? (Multiple responses permitted)

(Base: All respondents)



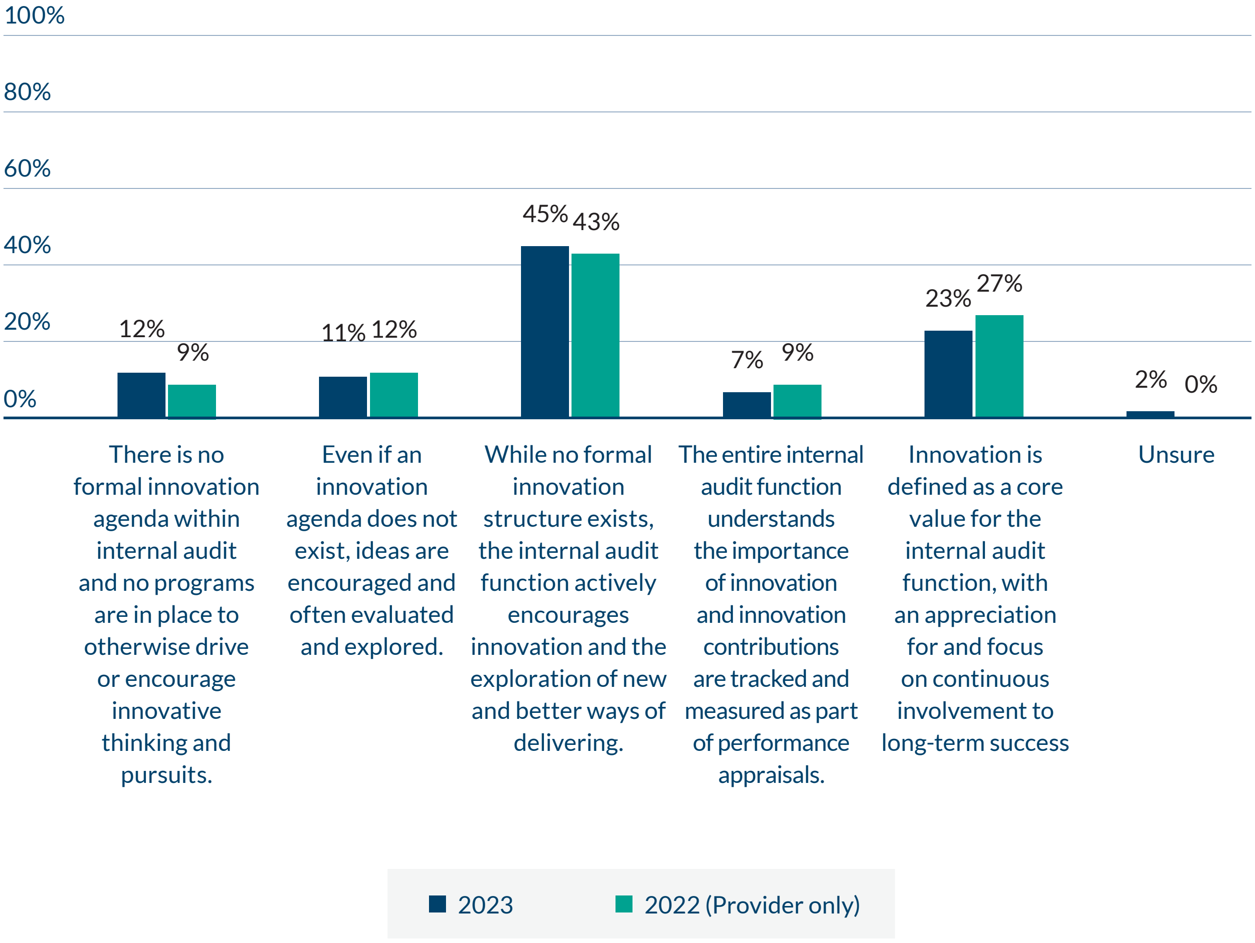
What next-gen areas, if any, are you interested in implementing but will require third-party skills / assistance to do so effectively? (Multiple responses permitted.)

