Tackling Traditional Audit Plan Concerns and Expanding Focus on Fraud, Third Parties and Data

Key Findings From the Latest Survey Conducted by Protiviti and AHIA on Healthcare Provider Organization Internal Audit Plan Priorities

ahia
Assoc. of Healthcare Internal Auditors

protiviti®
Global Business Consulting

Table of Contents

Executive Summary 01

Provider Internal Audit Plan Priorities and Other Key Takeaways 04

Conclusion 17

Appendix A: Internal Audit Functions and Moving Forward With the Next-Gen Journey 18

Appendix B: Additional Survey Insights 24

Appendix C: Payer Priorities, Other Key Takeaways and Other Payer Risks to Consider 39

Executive Summary

As the COVID-19 pandemic continues to wind down, many healthcare provider organizations are transitioning into a blocking-and-tackling mode, although it's far from business as usual. Relieved of the constant pivoting that the public health emergency (PHE) has demanded for more than two years, these organizations now seek to focus more attention on the "new basics" to deliver business results and plan for the future. Organizations also face the challenge of doing more with fewer resources while continuing to deliver on their mission to provide high-quality patient care — albeit in a changed world.

The new basics for healthcare provider organizations include addressing the residual impacts of the pandemic on core healthcare functions, including back-office operations like billing and accounts receivable management. We see many healthcare organizations prioritizing revenue integrity initiatives to reduce the risk of revenue leakage and focusing on improving revenue cycle processes. Many leading organizations are aiming to build on innovation and transformation initiatives executed out of necessity during the pandemic, including finance, human resources and supply chain processes, to continue to increase resiliency and efficiency and create competitive advantage.

Another new basic in healthcare is taking fraud management activities to a new level. Fraud management tops the list of internal audit priorities in this year's Healthcare Internal Audit Plan Priorities Survey, a reflection of the pressure that healthcare organizations are under to become adept at identifying and defending against rampant fraud. To understand how concerned healthcare organizations are about this issue, consider that in last year's survey, fraud management ranked 11th on healthcare providers' list of top priorities. Fraud management also holds the second spot on the list of internal audit priorities for healthcare payers (see page 39), but in our 2021 survey, it didn't even make the list of top risks for this group.

The pandemic has helped to fuel healthcare fraud exponentially, which is now impacting all aspects of the healthcare system. Telehealth scams and fraudsters recruiting help from "good actor" physicians to carry out their scams are only two examples of common fraud risks in today's environment. (As noted later in this survey report, combating modern fraud scenarios like these demands both vigilance and agility, as well as the application of next-generation internal audit capabilities.)

New basics include addressing other "old" challenges exacerbated by the pandemic

Healthcare provider organizations' focus on the new basics includes making new attempts to find solutions for challenges that are disrupting operations — and eroding the bottom line — well before the pandemic. Some of these issues have worsened since and, in many cases, because of the PHE. These challenges include rising regulatory pressures, the fight against opioid and substance use disorders, and significant labor shortages amid fierce competition for skilled talent.

The shortage of talent in healthcare is not just affecting the front line. Healthcare organizations, like many other businesses, are struggling to hire and retain talented workers in all areas, including accounting, finance and information technology functions. Also, like employers in all industries, healthcare organizations are trying to adjust to employees' expectations about the "where" of work, with an increasing number of staff showing less willingness to work in a "pre-pandemic" environment and expressing instead a strong preference for more flexible work models.

Rising employee turnover, transfers and the use of nonemployees to help fill in gaps, the expansion of hybrid and remote work, rapid digitization during the pandemic, and the growing use of specialized applications, including web-based apps, have all conspired to make user access management one of the top three priorities in this survey. Healthcare provider organizations are grappling with a high volume of user access changes that are overloading identity and access management (IAM) teams and creating security gaps and compliance risks.

For internal audit teams in healthcare, a clear need to accelerate next-gen capabilities

Many internal audit functions in the healthcare industry are at risk of not being able to help adequately support efforts to address pandemic-induced and long-standing issues while also pursuing new opportunities and charting a path for growth in a post-pandemic environment. The lack of advanced technological capabilities in internal audit is a key factor.

Findings from this year's survey show that only 27% of internal audit functions in healthcare have already implemented or are optimizing advanced analytics — although another 21% report they're currently implementing this capability. When surveyed about automation efforts, 10% of respondents have implemented or are optimizing automation, while 9% are in the process of doing so.

5% of the functions we surveyed reported that they're implementing artificial intelligence (AI) and machine learning (ML) capabilities. And while many respondents are interested in bringing advanced analytics (23%) or ML/AI capabilities into the function, many are doubtful they can procure the resources to do so. (See charts starting on page 24 for additional insights.)

Competing priorities and budget constraints stand in the way of many internal audit organizations increasing their focus on innovation and transformation efforts. More than half (59%) of respondents reported that their function has either not completed or is not currently undertaking any transformation or innovation initiatives. A silver lining, though, is that a significant percentage of respondents (43%) said that while no formal innovation structure exists in their function, the internal audit function actively encourages innovation and the exploration of new and better ways of delivering.

As we move on to explore the full results from our 2022 survey and provide our recommendations to internal audit functions based on their stated priorities, we provide an assessment similar to what we offered in last year's survey: Internal audit functions need more support to transform their organization and help it meet current challenges while preparing for what comes next. And now, a year later, the need to accelerate change and advance capabilities has become only more urgent.

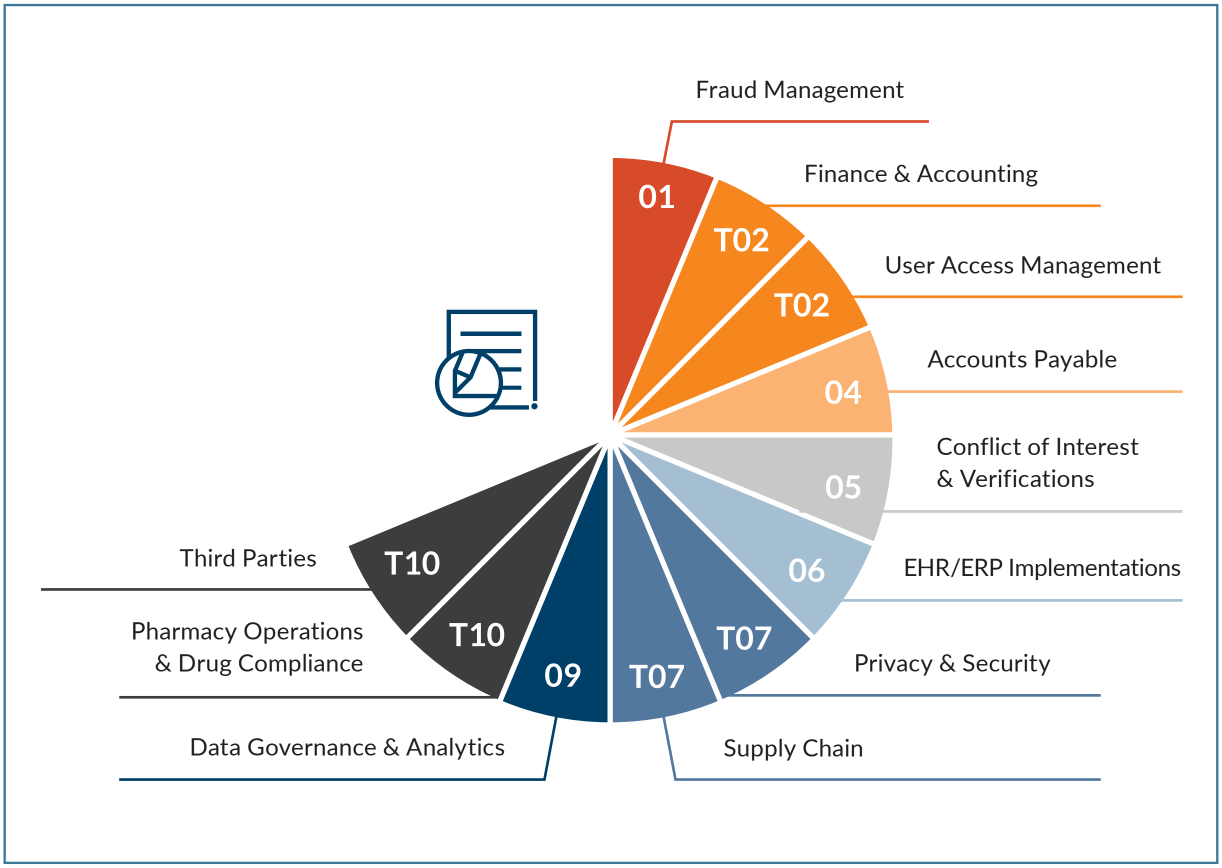
The Association of Healthcare Internal Auditors (AHIA) and Protiviti will be summarizing further themes and results from the healthcare internal audit plan priorities survey in AHIA's *New Perspectives* publications, the digital journal of AHIA. This will include providing additional insights on audit practices, staffing, resource allocation, top fraud concerns, ERM, internal controls over financial reporting and the adoption of next-gen concepts. The *New Perspectives* articles, coupled with this healthcare provider organization internal audit plan priorities publication, will serve as key resources for healthcare internal audit practitioners to benchmark their internal audit programs to industry leading and contemporary healthcare internal audit metrics and performance attributes.

> “Internal audit functions, because of their broad and objective view of the business, are uniquely suited to help healthcare organizations identify and manage critical risks and uncover new opportunities in the post-pandemic business environment. But to do that, they must resist the urge to develop audit plans that conform only to their current bench strength. To address all areas that executive management and the board highlight as requiring internal audit’s attention, many functions will need to extend their capabilities by expanding their tool sets and leveraging more highly skilled human resources. These investments are well worth it, as they will lead to a more future-fit internal audit organization — and a more resilient business overall.”

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

Provider Internal Audit Plan Priorities and Other Key Takeaways

Top provider priorities for 2022



Note: "T" indicates a tie.

01 Fraud Management

The PHE exacerbated healthcare-related fraud by giving bad actors more opportunities to take advantage of the entire healthcare system, from commercial payers, providers and patients to government entities. Fraudsters' approaches have also grown more brazen and sophisticated, and healthcare organizations must be agile enough to manage the newest schemes. They must also try to identify the latest fraud scenarios preemptively.

The rapid use of telehealth during the PHE revived old issues and concerns while introducing new fraud schemes. Therefore, implementing innovative methodologies for managing fraud risks is paramount for healthcare organizations. So, too, is validating business and compliance plans to identify, assess and help close control gaps and prevent risks from evolving into more serious issues.

Many modern fraud schemes in healthcare involve bad actors utilizing "good actor" providers. For example, fraudsters are recruiting physicians to participate in seemingly legitimate business ventures, but the physicians end up at the center of substantial fraud schemes. These scams can affect the healthcare organization and its reputation and result in extensive, drawn-out government investigations. Increases in prescribing and ordering uncommon items or unusual billing patterns by physicians may be evidence of potential schemes.

During the PHE, the government increased collaboration among federal agencies to share data and information on fraud schemes like unnecessary ordering of genetic testing and COVID-19 testing. Internal audit, compliance and other fraud-fighting departments are collaborating to leverage multiple sources of data and resources to help illuminate potential fraud. Next-generation internal auditing is crucial to an organization's success in identifying fraud risks.

Key areas for internal audit to focus on during their audits and assessments include:

- Using advanced analytics and automated processes to enable continuous monitoring to help detect outliers faster, identify providers unknowingly participating in fraud schemes and avoid investigations.
- Flagging potential misuse of *locum tenens* physicians and the Q6 modifier on healthcare claims to circumvent payer enrollment and credentialing requirements.
- Monitoring the organization's physician ordering, referring and prescribing patterns for high-risk items associated with current telefraud schemes such as durable medical equipment, genetic testing and the off-label use of synthetic skin substitutes for wound care. (This was the subject of the Department of Health and Human Services (HHS) Office of Inspector General's (OIG's) "Special Fraud Alert" issued in July 2022: oig.hhs.gov/documents/root/1045/sfa-telefraud.pdf.)
- Ensuring that providers listed on the Centers for Medicare and Medicaid Services (CMS) Preclusion List are not billing for, ordering or prescribing items and services. Payers are required to deny payment for a healthcare item or service furnished by an individual or entity on the CMS Preclusion List.
- Monitoring and auditing who can access your provider portals. The federal government has begun to understand the vulnerabilities involving provider portals, the potential for inappropriate access and intrusion by bad actors, and the resulting downstream fraud, waste and abuse (FWA) in the healthcare space. Most provider portals store electronic patient health information (ePHI) and provider credential (National Provider Identifier [NPI]) lookup tools for providers to utilize. However, both domestic and international bad actors have advertised their ability to get

inappropriate access to these provider portals and then sell the access to the portal or the stolen ePHI on the open web and the dark web. Current fraud management efforts should focus on auditing and investigating who has access to provider portals, flagging outlier usage or lookups, and other anomalies indicative of FWA.

In reviewing potential fraud, executives are also finding that internal audits uncover opportunities to improve the overall capture of services. Audits can help surface ways to improve documentation, charge capture and coding processes that mitigate revenue leakage.

T02 Finance & Accounting

Healthcare finance and accounting departments continue to face ongoing challenges in their organizations. Labor-related issues persist, especially as an increasing number of staff prefer a hybrid work model and are less willing to work in a "pre-pandemic" environment.

Organizations continue to focus on productivity and workforce optimization to help offset increasing costs due to labor shortages and competition for existing labor. However, they can only reduce costs so much without impacting their ability to provide high-quality patient care.

Meanwhile, global supply chain issues are driving up non-labor costs for healthcare organizations. These two issues colliding creates one of the greatest downward pressure environments that most organizations' operating margins have seen in decades.

Organizations are focusing more on revenue integrity activities to prevent recurring issues that can lend themselves to revenue leakage. Areas of focus in the revenue cycle include those processes in the identification, capture and billing of items, services, and procedures.

Healthcare organizations are asking finance departments to be more agile and embrace rolling forecasts in place of annual budgets, or at least shorten the annual budgeting cycle to better anticipate the future. Finance must help organizations leverage available financial and operational data to make more informed decisions. That includes making sure the data's integrity isn't compromised.

Key areas for internal audit to focus on during their audits and assessments include:

- Examining revenue cycle processes that can lead to missing charges, delays in claims processing, denials and reduced reimbursements. Examples of issues include poor charge description master maintenance; unoptimized use of tools and technology to capture items, services and procedures; operational gaps; and disparate data and reports to manage and monitor performance.
- Identifying trends such as increased regulatory requirements, decreasing reimbursements, shifts in care delivery settings and hybrid work when developing the annual internal audit plan. These and other trends might require different skill sets in internal audit or a different method of auditing than in the past.

Auditors will also need to partner with their finance and accounting teams to advance everyone's capabilities around financial controls, continuous monitoring tools, accurate and timely performance reporting, and the identification of potential cyberattacks.

T02 User Access Management

Given the Great Resignation and other ongoing workforce challenges, healthcare organizations are dealing with a high volume of user access changes. These changes are driven by the number of employment changes (i.e., hires, terminations, transfers) and the use of contractors, temps and consultants to fill in the gaps. The stress of these changes is adding up and requiring more work from identity and access management teams to keep up.

Additionally, healthcare organizations continue to have a large number of applications in use that may need to be provisioned in one-off processes because they may not be able to leverage centralized access management processes. This is due mainly to different departments or specialties using specialized applications, including web-based software as a service (SaaS) applications that often need to be provisioned directly in the system.

The result is potential backlogs or missed action items related to adding users, documenting access needs and approvals, or removing system access promptly for terminated individuals. Also, given the overall workforce strains across the rest of the organization, user access reviews are not being performed consistently, resulting in unauthorized individuals retaining system access longer than necessary.