(Base: All respondents)



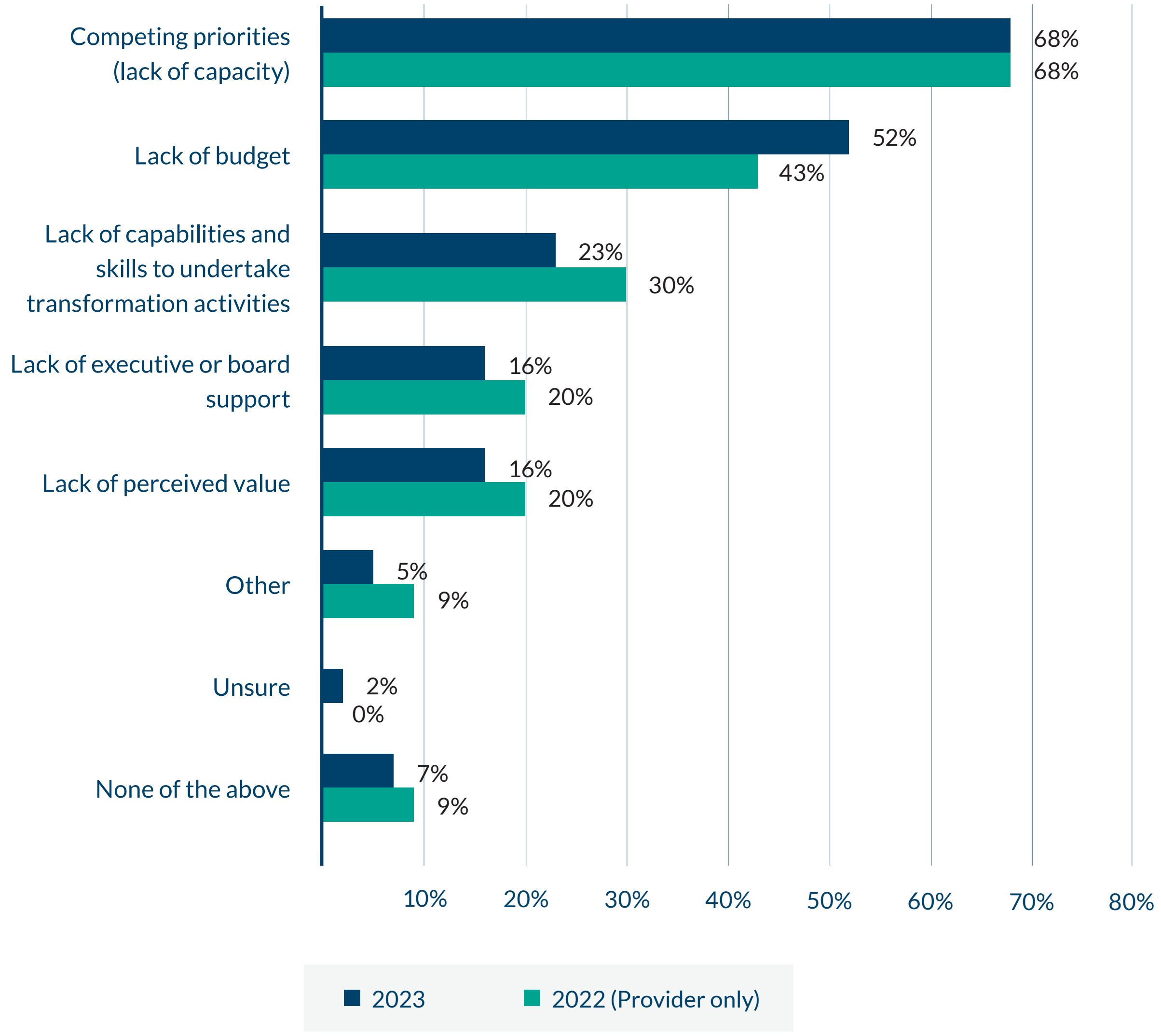
Which one of the following statements best defines the current maturity of your internal audit transformation or innovation activities?