Key areas for internal audit to focus on during their audits and assessments include:

- Assessing processes for managing user access and performing testing to determine how provisioning, deprovisioning and user access review challenges are playing out.
- Evaluating specific systems, departments or user groups that result in process deviations and assessing for risk management consistency to help bring awareness and improvements to current practices.

04 Accounts Payable (AP)

Within hospital systems, AP spend is typically second only to payroll costs. In this period of rising inflation, the internal audit department must focus its efforts on areas that protect cash flow while ensuring that spending is well controlled.

Key areas for internal audit to focus on during their audits and assessments include:

- Determining whether the AP department has sufficient, well-functioning internal controls and is operating efficiently.
- Reviewing spend going through the purchasing system. Ideally, most spend will be preapproved with a purchase requisition or purchase order (PO).
- Verifying the three-way match from the purchase requisition and PO to the receipt of the goods or services recorded in the system. This match should be systematically performed to approve the corresponding invoice.
- Assessing whether the approval of invoices for non-PO spend occurred properly before the payment and in conjunction with the relevant spending authority.
- Determining whether vendor setups are adequately approved and completed appropriately, which includes addressing optimal segregation of duties and training AP teams to recognize and escalate spoofing attempts.
- Focusing on identifying erroneous duplicate payments for an entire population using data analytics. Internal audit should focus on improvements in efficiency to become a more effective business partner.

05 Conflict of Interest & Verifications

Physician-owned distributorships (PODs) that derive revenue from selling or arranging for the sale of implantable medical devices remain a focus for regulators. The CMS expanded the Open Payments database on June 30, 2022, to include several additional provider types and additional and revised "nature of payment" categories for Program Year 2021 (January–December 2021):

- The added provider types are physician assistants, nurse practitioners, clinical nurse specialists, certified registered nurse anesthetists and anesthesiologist assistants, and certified nurse midwives.
- The new nature of payment categories are acquisitions, debt forgiveness, and long-term medical supply or device loan.
- Also, the accredited/certified and unaccredited/non-certified continuing education program categories are now combined into one: "Compensation for serving as faculty or as a speaker for a medical education program."

With increased OIG scrutiny, internal audit should assess the mechanisms used for regular monitoring and governance of vendor and POD relationships to ensure operational and reputational risks are being managed. This should also include employee, provider and vendor verifications. Failing to verify or monitor licenses and credentialing appropriately can result in noncompliance with applicable laws, regulations and accreditation standards. It also can put patients and staff at risk. Healthcare organizations with weak verification processes risk violating the CMS Conditions of Participation (CoP) and the False Claims Act.

Key areas for internal audit to focus on during their audits and assessments include:

- Analyzing the Open Payment database to identify payments reported for an individual that weren't disclosed within that individual's conflict of interest (COI) survey. Also, make sure to look at how research payments fold into the COI process.
- Validating processes to verify and document the business need for all payments (internal and external).
- Verifying appropriate approvals were received from all required individuals and committees while building out conflict management remediation plans.
- Confirming that credentialing, privileging and payer enrollment processes were performed within required time frames (e.g., upon hire, recertification), as per contracts, regulations and policies.
- Identifying the amount and source of foreign investment in research funding and endowments.
- Verifying that state licenses, certifications, references, controlled substance registrations and insurance were verified within required time frames, as per laws, regulations and policies.

Auditors should also focus on exclusion checks. Examples include the OIG List of Excluded Individuals and Entities (LEIE), state-specific Medicaid exclusion lists and the General Services Administration (GSA) System for Award Management (SAM).

06 EHR/ERP Implementations

With the frantic pace of change in healthcare, organizations are investing more in electronic health records (EHR), enterprise resource planning (ERP), customer relationship management (CRM), claims management systems and other technologies to drive operational and quality enhancements and cost efficiencies. Whether implementing new systems, upgrading existing platforms or optimizing system configurations, these investments can lead to significant business transformation and improvements in patient care.

Often, when making enhancements to systems, organizations concentrate too much on isolated tasks instead of designing and configuring key aspects of a function in an integrated fashion with the end-to-end process in mind. We believe there are eight critical elements to consider when designing an optimized end-to-end solution as part of an implementation or upgrade:

1. Key process activities and flows
2. Triggering events
3. Business rules that an activity should follow
4. Vital data elements and necessary attributes
5. Related systems of records
6. Key integrations
7. Reporting requirements
8. Governance, security and compliance requirements that must be met

EHR, ERP, CRM, claims management and other systems are extremely complex to secure. Out-of-the-box security roles often contain inherent security concerns, including sensitive access and segregation of duties conflicts. Security roles and user access should be tailored to the organization's needs. Also, the fact that cloud-based systems blur lines between operations and IT should be considered during upgrades and new implementations.

Newer technologies come equipped with increased control capabilities, including workflows, validations, tolerance settings and a host of other automated controls. As part of any technology initiative, organizations should spend adequate time assessing control-enhancing features to determine whether they should be turned on and how best to configure and incorporate them into their overall governance and compliance processes.

To realize strategic objectives and planned benefits, healthcare organizations should focus on several key areas and dedicate sufficient resources to ensure related initiatives are successful. Given the amount and pace of change that these new technologies introduce, there are many key areas for internal audit to consider and focus on that include:

- Establishing the appropriate level of program governance.
- Evaluating whether the solution design adequately defines each critical element and incorporates them into an integrated, end-to-end process model.
- Confirming that advanced control-enhancing features of EHR and ERP systems are appropriately turned on, configured and tested.
- Ensuring sufficient time and energy are dedicated to tailoring security roles so that sensitive functions are protected and segregated appropriately.

Lastly, understand that while new technologies can provide tremendous operational benefits to healthcare organizations, they can also dramatically change the control environment.

T07 Privacy & Security

Cyber threats disrupt the healthcare industry, as they do for all industries. However, because healthcare organizations have been focused on the PHE and trying to keep up with the flow of patients, information security efforts have taken a back seat.

The result is a notable regression in the maturity of information security environments across healthcare organizations compared with pre-pandemic levels. This is due to the lack of ability to continue to keep up and perform preventive actions to ensure processes are still well-designed and actionable. Healthcare organizations have deferred many security-related activities in recent years, including:

- Technical penetration testing
- Security incident response testing activities
- Disaster recovery exercises
- User access reviews
- Policy and procedure reviews and updates

- Information security program assessments
- Associated investments and projects designed to address areas of weakness

The threat and vulnerability landscape changes on a seemingly hourly basis in cybersecurity, making it difficult to address new items constantly. Many of these items start to blur the lines of what we have typically monitored for through a cybersecurity lens as they get into other components that may impact the broader sense of what constitutes security and even privacy. Some of the latest items hitting the news have included: Meta Pixel in use on websites scraping potentially sensitive data and sending it to Meta (Facebook) for analytics/marketing, often without the organization truly being aware, use of stolen NPIs to falsify claim and reimbursement information, and social engineering actions targeting clinicians and where their reimbursements are being sent.

Healthcare organizations are struggling to attract and retain skilled information security professionals. Because these skills are in such high demand across the world, top security professionals essentially have their choice of opportunities. Privacy programs also face the challenge of doing more with fewer resources due to pandemic-triggered staffing changes. Some healthcare organizations only recently started to address their labor issues by recruiting experienced talent to fill positions previously furloughed.

The pandemic has also created challenges in the everyday work environment. For example, many staff members are transitioning to a fully remote or hybrid work model. Also, there are decreased opportunities to conduct on-site activities such as privacy walkthrough audits and in-person trainings.

Health Insurance Portability and Accountability Act (HIPAA) enforcement remains strong. This further emphasizes the importance of conducting periodic assessments of a healthcare organization's privacy and security program to identify and mitigate risks. This is especially important in cases where an organization's risk profile may have changed due to newly implemented processes, workflows, tools and technologies precipitated by the pandemic.

A focus should be placed on current areas of scrutiny from the Office for Civil Rights (OCR), such as a patient's right to access their medical records or other anticipated areas of regulatory scrutiny, such as the organization's compliance with the Information Blocking Rules.

It is a critical time for healthcare organizations to assess and understand any current challenges related to their privacy program. That will help the organization anticipate the hurdles it may face from operational changes caused by the finalization of the proposed HIPAA Privacy Rules. These rules could have far-reaching impacts across compliance and privacy programs as well as other organizationwide departments such as patient access and health information management (HIM).

Internal audit can play a critical role in assessing and monitoring the challenges impacting a healthcare organization's information security and privacy posture and raising those potential concerns as an independent voice to the organization's management to ensure these issues remain top of mind and are addressed accordingly.

Key areas for internal audit to focus on during their audits and assessments include:

- Determining whether controls are in place for timely response to individual rights requests from patients or their legally authorized representatives.
- Assessing the processes used to monitor compliance with Business Associate Agreement Requirements, such as appropriately executing agreements in a timely manner and managing and tracking agreements and vendor relationships on an ongoing basis.

- Periodically reviewing the HIPAA Privacy and Security Gap Assessment and associated remediation plans to ensure they accurately reflect current operational processes and the status of ongoing improvements and remediation activities.
- Evaluating information security risk analysis and associated risk management plans for frequency, completeness and ongoing improvement.

Also, assess the organization's incident response plans and how they are being practiced, tested and updated to validate their usefulness.

T07 Supply Chain

Internal audit functions should ensure that the supply chain function (as identified by the healthcare organization) has a plan in place to define and implement resilience into the organizational supply chain. Supply chain resilience includes aspects of traditionally defined procure-to-pay, clinical integration, distribution and inventory management, as well as executive-level goals and business continuity plans. Resilience will invariably include relationships with the organization's primary and secondary group purchasing organizations (GPOs), distribution partners, and individual vendors.

Supply chain functions should be governed by clinically and financially promulgated goals to best utilize strategic sourcing and mitigate potential supply disruptions. Primarily due to pandemic-related supply chain disruptions, organizations with a resilience-first mindset are moving away from LUM (logical unit of measure or lowest unit of measure) inventory and ordering approaches and toward a (limited) buy-and-hold model. Finding the correct balance will be integral to managing an organization's inventory and costs effectively.

Additionally, some organizations may encounter the problem of inventory accrued during the pandemic and potential obsolescence, shrink and waste. Fixed-asset aging and tracking will continue to be an important function of the supply chain, which, due to market uncertainties, may be required to forgo scheduled or planned upgrades and refreshes so that the organization can defray the rising costs of essential products and services.

Vendors continue to join and split products and categories as they seek to gain the most advantageous product mix in specific markets. Partnerships with like-minded organizations and contractual agreements with GPOs, to aggregate spend, will require significant due diligence to protect the organization from potentially damaging consequences. Procure-to-pay (P2P) and inventory data should be readily accessible and actionable for its respective departments.

Key areas for internal audit to focus on during their audits and assessments include analyzing P2P operational risks, such as:

- Payment summaries, analysis, stratification and type analysis
- Invoice stratification
- PO vs. non-PO spend, volume and conversion
- Suppliers with both PO and non-PO spend
- Supplier master file
- Working capital/transactional (e.g., payment terms analysis and variation, average days to pay, interest expense incurred)
- Spend audits by general ledger and duplicate payments

Also, analyses of inventory data should include replenishment operations processes, such as PAR demand signal and order triggering, bin management, cycle counting, stock on hand, inventory position and utilization, and ERP data transaction processes.

09 Data Governance & Analytics

The overall change in healthcare reimbursement and continued shift from fee-for-service to pay-for-performance reimbursement models (i.e., value-based care) is driving an exponential increase in the scope and span of provider, payer and regulatory data requirements. In addition to the increased data footprint, this change adds complexity and magnifies the importance of how data is integrated and aggregated in determining a single source of truth and overall interoperability.

Healthcare organizations must measure data points across the entire care continuum to evaluate and monitor how well they are performing by demonstrating improved outcomes. There is more scrutiny than ever as regulatory oversight requirements force more transparency through reporting that is made available to the general public.

This all leads to healthcare organizations placing a heavy emphasis on how to use data more effectively to improve patient care, member and provider engagement, population health management, decision-making, timely monitoring and auditing activities, and analytics and reporting in a way that is easy to understand.

Many healthcare organizations believe they are leveraging advanced analytics in practice. However, fundamental and sound data governance practices are often significantly lacking across the industry, resulting in disjointed efforts and a perceived lack of value. Population health initiatives, including more advanced practices that use artificial intelligence (AI) and machine learning (ML) to drive preemptive intervention, remain heavily reliant on a data-rich environment frequently plagued with issues across provider organizations.

Key areas for internal audit to focus on during their audits and assessments include:

- **Data governance** — Conducting reviews of data quality, data lineage, sourcing, security, utilization, transformation, and other aspects of managing and cataloging data as an asset.
- **Continuous monitoring** — Designing and 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** — Performing a current state analysis to understand current data and analytics (D&A) strategy and capabilities and organizational goals, and assessing the corresponding road map to ensure alignment.

T10 Pharmacy Operations & Drug Compliance

Pharmacy operations and drug compliance continue to be a strong focus for organizations, given the complex regulatory landscape and the worsening opioid crisis. Upcoming regulatory changes, enforcements and recent U.S. Department of Justice (DOJ) rulings around opioid prescribing and the 340B program will require a much greater focus from healthcare organizations' operations, internal audit and compliance departments.

Key areas for internal audit to focus on during their audits and assessments include:

- **Opioid prescribing** — A health system in Colorado was fined for not properly supervising the opioid prescribing practices of their employees. Audits should confirm proper monitoring of prescribing, including compliance with state laws for checking the Prescription Drug Monitoring Program (PDMP), and implementing pain agreements, drug screens, and morphine milligram equivalent (MME) limits. Analytics and continuous monitoring will provide real-time outliers.

- **Drug diversion** — A health system in Texas was penalized for failed internal controls and safeguards that led to the diversion, misuse and abuse of opioids. Pharmacy technology has greatly changed the way organizations are monitoring for drug diversion. Still, organizations struggle with properly implementing advanced analytics and the resourcing and communication among key stakeholders. Audits should focus on the appropriate use of analytics tools, continued support and development of drug diversion programs, and consistent and effective investigation and reporting protocols. Additionally, education and awareness of impairment and diversion for all staff should be evaluated to support a culture of safety for patients and staff.
- **340B Program** — Manufacturers continue to restrict drug discounts for external (contract) pharmacies, and the Health Resources and Services Administration (HRSA) has issued warning letters for violating the 340B requirements. The recent federal ruling regarding drugmakers that have the authority to restrict sales of 340B-discounted products to contract pharmacies is being appealed. Also, the U.S. Supreme Court ruled in June 2021 that the HHS payment reductions for 340B drugs were unlawful. Covered entities should estimate lost reimbursement from CMS payment cuts, continue self-audits to ensure compliance with program requirements, and perform independent program reviews to verify proper contract pharmacy arrangements and program optimization to ensure all qualified discounts are received.
- **Pharmacy Benefit Manager (PBM)** — Formulary design, supply chain, 340B, rebates, medication therapy management (MTM) programs and manufacturer rebates all continue to be a focus of the U.S. Federal Trade Commission (FTC) and intense public scrutiny. Prescription drugs are often the first expense and experience a member has with their health plan, so strong processes and controls are needed to drive quality outcomes, financial performance and regulatory compliance.

Upcoming guidance and enforcement around sterile compounding, electronic prescribing of controlled substances (EPCS) and the Drug Supply Chain Security Act (DSCSA) should also be considered for internal audit review.

T10 Third Parties

Healthcare organizations partner with third-party vendors, suppliers, contractors and other business partners to outsource services, drive service excellence, increase efficiency, control costs and risks, or gain other competitive advantages. Some organizations have large, well-established third-party networks, while others are in the early stages of developing vendor relationships. With increasingly complex third-party ecosystems, the PHE coupled with geopolitical crises, rising customer demands, disruptions in the supply chain, a rapidly changing regulatory environment and ever-looming cybersecurity threats, there is tremendous pressure on these organizations to ensure their vendors maintain consistent compliance with internal policies and evolving regulations.

Vendor risk management is the practice of evaluating business partners, suppliers or third-party vendors both before a business relationship is established and over the duration of a contract. It has advanced from an annual checklist exercise to a critical daily function. An organization's approach can significantly affect its ability to achieve its goals. 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 the success of an organization.

In general, healthcare organizations and executives recognize the importance of vendor risk management; however, few organizations can say they are doing it effectively. In fact, many organizations report they have recently experienced a third-party incident. For the many healthcare organizations who struggle with vendor risk management, the inability to adequately assess and understand the risks that vendors pose can become incredibly costly. Many healthcare organizations do not believe that their vendor risk assessments, as they exist today, are valuable for providing actionable insights to the C-suite and board of directors.

Meanwhile, organizations rapidly maturing their vendor management capabilities and processes are realizing significant competitive advantages. A well-defined vendor management function also provides early warning, allowing an organization to plan its response and drive effective risk mitigation rather than simply trying to react on an emergent basis.

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 testing the program management has developed and implemented and providing value-added feedback.

Key areas for internal audit to focus on during their audits and assessments include:

- Ensuring there is a well-defined vendor governance framework.
- Reviewing appropriate governance documents.
- Confirming there is an effective vendor sourcing and selection process.
- Determining if there are established contractual standards.
- Assessing whether there are efficient intake and onboarding processes.
- Assisting with periodic due diligence and continued oversight.
- Developing an internal vendor risk assessment or scoring process.
- Establishing a robust vendor inventory and performance monitoring process.
- Creating effective termination and offboarding processes (as needed).
- Assessing the organization's processes to classify and perform due diligence on vendors based on inherent risks.
- Performing background checks and uncovering risk indicators within public databases.
- Reviewing how contractual documents are created, retained and reviewed as a function of identified risk.
- Identifying third-party risks using advanced analytics and automation.
- Evaluating the vendor risk management life cycle to determine how effectively the organization uses ongoing assessments and performance monitoring mechanisms (e.g., scorecards, questionnaires, standards for service-level agreements (SLAs), automation and other tools) to manage the overall portfolio of vendor risk.

Also, internal audit should verify compliance with business associate agreements, evaluate third-party relationship changes where patient information is exchanged since the execution of the original agreement, and review business associates' controls.

Other key takeaways

Looking to 2023

Areas that are not included in the 2022 audit plan but appear to be priorities for 2023 include:

- IT Disaster Recovery
- Billing Accuracy and Accounts Receivable
- Employee Time/Expense Reporting and Payroll
- Financial Relationships With Physician/Other Referral Sources, Associated Compliance Risks, and Physician-Owned Distributorships
- IT Governance

Lack of skills and competencies

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

- Emerging Technologies (Automation, AI, Predictive Analytics)
- Changing Delivery Model Across the Care Continuum
- Compliance, Utilization, and Quality/Risk Committees
- Environmental Compliance, Infection Control and Prevention, and Hazardous Waste Disposal
- Graduate Medical Education (GME)
- IT Disaster Recovery

"Most internal auditors today understand the direction internal audit is heading and are putting together what is required to transform internal audit into a next-generation function, including advanced data analytics tools and deep digital skill sets. The challenge is helping the healthcare organization's leadership to understand why they should invest in the function's transformation now, and what it will mean for the business in the long term if it does — or doesn't."

— **Jarod Baccus**
Director, Healthcare Internal Audit Practice Leader
Protiviti

Conclusion

The healthcare industry is emerging from a period of unprecedented disruption, but in many respects, some of the most daunting challenges for healthcare provider organizations still lie ahead. Risk is everywhere, from pervasive fraud to data security threats to complex regulations. But so are opportunities, including new healthcare delivery and workforce models and revenue generation channels.

What is critical for healthcare provider organizations to keep in mind as they plan for a post-pandemic future with increasing confidence is that their internal audit functions likely played no small part in helping to see them through the crisis. Businesses that had the added advantage of being able to lean on an internal audit team that was already evolving into a next-generation function before COVID-19 are likely much more resilient and agile now because of it.

Healthcare provider organizations need to invest more in their internal audit functions. As our 2022 healthcare internal audit plan priorities survey shows, many internal audit organizations are at risk of falling behind technologically despite their desire to modernize tools and systems and expand their workforce. Ensuring that internal audit teams have the financial resources and other support necessary to advance their technological capabilities, build highly skilled and engaged teams and focus more on innovation is necessary not only to build a true, next-gen function, but also a future-forward healthcare organization.

Appendix A: Internal Audit Functions and Moving Forward With the Next-Gen Journey

Healthcare provider organizations have been hit especially hard by the PHE. The past two years have seen some internal audit innovation and transformation among these organizations as they've pivoted and adapted in response to the crisis.

Innovation and transformation are now mainstays in helping to ensure organizations in any industry can stay relevant and competitive over the long term. According to our latest Next-Generation Internal Audit Survey, two in three internal audit functions are now engaged in or have completed innovation and transformation initiatives — a 6% increase from our 2021 survey.[1] However, only one in three internal audit functions in the healthcare industry is currently undertaking any innovation or transformation initiatives.

Another key takeaway from our research is that if the internal audit function has yet to undertake any form of innovation or transformation activities, it's missing opportunities to remain relevant. It's also likely lagging behind the competition — and building barriers to accessing and developing talent.

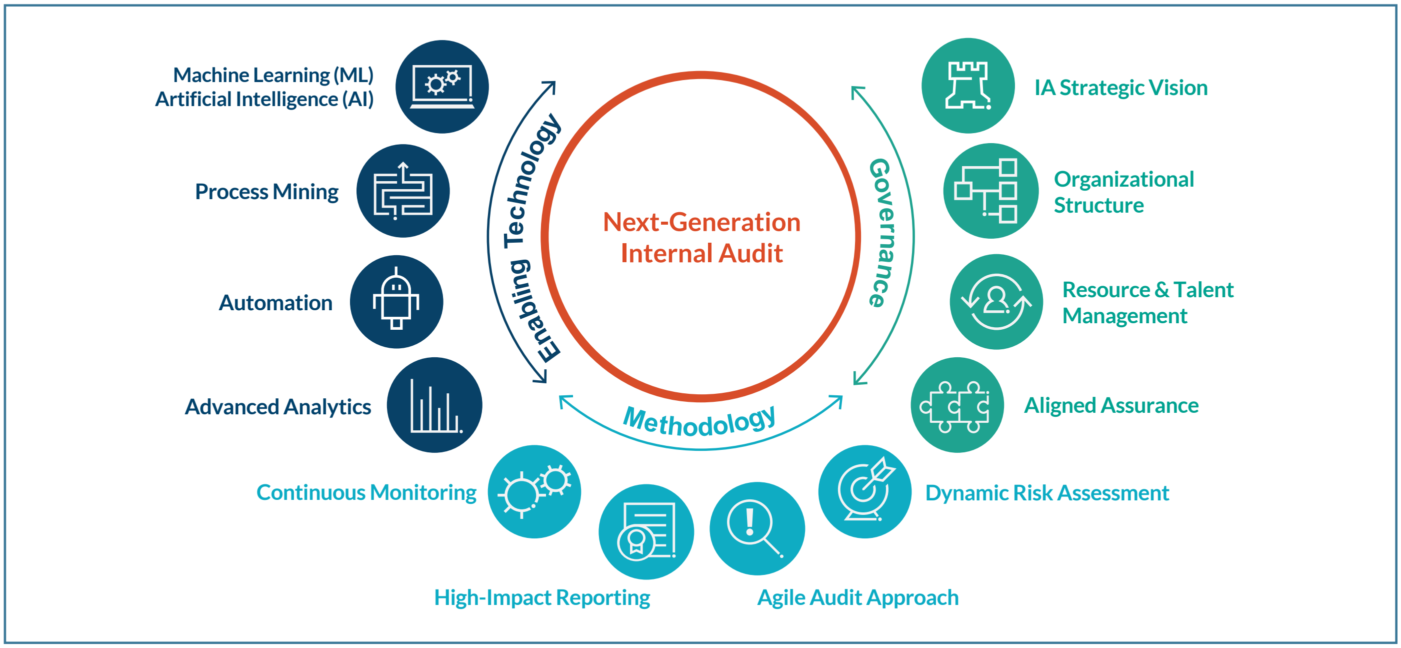
These all-industries themes[2] include:

- Increasing the use of data and analytics solutions.
- Improving the risk assessment approach.
- Furthering the pursuit of continuous auditing and monitoring.
- Evolving collaboration and aligning of internal audit with other assurance functions.

As with all industries, many of the key challenges across the healthcare industry that we expect to continue in 2023 are directly or indirectly related to internal audit and next-gen concepts such as innovation and transformation. These challenges include:

- Leveraging data and data governance practices.
- Emerging technologies and digital transformation.

Next-Generation Internal Audit Framework

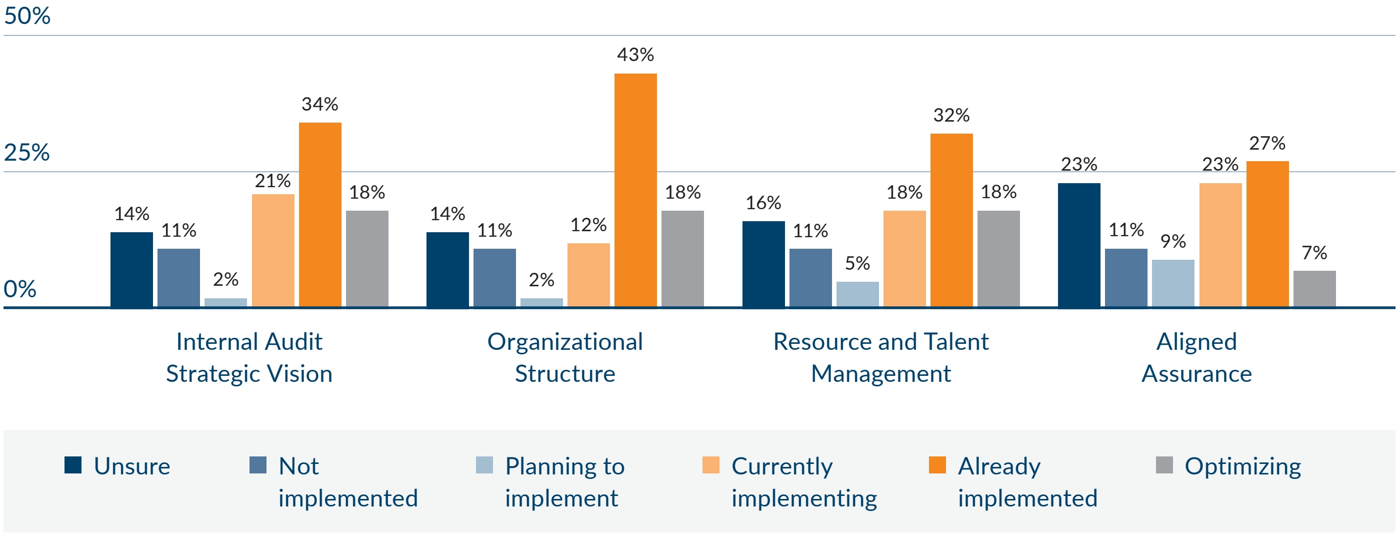


[1] *Innovation and Transformation Are Driving the Future of Internal Auditing*, Protiviti, 2022: www.protiviti.com/US-en/insights/whitepaper-next-gen-internal-audit-survey.

[2] Ibid.

Governance

Please outline your internal audit department's level of implementation related to the following Governance components.



When the COVID-19 pandemic hit, many internal audit functions determined it would be a good time to reassess their department and ensure they were nimble and aligned to best help their organizations through the pandemic.

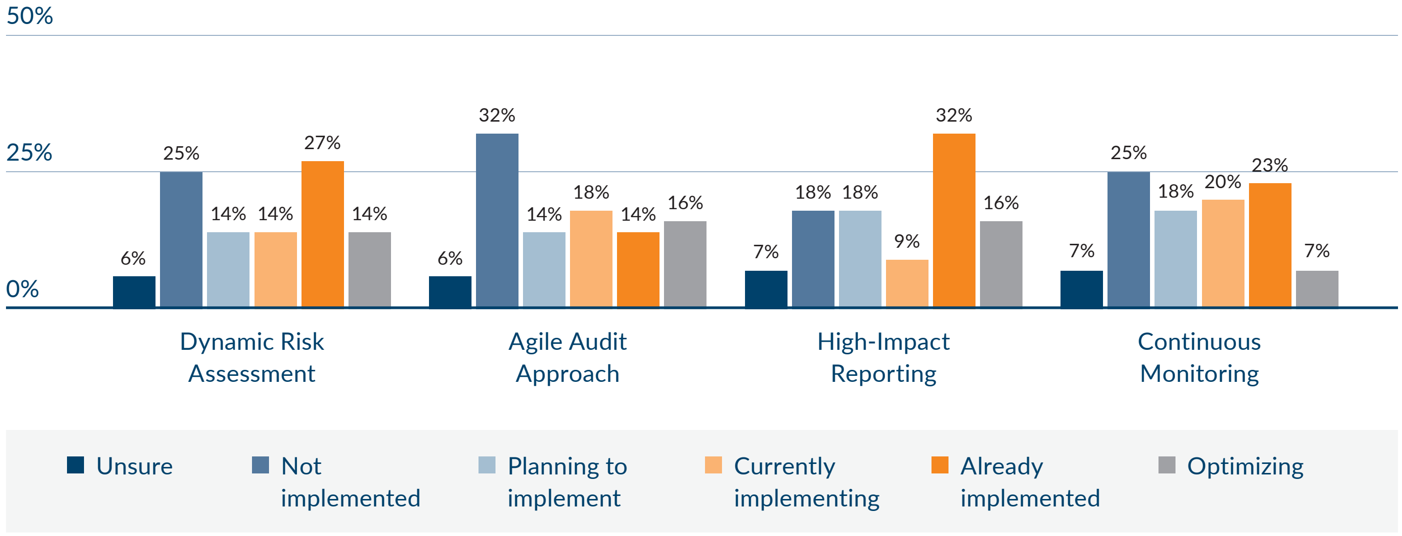
This year's data continues to show a migration from methodology to governance. It appears that over 70% of respondents are between "currently implementing" and "optimizing" their internal audit strategic vision and organizational structure, both an increase from 2021. Out of all the next-generation internal audit components, the governance category has been prioritized by the largest percentage of healthcare internal audit functions in 2021 and 2022, according to our survey.

Strong governance competencies are the foundation of an internal audit function. They determine how internal audit fits into the organization's strategy, how the function is structured, how it maximizes the use of staff and high-demand resources, and how it cooperates with "second lines" (e.g., compliance, risk) within the organization. The key is simply getting started and moving forward; this should be seen as an opportunity rather than an issue.

Our research shows that two-thirds (66%) of internal audit functions in the healthcare industry are choosing to fill the gaps of next-gen skill sets with a strategic co-sourcing partner that has specialized expertise not found in-house, which is up 14% over last year's data.

Methodology

Please outline your internal audit department's level of implementation related to the following Methodology components.