(Base: All respondents)



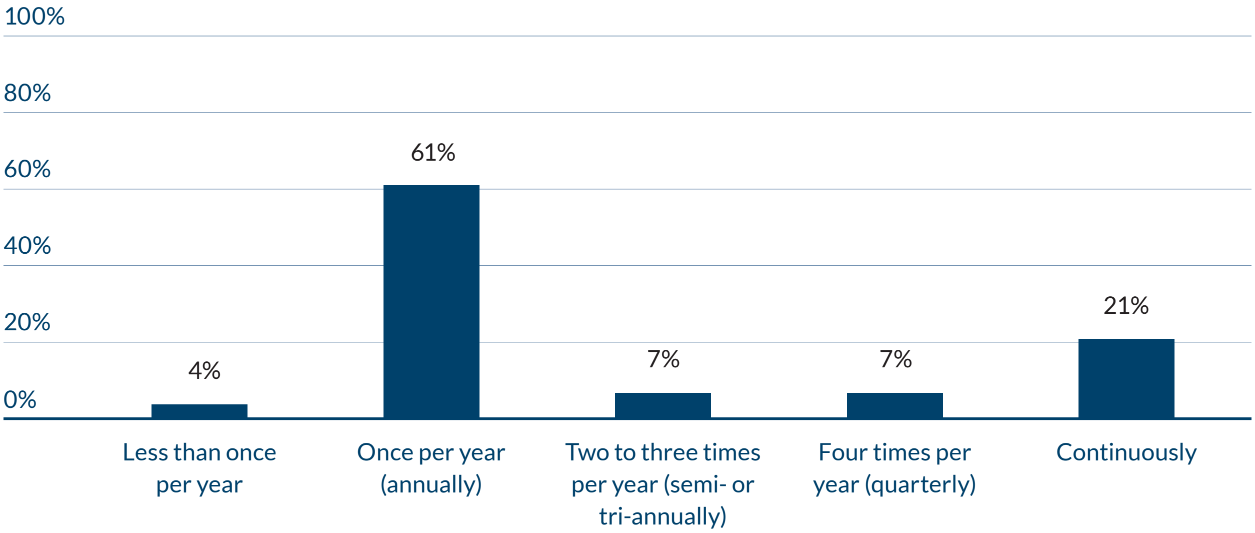
What are the barriers or inhibitors to increased focus on innovation/transformation? (Multiple responses permitted)

(Base: All respondents)



How often, if at all, is the risk assessment process performed and/or refreshed?

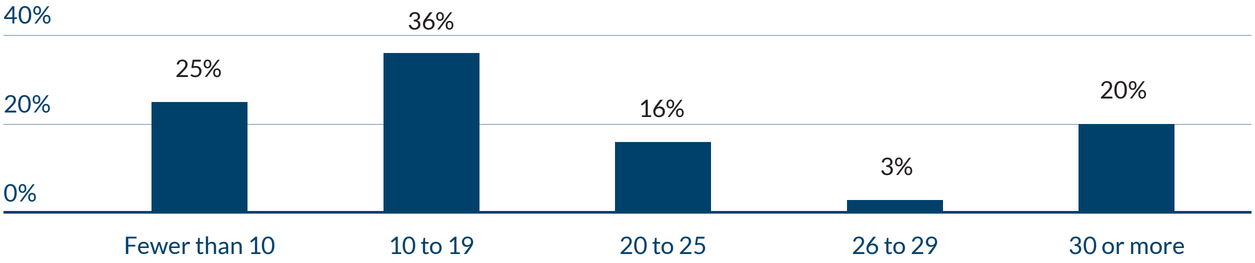
(Base: All respondents)