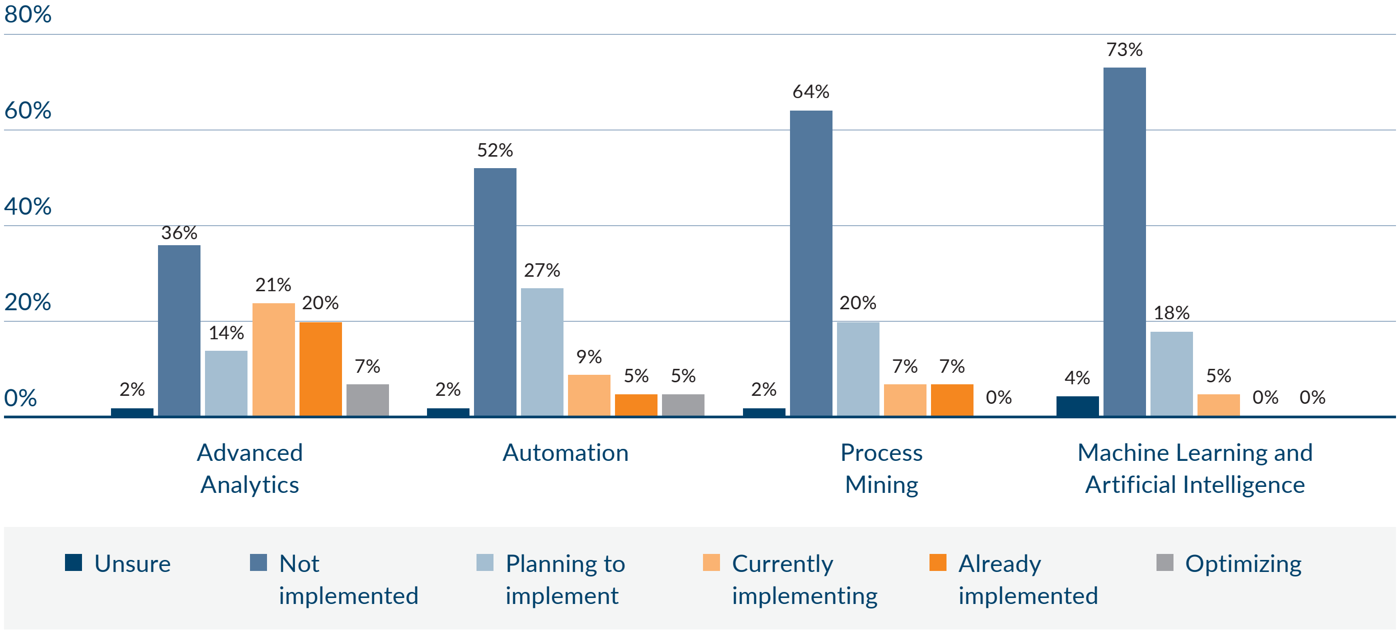
High-impact reporting continues to be a priority and, for the second year in a row, is the largest methodology component and is used by the largest percentage of healthcare internal audit functions, according to our survey. Examples of high-impact reporting include:

- Interactive follow-up and corrective action dashboards, which can provide an overview of all open and closed corrective action plans, follow-up findings and/or investigations, alerts to management about items coming due and items past due, and a repository of historical items; these measures help to facilitate timely resolution of open action items, follow-ups and accountability across the organization.
- Implementing a disclosure management and monitoring tool by leveraging data analytics allows organizations and providers to monitor and provide a holistic view of providers' and advanced practice providers' (APPs) potential conflict of interests and related payments.
- Dynamic risk assessment dashboards to identify, analyze, prioritize and evaluate an organization's clinical, compliance, financial, IT, operational and revenue cycle risks proactively and continuously; these measures can help the organization reach strategic initiatives and goals.

Consistent with prior years, most internal audit functions in the healthcare industry (59%) continue to perform and/or refresh their risk assessment process only annually. However, there was a slight shift in our latest survey, with 27% of the respondents reporting that they're moving toward a more dynamic risk assessment approach where they review risks continuously to help track the real-time pulse on their organization's health.

Enabling Technology

Please outline your internal audit department's level of implementation related to the following Enabling Technology components.



Implementation levels are the lowest among the enabling technology components, with ML/AI, process mining and automation being the lowest (5%, 14% and 19%, respectively, currently implementing or better). These findings aren't surprising, as these areas are complex, expensive to implement and unfamiliar to most internal audit functions. All four of the enabling technology components:

- Rank as the top four components most organizations are interested in implementing; however, organizations are also doubtful they can procure resources with the right skill sets to use them. Therefore, most leaders tend to lean more on co-sourcing, rotational staff from the enterprise and guest resource programs to develop and deliver certain skills and capabilities, particularly with regard to technical and enabling technology areas.
- Rank within the top five components that organizations believe they will need the assistance of a third party to audit.
- Continue to rank as the lowest competency scores year over year.

Perhaps the most interesting item to note is that many organizations want to build out their methodology components. However, many have yet to implement advanced analytics, a critical capability for this process.

Protiviti's vision for the next generation of internal auditing

The specific governance structures, methodologies and enabling technologies that next-generation internal audit groups introduce vary. However, nearly all of the transformations Protiviti has supported or seen have addressed most, if not all, of the competencies, qualities and components in three broad categories illustrated below. A summary of each follows.

Governance

- **Internal Audit Strategic Vision** — Next-generation internal audit organizations should seek to define a clear and concise strategy to establish the function's purpose, enable achievement of objectives within the established vision and mission, and facilitate a culture of innovation that helps achieve the function's strategy and ensure future relevance.
- **Organizational Structure** — A traditional internal audit hierarchy begets a traditional approach. As new methodologies are embraced, the organizational structure to support them will begin to look very different. The structure must be developed to allow for sufficient and flexible coverage across legal entities, geographies in which the organization operates and risks facing the organization. Reporting lines and roles and responsibilities of both audit and support teams will be redrawn. The composition, size and locations of the audit and support teams will also look very different. Flexible resource models will be employed to gain access to skill sets and capacity as needed.
- **Resource and Talent Management** — In today's corporate climate, a resilient workforce will prove vital to a company's ability to pivot in the face of changing market realities. The workforce of the future needs to be reimagined for increased flexibility and be able to respond to rapid changes in business. Next-generation internal audit groups need to ensure that robust resource management strategies and processes are in place to acquire, manage, retain and enhance the resources, skill sets and capabilities that will enable the internal audit function to achieve both core assurance and transformational goals and objectives.
- **Aligned Assurance** — Aligned enterprise assurance is a correlation of risk, controls and a broader view of the control environment across the three lines and by and between the organization's assurance functions. It seeks to maximize operating efficiency and provides clearer visibility of results to stakeholders. This approach facilitates governance and management of risk within an organization's risk appetite and aims to optimize the coverage of assurance obtained from management, and internal and external assurance providers on the risk areas affecting the organization.

Methodology

- **Dynamic Risk Assessment** — Internal audit functions that desire to enhance and transform their organization should continually seek to adapt their risk assessment approach to quantify risk more effectively in a rapidly evolving business environment and execute relevant assurance work to align with key organizational risks and priorities. A dynamic risk assessment approach is designed to be increasingly data-driven and adaptive to emerging risks and proactively measure key existing risks, enabling organizations to identify changing risk trends in real time, quantitatively measure and prioritize risk, and drive the most effective use of assurance coverage.
- **Agile Audit Approach** — An agile audit approach uses a framework that is based on iterative and sustainable development, where requirements and solutions evolve through collaboration among cross-functional audit teams focused on quality. Internal audit and its stakeholders are focused on a

common goal of risk mitigation through responding to changing and emerging business needs and directions while simultaneously working to meet business and regulatory commitments.

- **High-Impact Reporting** — Internal audit demonstrates its value by communicating effectively and, in the process, utilizing simplified and high-impact reporting. This is the culmination of all internal audit's activities leading to the right type of communication tailored to each audience to achieve maximum impact. Communications should occur in various forms to stakeholders with different needs and expectations, including audit reports, risk assessments, audit committee presentations and reports to regulators. Next-generation internal audit functions communicate what stakeholders need to know and allow them to drill down to the details as needed.
- **Continuous Monitoring** — Next-generation internal audit organizations should seek to adopt a robust continuous monitoring program to optimize the efficiency and effectiveness of their audit operations and facilitate deployment of audit resources to more strategic efforts. Organizations should work to create a technology road map that includes the necessary data and functionality to facilitate a continuous monitoring program. Internal audit organizations also should consider the potential for continuous monitoring in the context of their broader assurance strategy.

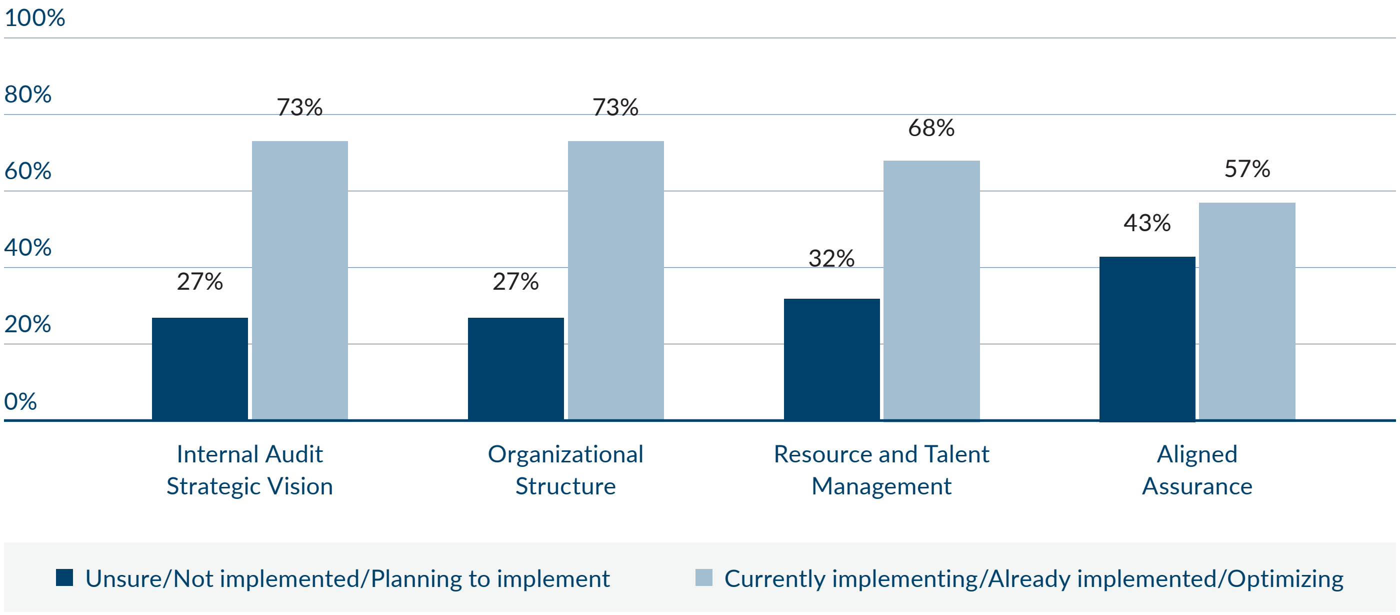
Enabling technology

- **Advanced Analytics** — Internal audit organizations should challenge their current state of analytics capabilities and commit to making better use of data, raise awareness, develop skills, explore new tools, establish a plan and drive incrementally increased use.
- **Automation** — As the popularity of automation increases, including but not limited to robotic process automation (RPA), internal audit departments should be asking about their organization's current strategy and plans and evaluating whether there are any processes or tasks that lend themselves to automation. This can increase the effectiveness and efficiency of audit work by improving audit quality and coverage as well as by automating routine audit tasks, which, in turn, frees up time for more value-adding work.
- **Process Mining** — Internal auditors should seek out new technologies that will help add value to their organizations beyond traditional audit methods. Enabling technologies such as process mining allow auditors to analyze large quantities of data easily, visually recreate processes from data, explore deviations and identify root causes of previously unknown issues. Process mining also allows for more dynamic and meaningful reporting.
- **ML and AI** — Organizations are rapidly looking to turn their data into value-added products and services through ML techniques. Internal audit departments need to be familiar with this field of study, the risks and opportunities it presents, and how it can be applied. AI and ML represent great examples of techniques with the potential to deliver significant value throughout the internal audit life cycle (risk assessment and planning, scoping, discovery, fieldwork, reporting, follow-up and monitoring) and change the way internal auditors use data to complete audit activities.

Appendix B: Additional Survey Insights

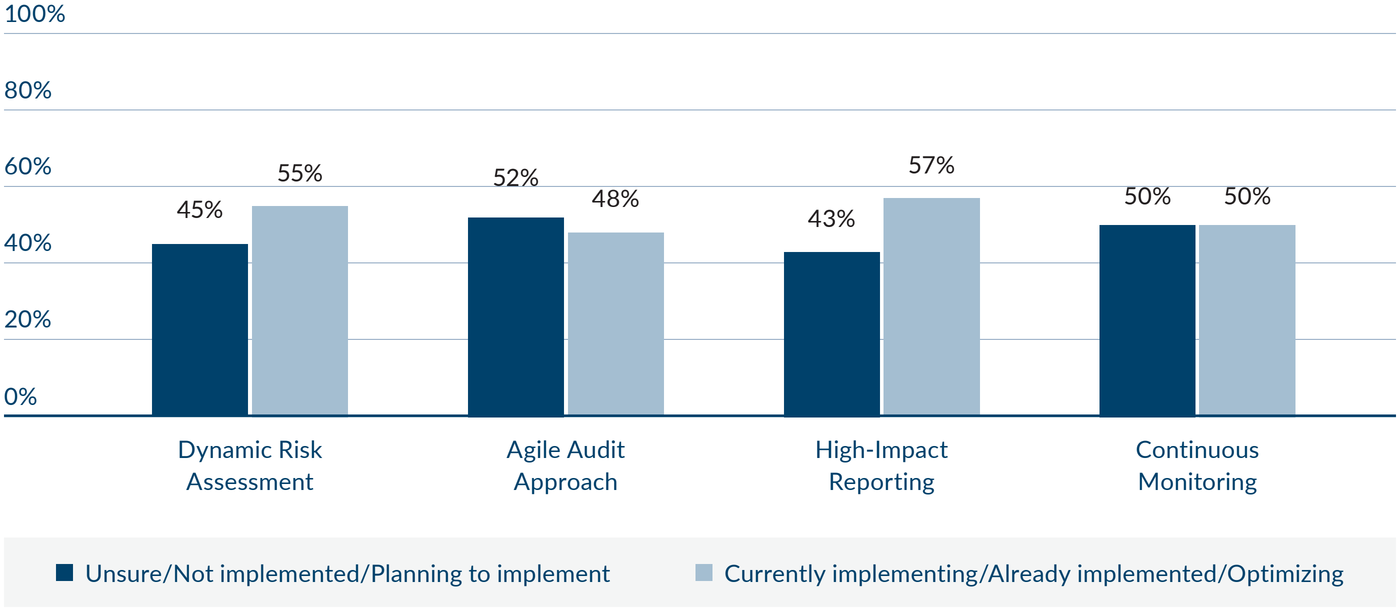
Please outline your internal audit department’s level of implementation related to the following Governance components.

GOVERNANCE



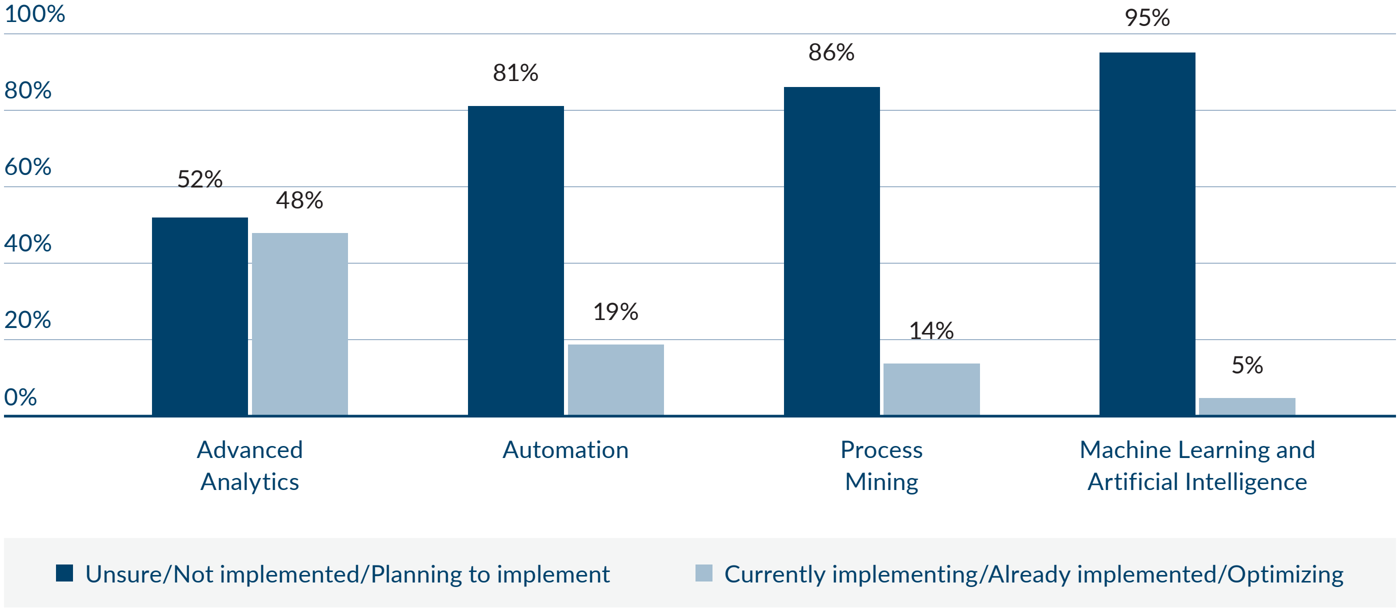
Please outline your internal audit department's level of implementation related to the following Methodology components.

METHODOLOGY

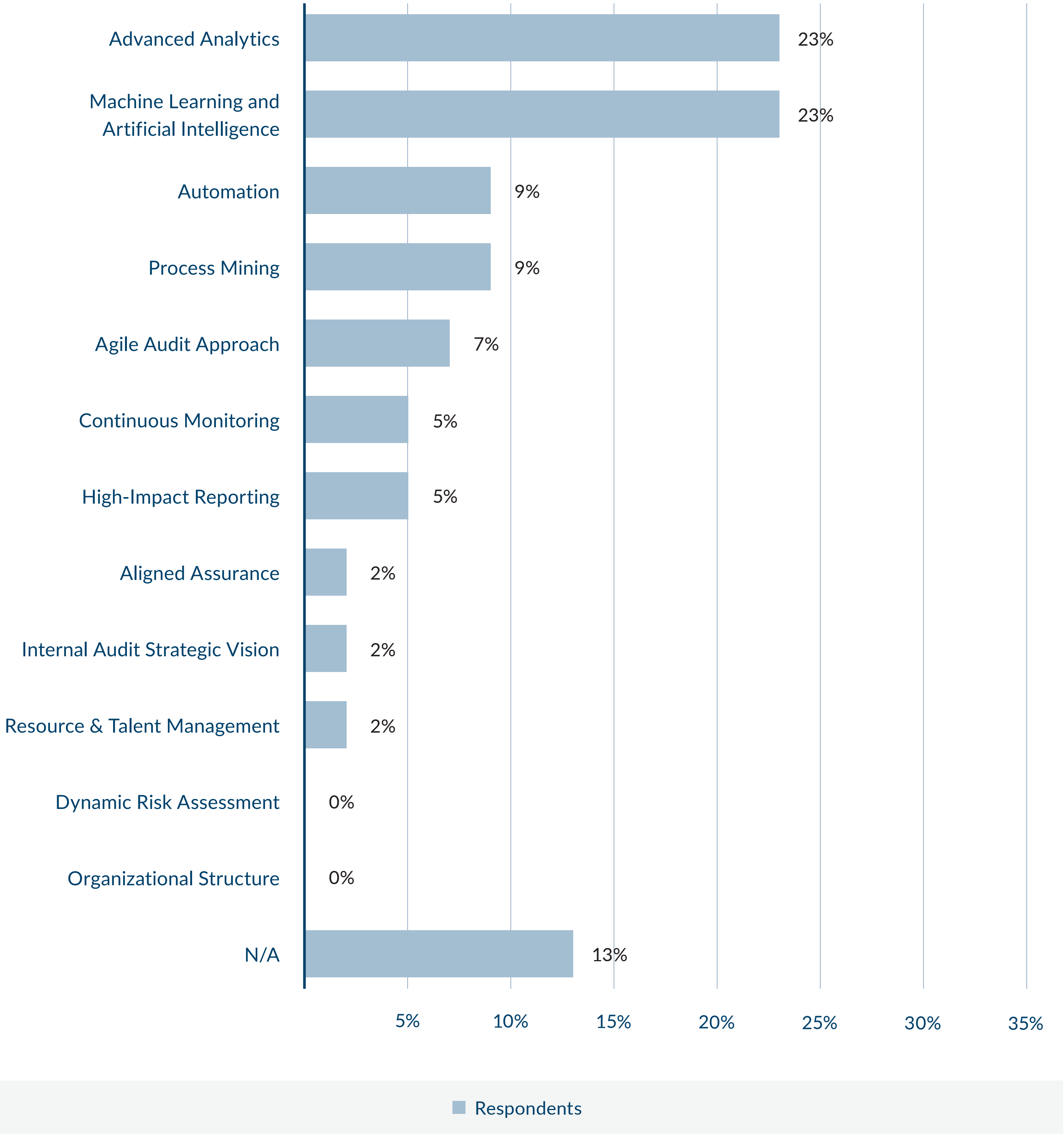


Please outline your internal audit department's level of implementation related to the following Enabling Technology components.

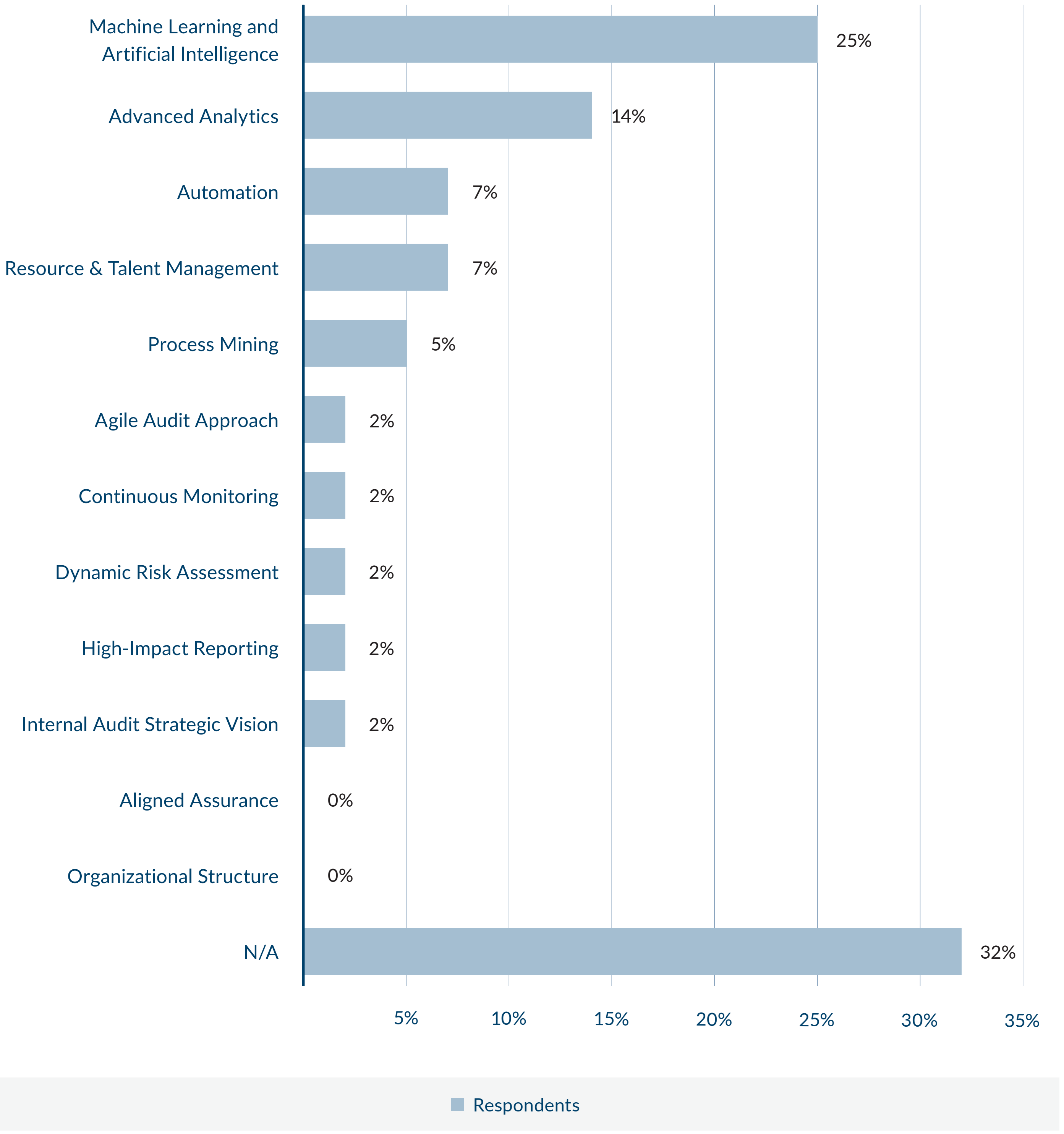
ENABLING TECHNOLOGY



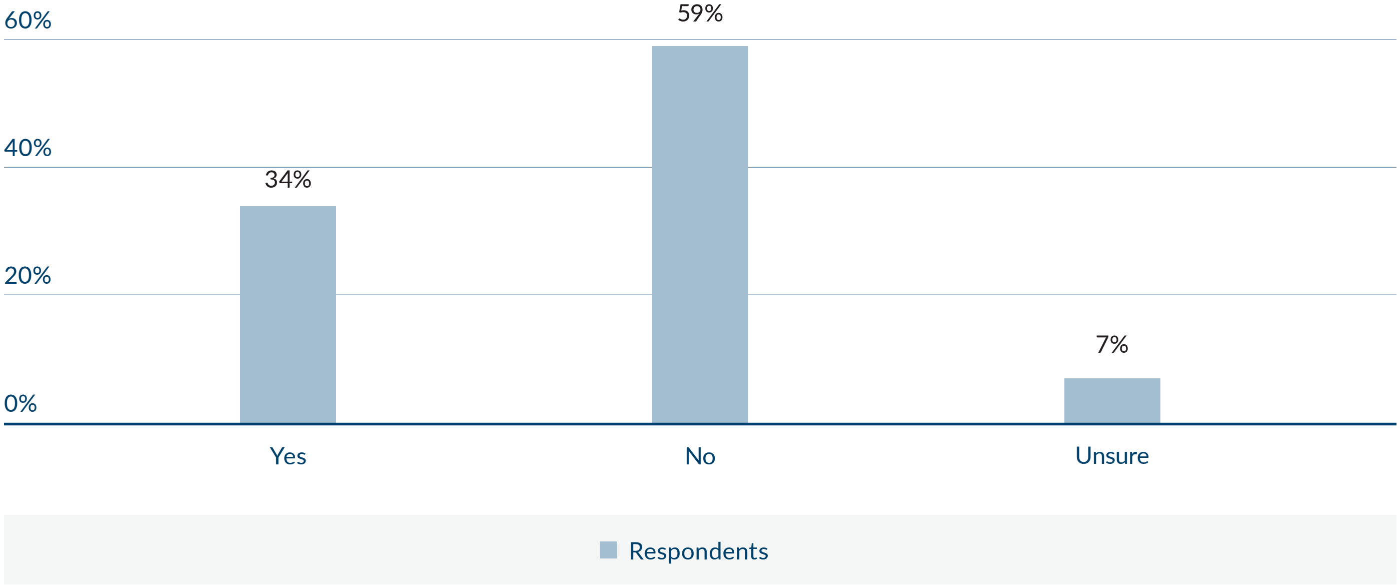
What next-gen area, if any, are you most interested in implementing within internal audit service capabilities but most doubtful that you will be able to procure the resources to do so?



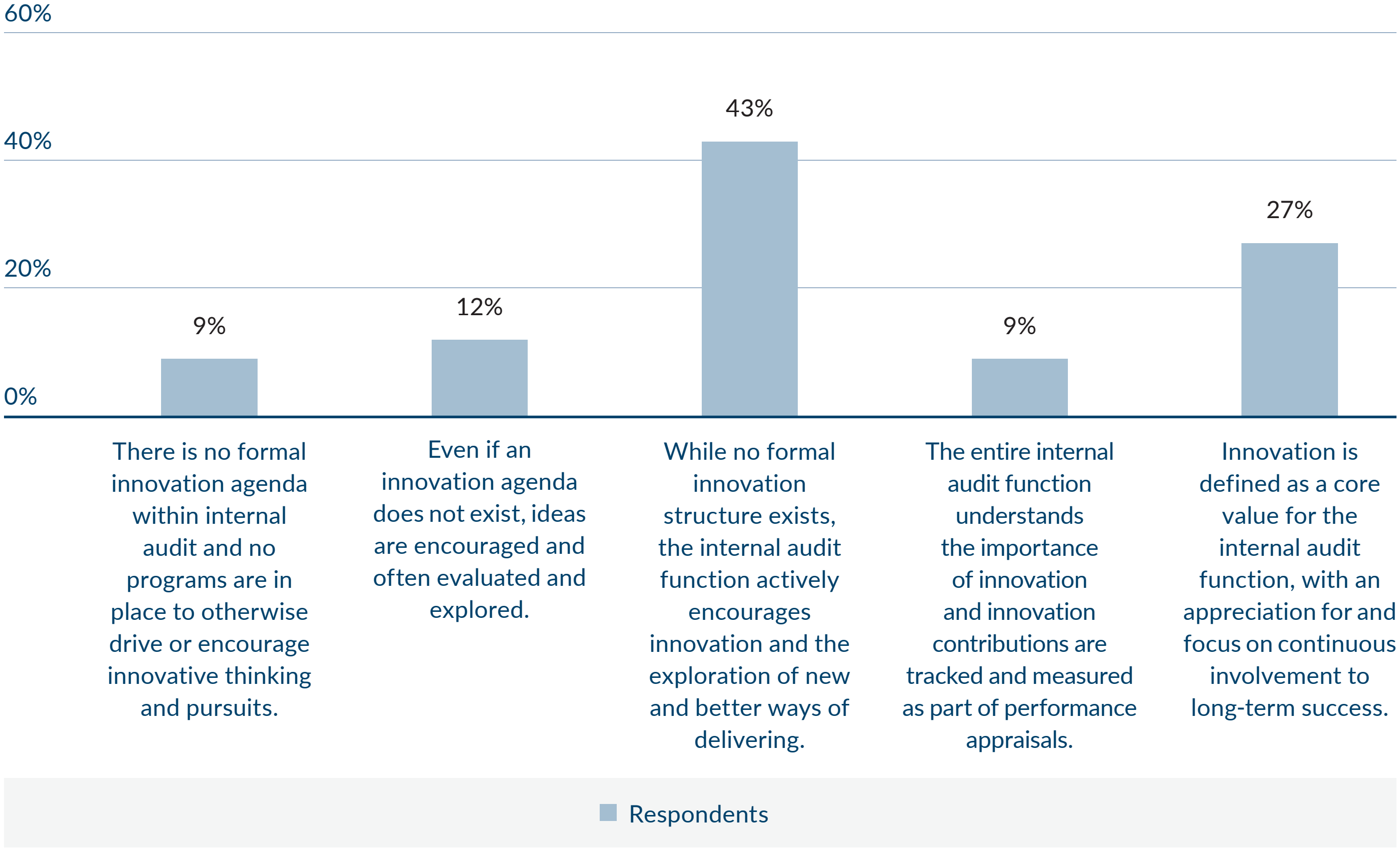
What is the number one next-gen area that you need to audit but will require third-party skills/assistance to do so effectively?