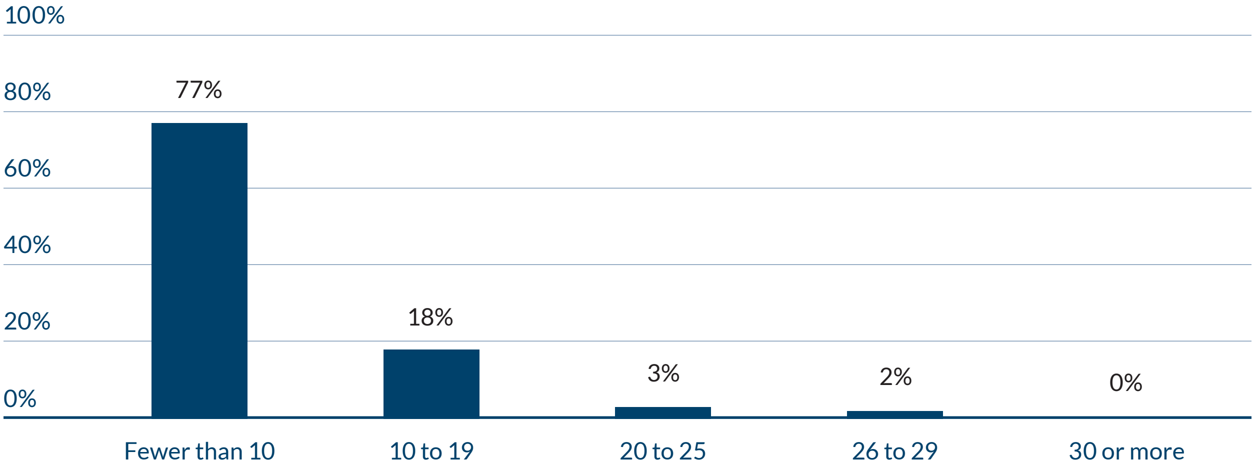
How many internal audits/projects are on the average annual audit plan for each of the following areas?

(Base: All respondents)

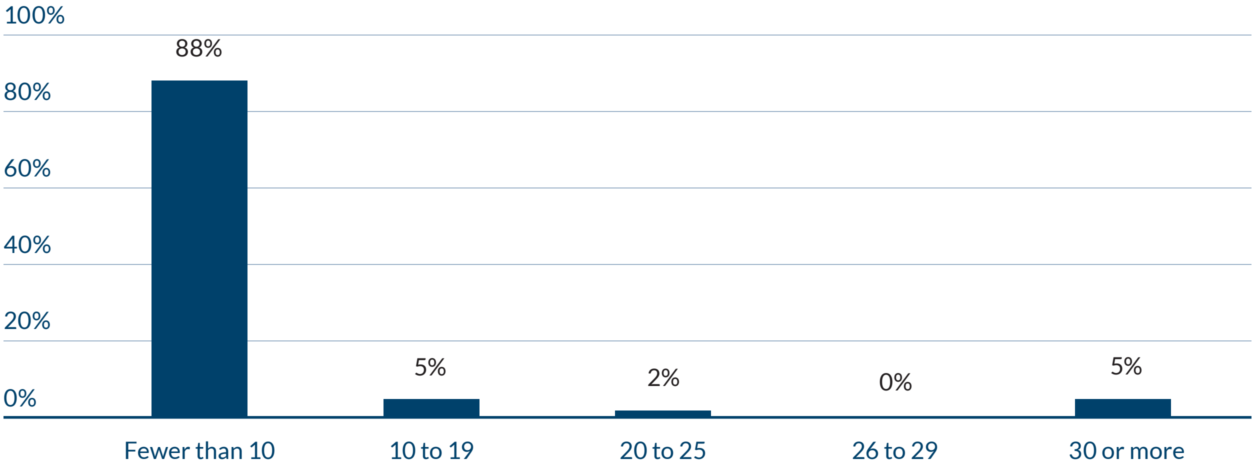
ASSURANCE (AUDIT)