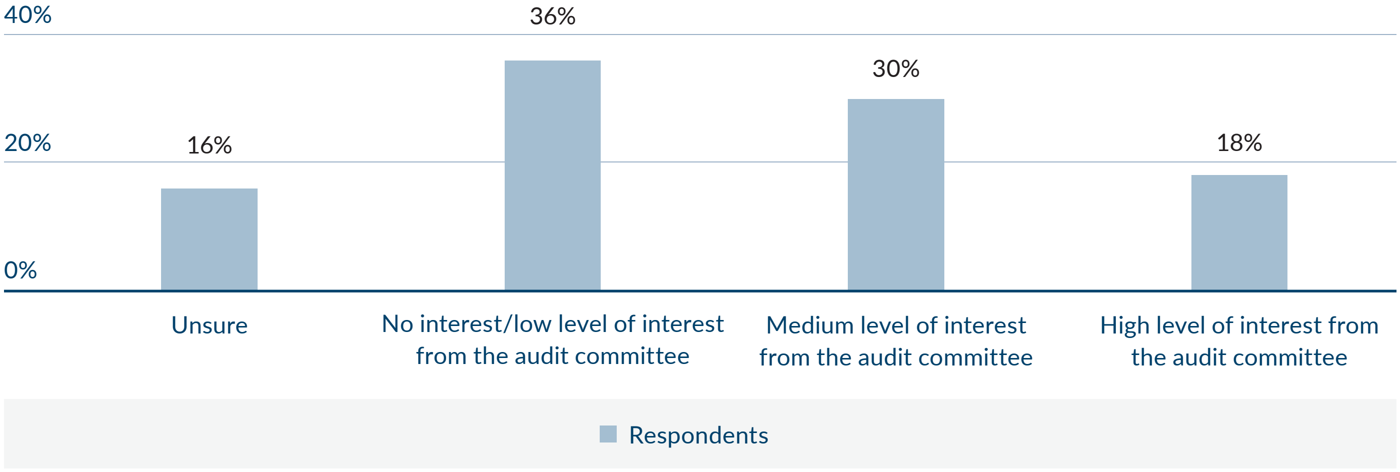
Has your internal audit department completed or is your internal audit department currently undertaking any transformation or innovation initiatives?



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

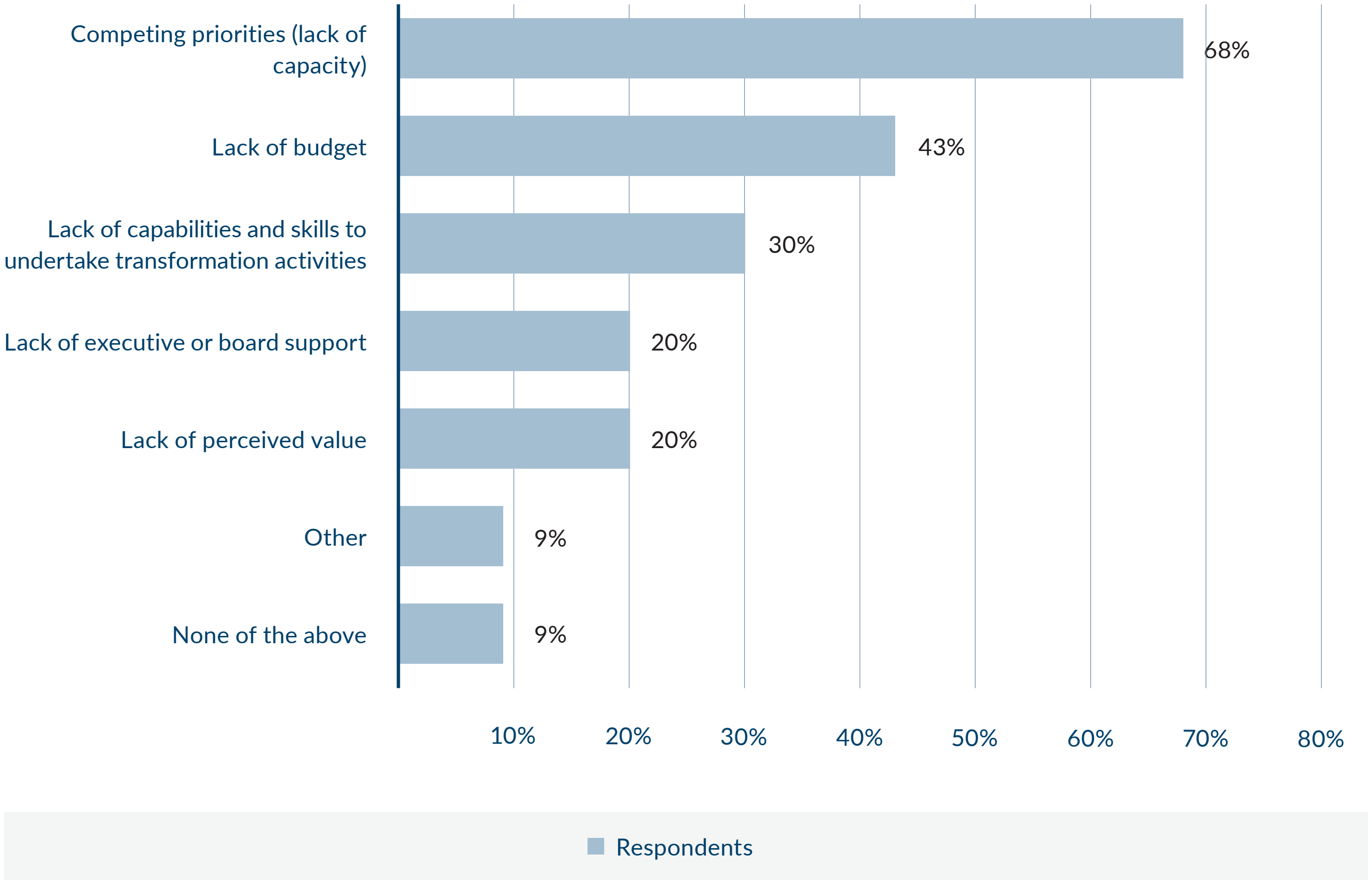


How much interest has the audit committee shown in internal audit's plans to undertake transformation or innovation activities?

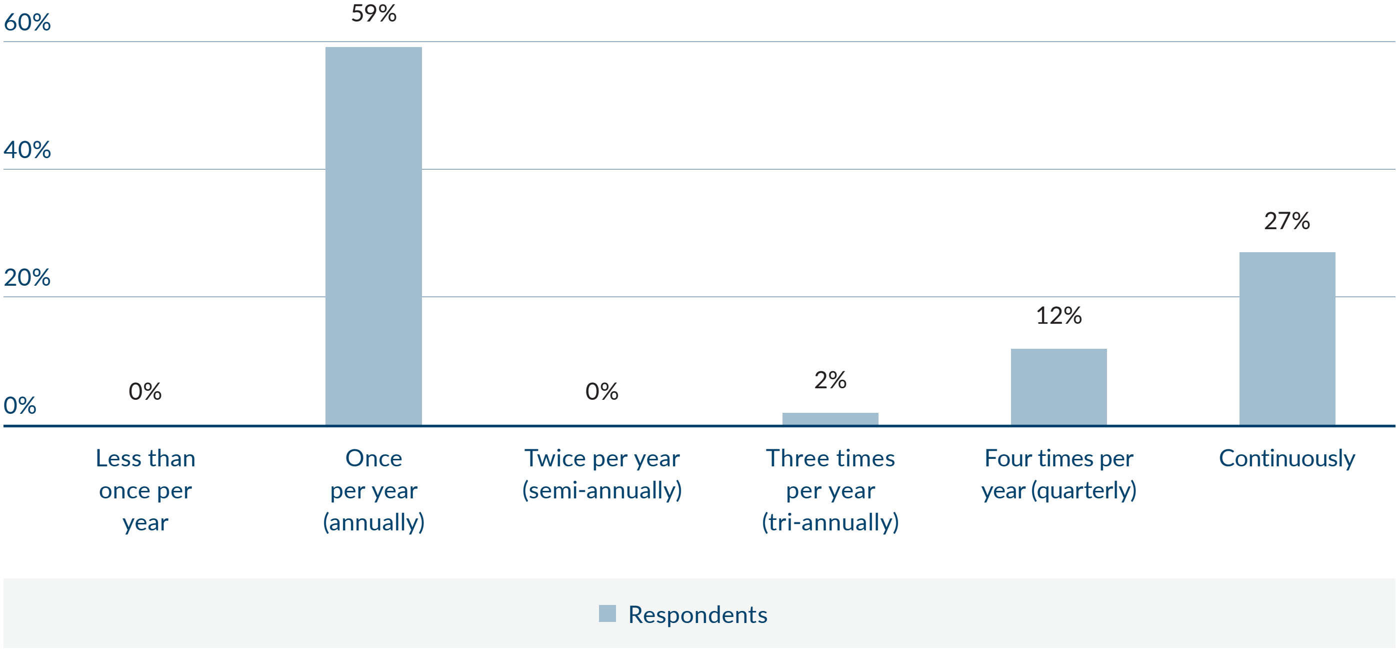


What are the barriers or inhibitors to increased focus on innovation/transformation?

Multiple responses permitted.

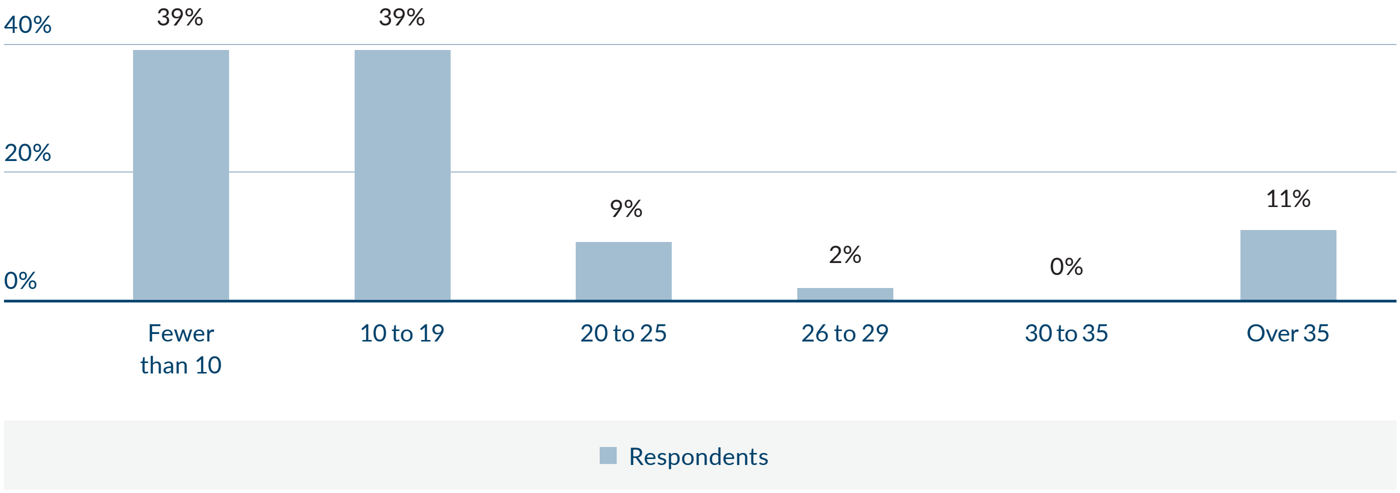


How often is the risk assessment process performed and/or refreshed?

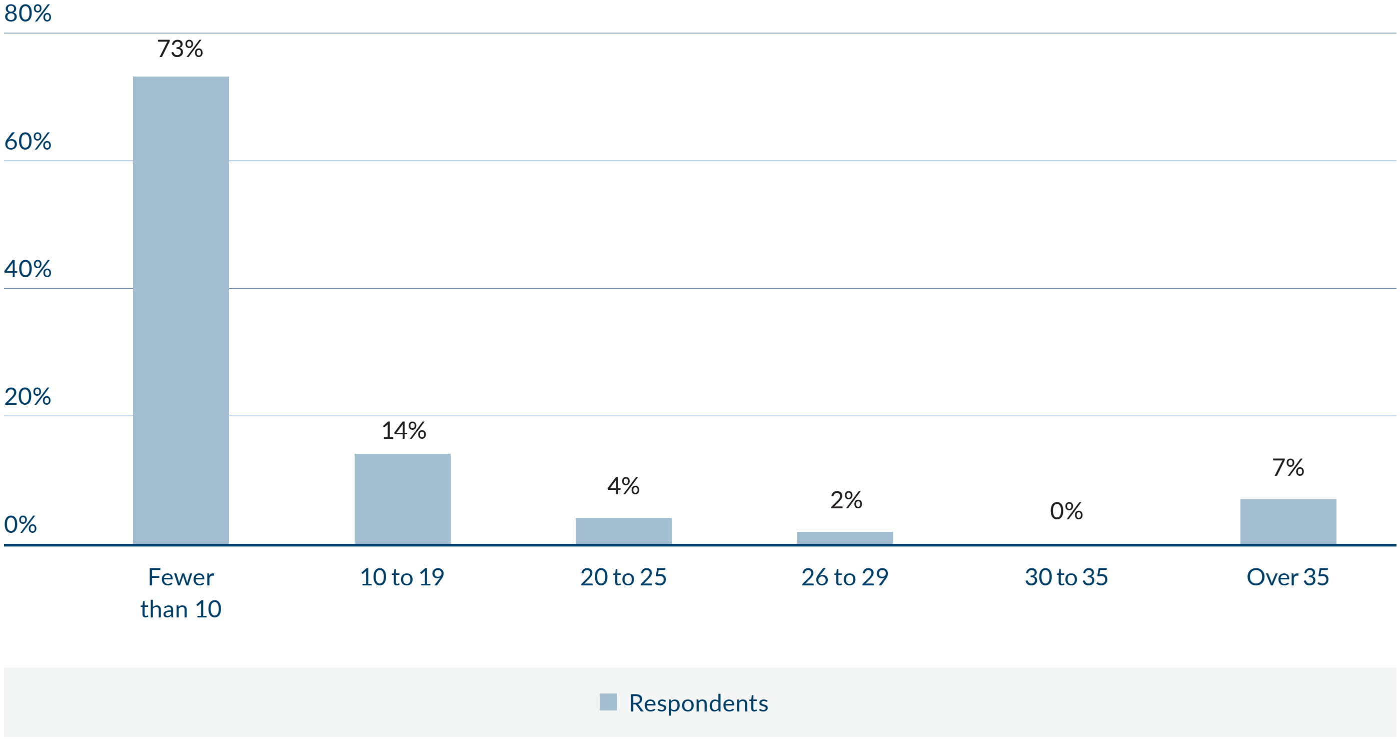


How many internal audits/projects are on the average annual audit plan?