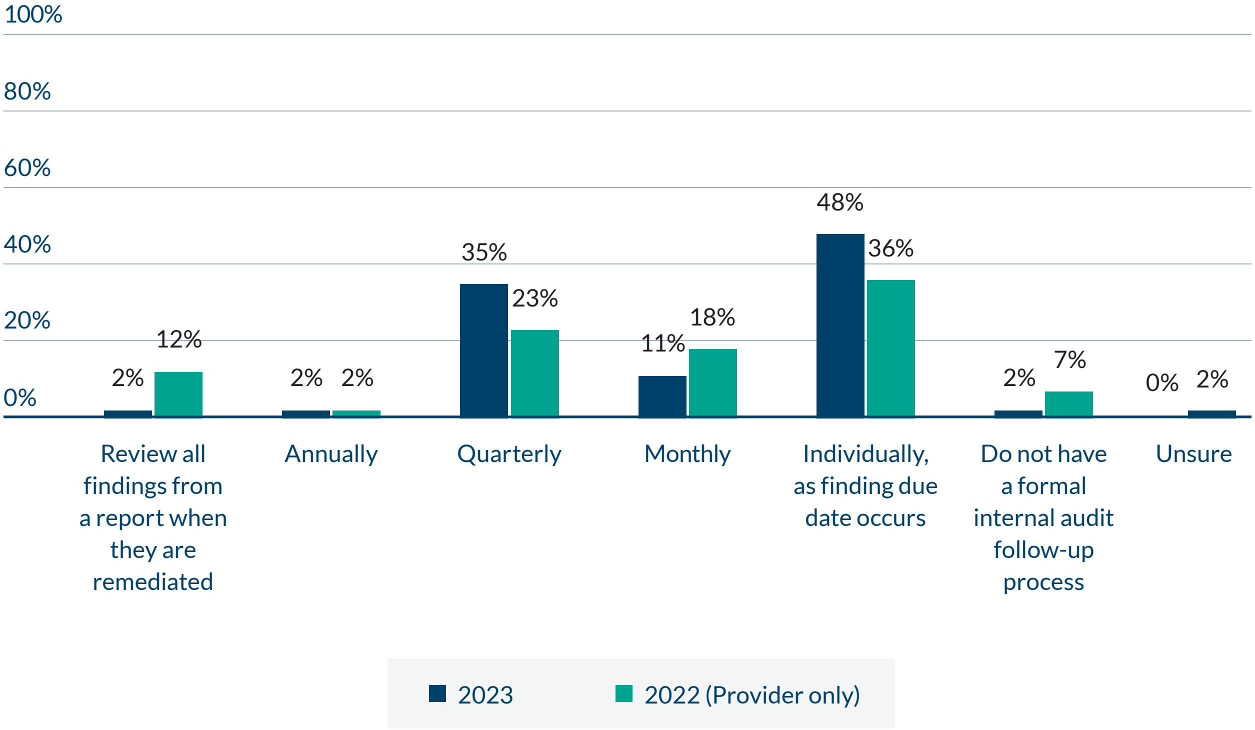
ADVISORY (CONSULTING)