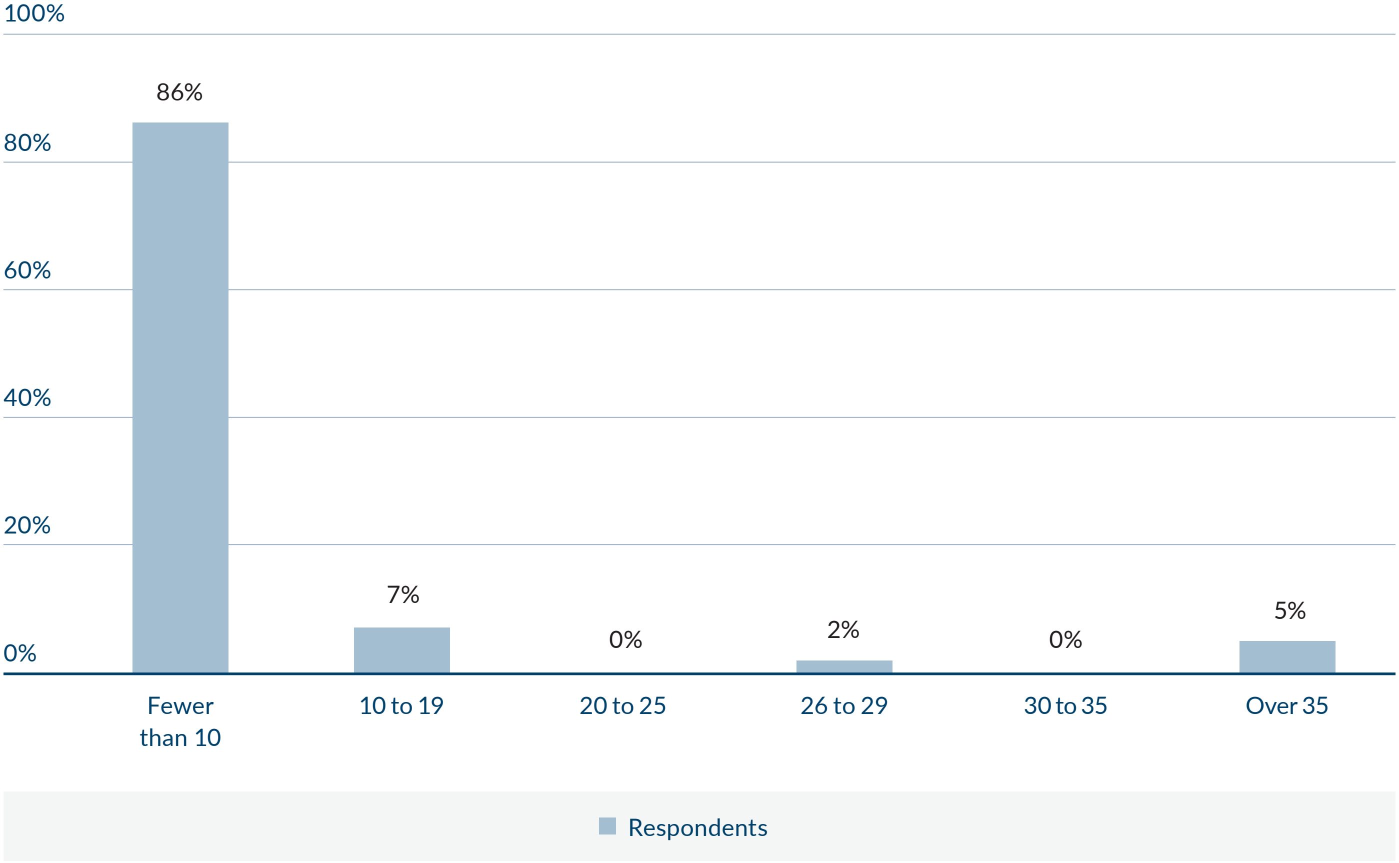
ASSURANCE



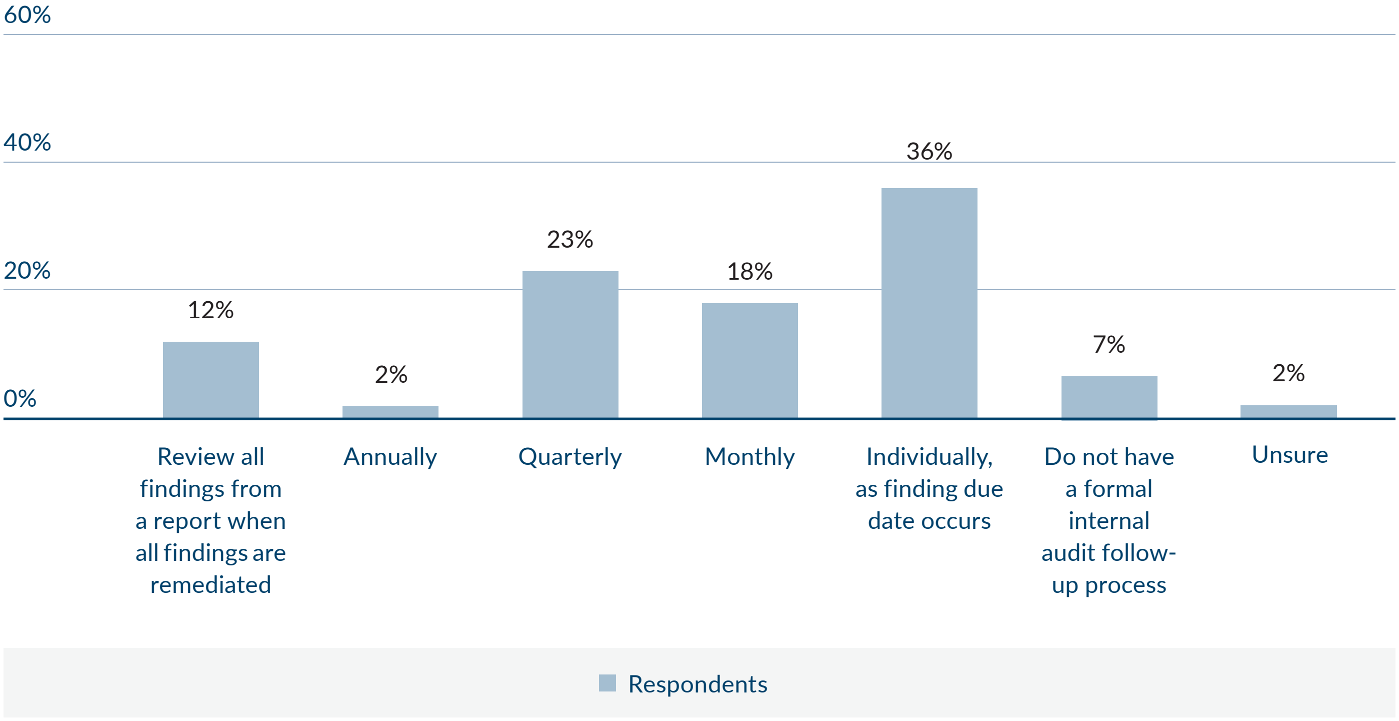
ADVISORY



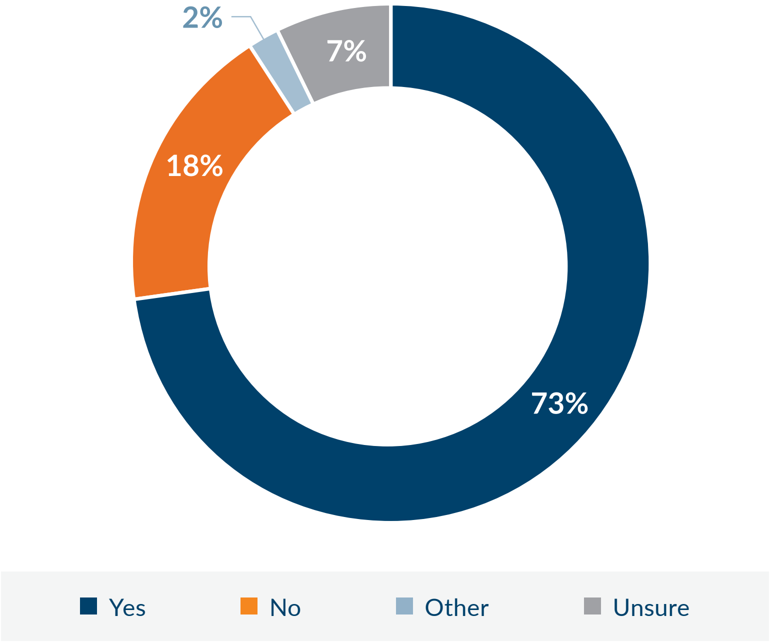
OTHER


100%
80%
60%
40%
20%
0%
86%
7%
0%
2%
0%
5%
Fewer than 10
10 to 19
20 to 25
26 to 29
30 to 35
Over 35
Respondents

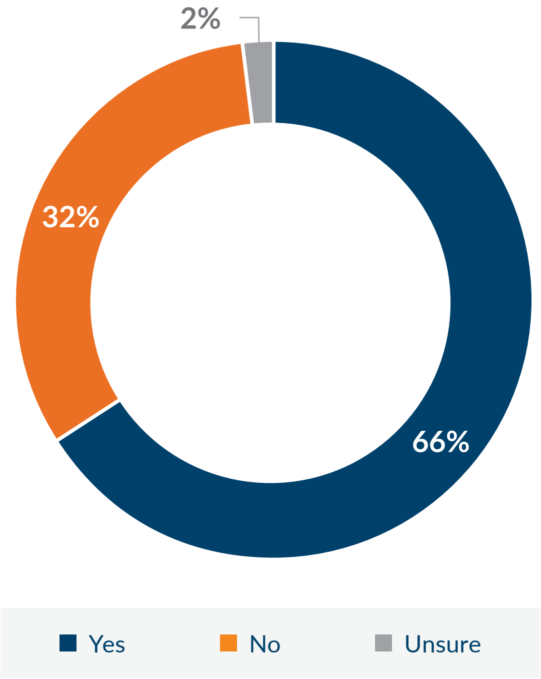
How often do you follow up on outstanding internal audit findings?



Do the internal audit department and compliance department coordinate their risk assessment process and ensure no duplication of work between the internal audit plan and the compliance work plan(s)?

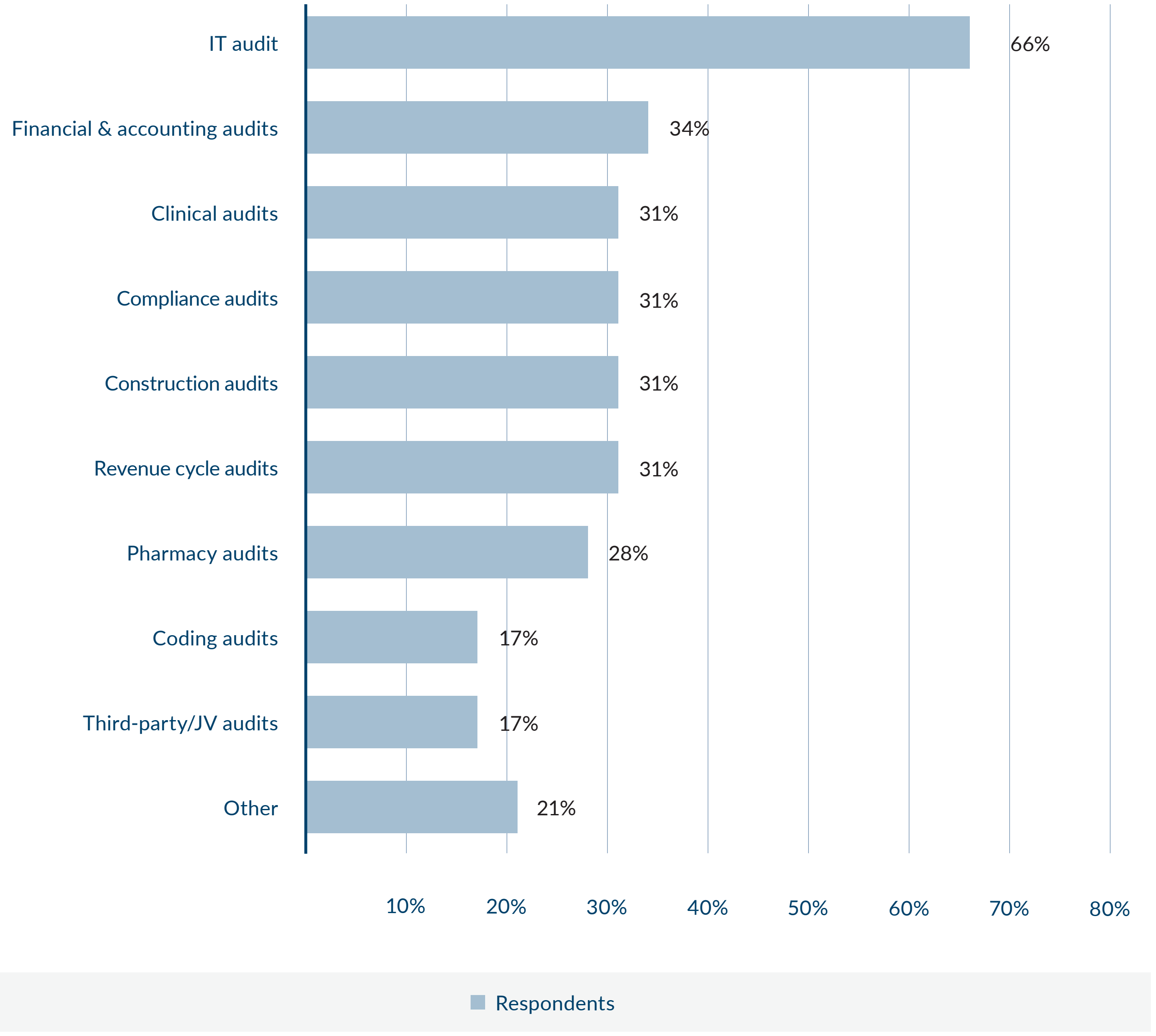


Do you co-source with any strategic partners/third-party vendors to execute the audit plan?

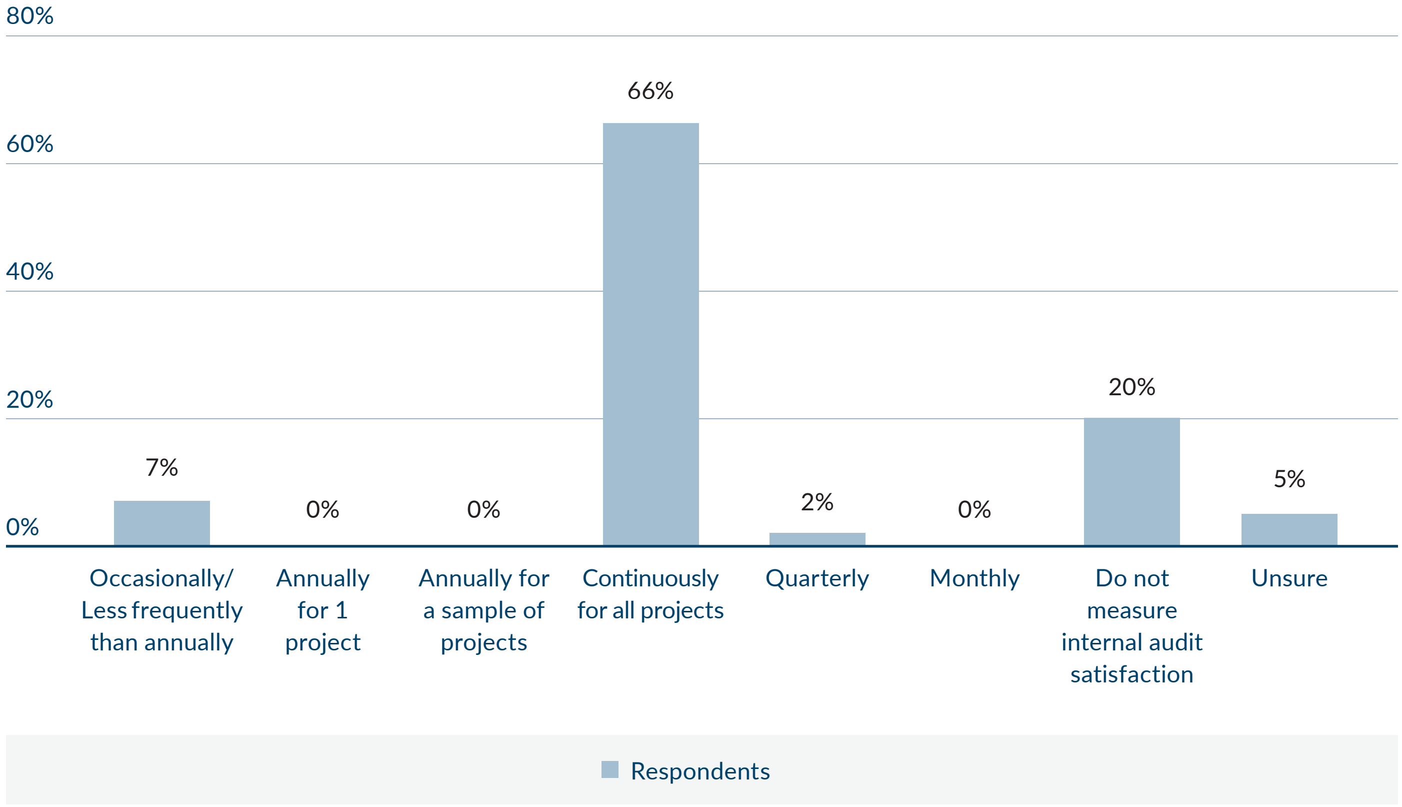


Which areas do you co-source? (Multiple responses permitted.)