OTHER

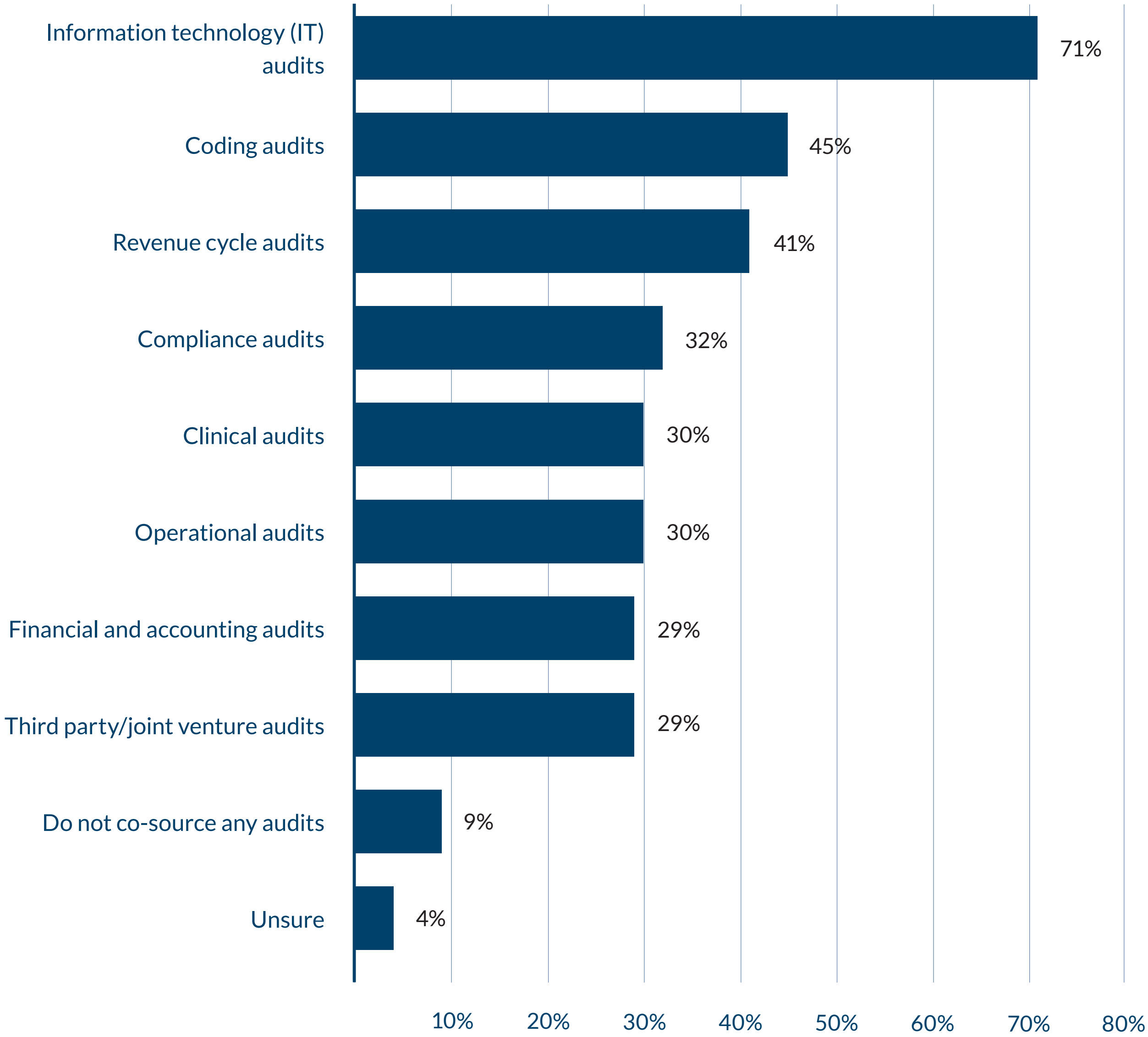


How often, if at all, do you follow up on outstanding internal audit findings?
(Base: All respondents)



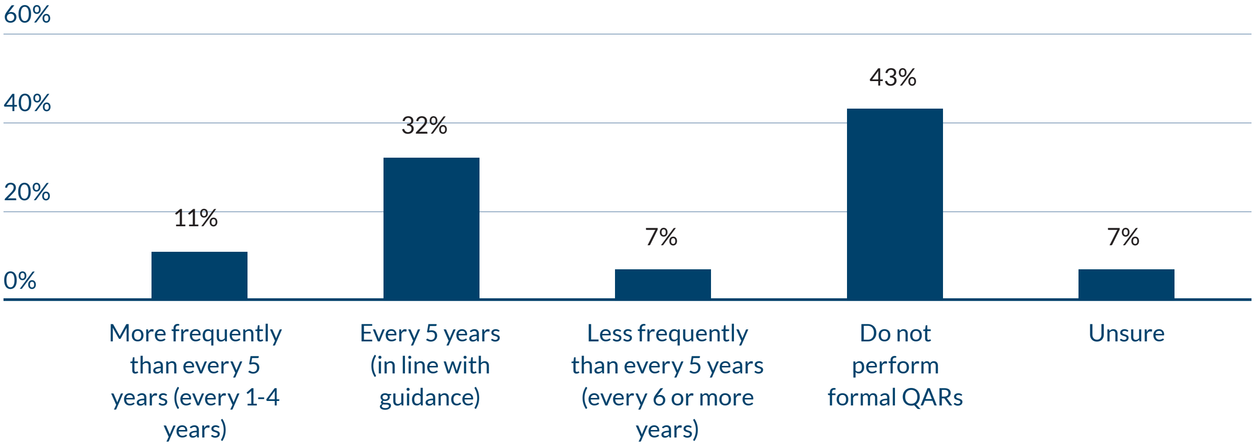
Which areas, if any, does your organization co-source with a strategic partner/third-party vendor to execute? (Multiple responses permitted.)

(Base: All respondents)



How often, if at all, do you conduct formal quality assurance reviews (QARs) (external or internal assessment with independent validation) for conformance to The IIA Standards?

(Base: All respondents)



About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 *Fortune* 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

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.

Contacts

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

Matt Jackson
Healthcare Internal Audit Leader
+1.214-284-3588
matthew.jackson@protiviti.com

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

SOUTH AFRICA *
Durban
Johannesburg

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 is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. PRO-0923