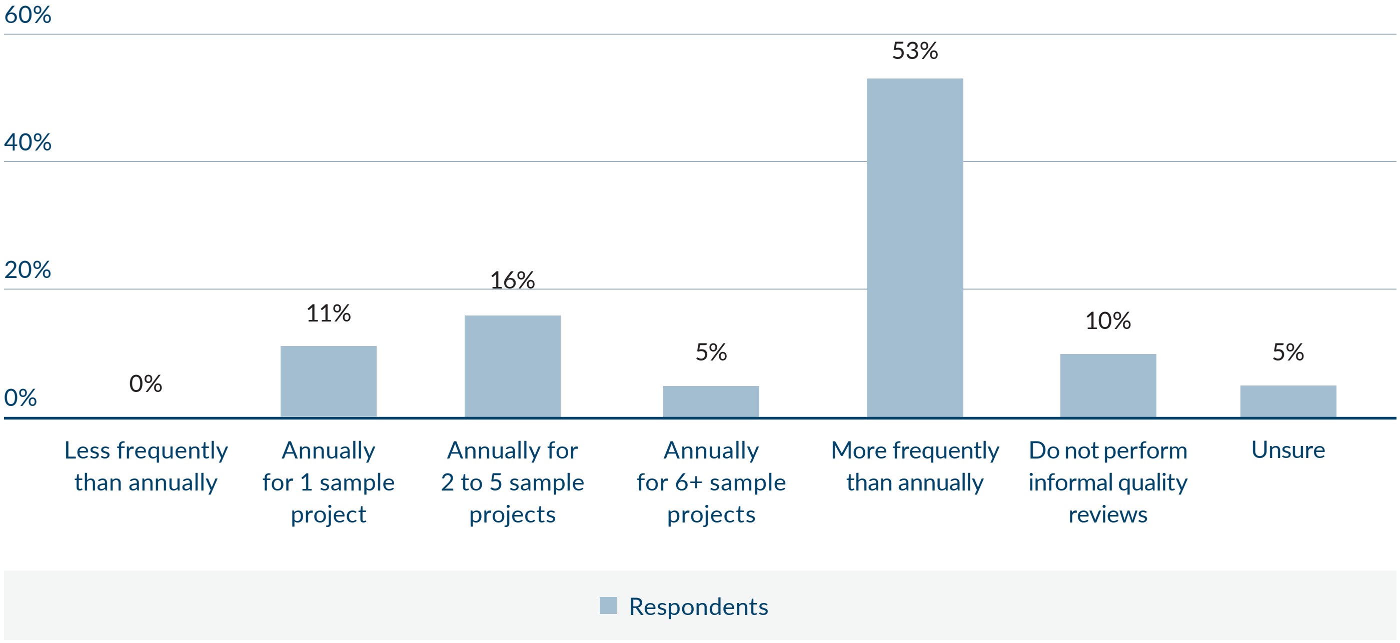
Sample: Respondents whose organizations co-source with strategic partners/third-party vendors to execute the audit plan.



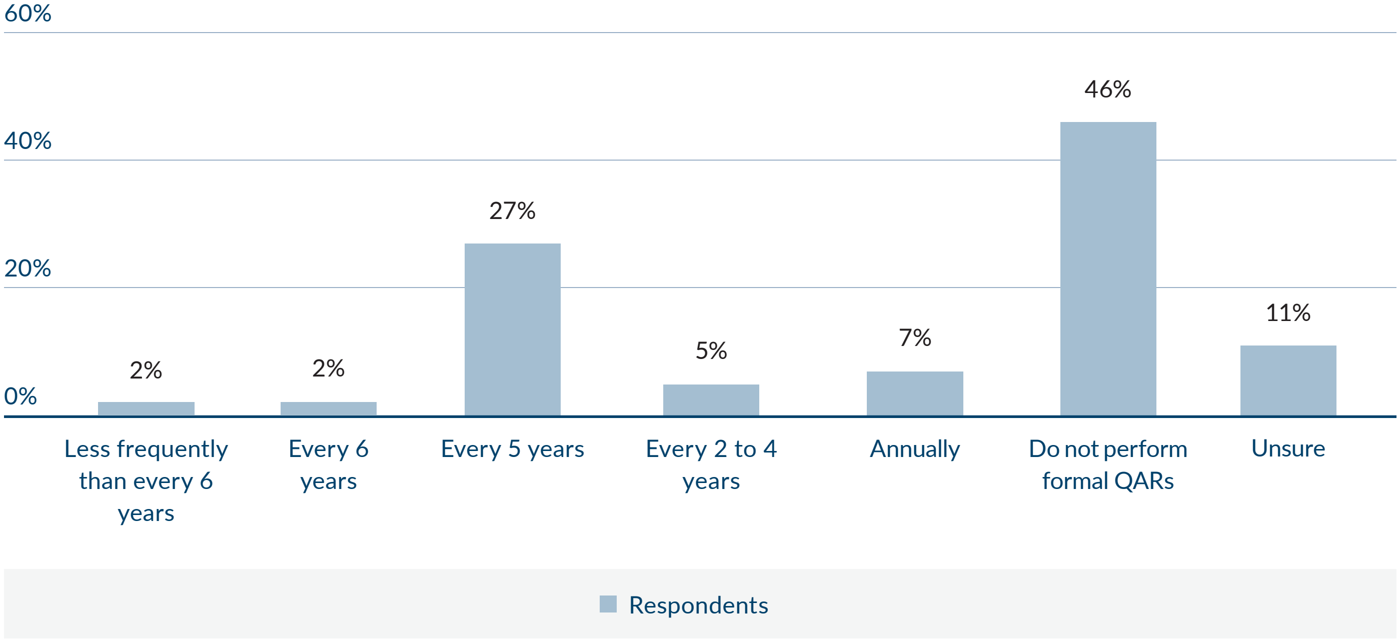
How often do you measure internal audit satisfaction across the organization?



How often do you conduct informal quality reviews for conformance to your organization's/department's standards?



How often do you conduct formal quality assurance reviews (QARs) for conformance to The IIA Standards?



Appendix C: Payer Priorities, Other Key Takeaways and Other Payer Risks to Consider

Top payer priorities for 2022

	2022 Ranking	Yes, on 2022 Audit Plan
User Access Management	01	76%
Fraud Management	02	64%
Finance and Accounting	T03	59%
Internal and External Financial Reporting and Cost Reporting	T03	59%
Privacy and Security of Protected Health or Other Sensitive Information	T03	59%
Accounts Payable	T06	53%
Third-Party and Outsourced Services Risk Management	T06	53%
Compliance Program Effectiveness, Response to Regulatory Changes, and Policy and Procedures Management	T08	41%
Conflict of Interest and Employee, Provider and Vendor Verifications	T08	41%
Data Governance, Data Analytics, Business Intelligence, and Other Data Monitoring/Reporting	T08	41%
Human Resources, Benefits, Compensation and Workforce Challenges	T08	41%
IT Governance	T08	41%

Note: "T" indicates a tie.

Other key takeaways

Looking to 2023

Areas that are not included in the 2022 audit plan but appear to be priorities for 2023 include:

- IT Disaster Recovery
- Business Continuity, Emergency Management, and Pandemic Preparedness/Response
- IT Asset Management
- Digital/Innovation Initiatives
- Employee Time/Expense Reporting and Payroll

Lack of skills and competencies

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

- Changing Delivery Model Across the Care Continuum
- Emerging Technologies (Automation, AI, Predictive Analytics)
- Joint Ventures, Mergers and Acquisitions
- Temporary Staffing, Recruitment and Unions

Key payer risks

Similar to all other healthcare organizations, internal audit functions across the payer landscape are grappling with the challenge of doing more with less while facing increasing risks, including regulatory pressures, margin compressions, data governance, quality concerns, labor shortages, provider reimbursement model changes, payment integrity, member and provider satisfaction, and many more.

Here are some of the top payer-specific risks and why they should be top of mind for healthcare organizations and their audit teams:

01 Accreditation, MAR, ORSA, Medicare FDR oversight, FWA/SIU, telehealth and surprise billing

The evolving regulatory landscape around telehealth and surprise billing, stringent financial and operational requirements, and the potential financial ramifications associated with these topics could lead to significant enterprise risks for health plans. Internal audit plans should consider performing readiness assessments and reviews of relevant processes and controls to evaluate compliance with evolving regulations.

Further, the increased use of telemarketing, social media and call centers to commit healthcare fraud has made payer and provider portals targets of cyber intrusion by bad actors looking to steal and sell patients' protected health information (PHI) on the open market and dark web. Privacy, cybersecurity and targeted fraud prevention audits may help address these evolving risks.

02 Marketing materials, sales commissions and contract bid process

A plan's interaction with members and potential enrollees is a sensitive topic and one that is under growing scrutiny from the DOJ. The CMS revised the Medicare Communications and Marketing Guidelines (MCMG) at the beginning of 2022 to provide plans guidance for ensuring compliance of marketing practices. This includes monitoring and overseeing the activities of subcontractors and downstream entities, including independent agents and brokers that sell Medicare drug and health plans.

Internal audit should consider reviewing the process for ensuring marketing materials are in accordance with MCMG guidelines. Further, the assessment of third-party and agent-broker oversight, sales commissions, and the CMS contract bidding process should be considered to address these risks.

03 Changing delivery models across the care continuum (population health, aging patient population, Accountable Care Organizations (ACO) and value-based contracting)

As the transition to value-based care models continues, changes within health plan operations, including provider contracting, network administration, fee structures and pricing models, will also evolve.

Internal audits can be beneficial for evaluating updated processes and controls and helping the business assess the effectiveness of its contracting approach in achieving these strategic initiatives.

04 Risk score/risk adjustment factor (RAF), Medical Loss Ratio (MLR) calculation, and plan benefit pricing

Accurate risk scores are vital to ensuring plan members receive the care they need, and they're becoming even more important in light of the new CMS and OIG regulations and audit results. Health plan processes for assessing and calculating these scores and ratios can be highly complex.

Internal audit plans should consider operational, financial and regulatory reviews in these areas to ensure key risks are addressed and evolving regulations are considered.

05 Premium billing/collections/reconciliations, state reporting, and financial controls

Financial functions associated with premium billing, collections and reconciliations remain a key financial and business risk area. Combined with ongoing compliance with the Model Audit Rule (MAR), Sarbanes-Oxley (SOX) and other regulatory controls requirements, core financial controls continue to deserve coverage in the internal audit plan.

By using controls testing and results from compliance efforts in operational or financial audits of these areas, internal audit may gain efficiencies and address emerging risks in core financial processes.

06 Encounter claims data integrity and benefit/contract configuration

Annually, health plans face the challenge of properly configuring contracts and benefits into claims processing systems for the coming plan year. Internal audit should focus efforts on the processes and controls operating over the timely and accurate configuration and testing of benefits and contract terms in the claims processing system before implementation in the product environment.

The integrity of encounter claims data being compromised also creates significant risks for a health plan. Aside from the impact that a breakdown in the data can have on the quality of service provided to a member, data integrity issues put the plan at significant financial risk for overpayments and underpayments, regulatory reporting, and much more.

Internal audit should also consider assessing the effectiveness of the payment integrity program, including vendor oversight.

07 Formulary design, supply chain, 340B, rebates, Medication Therapy Management (MTM) programs and virtual-first health benefits

Key risk areas within the pharmacy and PBM space continue to be a focus and are subject to potential regulatory scrutiny. The FTC recently announced an inquiry into the PBM industry to evaluate prior authorizations, pharmacy reimbursements, the impact of manufacturer rebates and fees on formulary design, and more. Compliance audits should focus on assessing practices related to fees and clawbacks, drug formularies, methods to determine pharmacy reimbursements, prior authorizations, and administrative restrictions.

Regarding 340B, covered entities should estimate lost reimbursement from CMS payment cuts, continue self-audits to ensure compliance with program requirements, and perform independent program reviews to verify proper contract pharmacy arrangements and program optimization to ensure all qualified discounts are received.

08 Member engagement, new member data integrity, call center support, member appeals and grievances

Healthcare consumers are becoming more sophisticated, using quality and satisfaction scores to help drive their purchasing decisions. Call centers and appeal and grievance/complaint departments are often the face of the company and set the stage for plan members. Poor member experiences in these areas present reputational risks, increased disenrollment, a drop in Part C & D Star Ratings, and additional scrutiny from the CMS over increased member complaints submitted to the Complaint Tracking Module (CTM).

Internal audit plans should consider the member enrollment process, member data integrity and call center operations. Appeals and grievances also continue to be an area of focus during CMS audits.

09 Provider complaints and appeals, prior authorizations, provider satisfaction surveys and network directory

Health plans are under closer scrutiny for their prior authorization practices, especially in the Medicare Advantage arena. Provider directory accuracy also remains an area of focus, especially given the new No Surprises Act and price transparency guidance enforcing penalties for each incorrect entry.

10 Coordination of benefits (COB), Medicare Secondary Payer (MSP), and pre- and post-pay edits

Processes and controls operating over the coordination of benefits, especially those involving MSP, are critical to claims payment integrity. The configuration and testing of pre- and post-pay edits are also critical to successful claims processing.

Internal audit should consider performing operational reviews of these processes and controls to help ensure claims payment integrity. In areas where pre- and post-pay edits may be more manual and subject to human error, effective processes and controls can help ensure accurate claims processing.

> *"We are very fortunate to have the opportunity to partner with Protiviti on the Healthcare Internal Audit Priorities Survey. The insights derived from the survey results help with our risk assessments and with benchmarking to other organizations. Especially for a small audit shop such as mine, it is helpful to know what others are doing and how we can innovate to be more effective and valued by our hospital system."*

— **Renée W. Jaenicke**
Director of Internal Audit and Compliance
Salinas Valley Memorial Healthcare System
Board Member, Association of Healthcare
Internal Auditors

ABOUT AHIA

The Association of Healthcare Internal Auditors (AHIA) is an international organization dedicated to the advancement of the healthcare internal auditing profession, which includes auditing disciplines such as operational, compliance, clinical/medical, financial and information technology. AHIA was founded in 1981 to provide leadership and advocacy to advance the healthcare internal audit profession by facilitating relevant education, certification, resources and networking opportunities.

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 its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2022 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 Industry Leader
+1.214.395.1662
richard.williams@protiviti.com

Jarod Baccus
Internal Audit Solutions Lead
+1.281.513.9559
jarod.baccus@protiviti.com

Leyla Erkan
Central Region Healthcare Lead
+1.312.213.5606
leyla.erkan@protiviti.com

Bryon Neaman
Northeast Region Healthcare Lead
+1.410.375.7946
bryon.neaman@protiviti.com

Vickie Patterson
Southeast Region Healthcare Lead
+1.813.348.3407
vickie.patterson@protiviti.com

Alex Robison
West Region Healthcare Lead
+1.602.273.8022
alex.robison@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