ahia
Assoc. of Healthcare Internal Auditors

protiviti®
Global Business Consulting

Navigating critical healthcare areas through internal audit

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

Table of Contents

Executive Summary

Coming off several years of a pandemic and the associated public health emergency, the healthcare industry continues to face complex and unpredictable risks in 2024 that could have long-lasting impacts across several critical areas. Healthcare internal auditors play an important role in helping their organisations manage potential risks, stay on top of regulatory compliance, optimise operations and address other pressing concerns.

The latest Healthcare Internal Audit Plan Priorities Study, conducted by Protiviti and the Association of Healthcare Internal Auditors (AHIA), revealed six key areas of focus for internal auditors:

Cybersecurity & IT Governance

Financial Integrity

Fraud Management

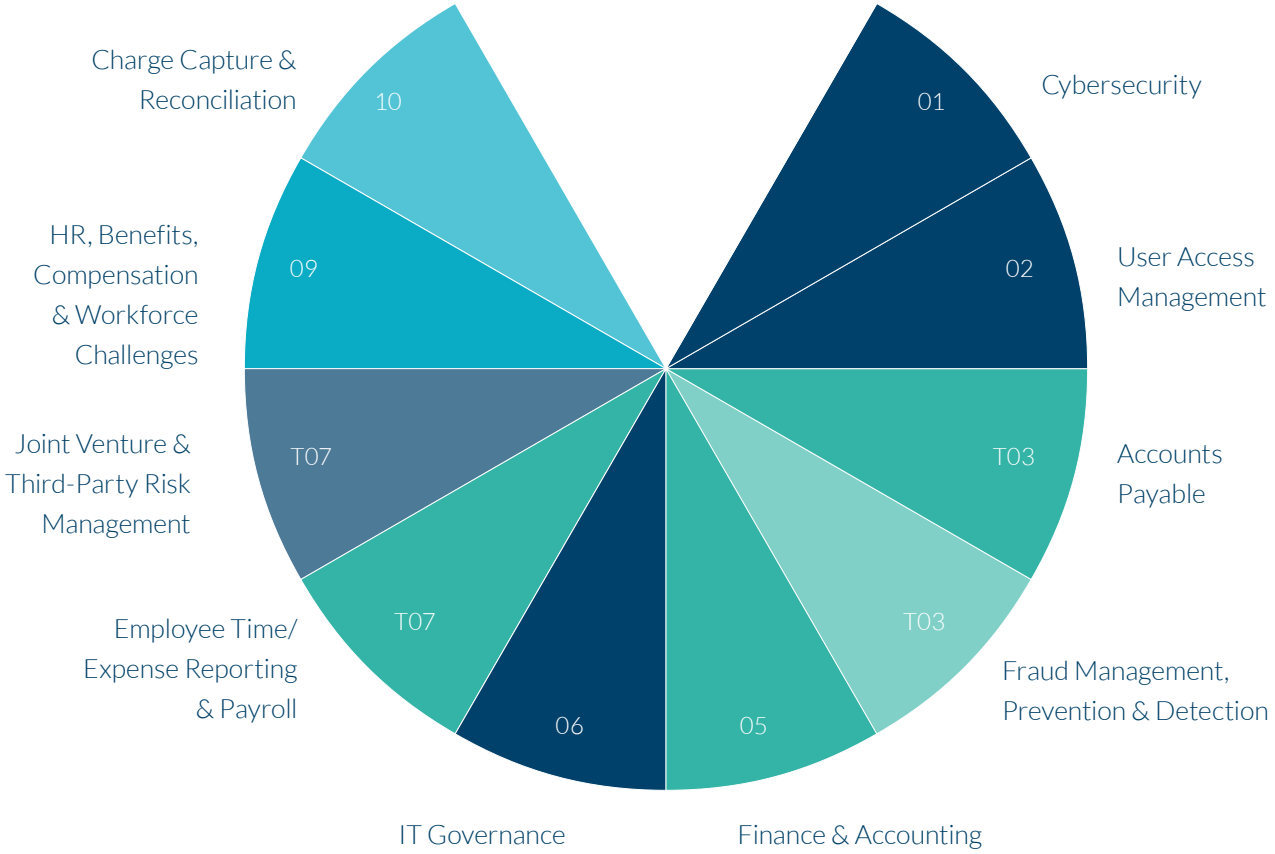
Third-Party Risk Management

Human Resources

Revenue Cycle

Internal Audit Plan Priorities & Key Themes

Top 10 healthcare internal audit plan priorities



Cybersecurity & IT Governance | Financial Integrity | Fraud Management

Third-Party Risk Management | Human Resources | Revenue Cycle

Note: "T" indicates a tie.

From cybersecurity — including the ongoing and rising threat of ransomware attacks — to managing user access and fraud, to helping ensure integrity in financial and IT systems, internal auditors in healthcare organisations face a growing list of priorities that mirrors changes and risks in the industry. Emerging technologies, including but not limited to generative AI, are bringing new opportunities and also elevating risks in these areas as well as with privacy, data and third-party relationships. As they prioritise their audits to encompass these many issues, CAEs must continue to stay focused on achieving high levels of ROI while also serving as effective and relevant business partners for their boards and C-suite leaders as they support organisational performance and growth.

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

Cybersecurity & IT Governance

01 Cybersecurity

Recent high-profile cyberattacks against healthcare organisations underscore an ever-present and evolving threat landscape. It's no surprise that cybersecurity and IT governance continue to top the list of internal audit (IA) priorities in our 2024 study. Other top-ranking priorities include user access management and ensuring robust IT governance.

Key IA focus areas for cybersecurity include:

- **Business resiliency:** Evaluating plans for continuing critical business functions if/when key systems or vendors are unavailable for extended periods
- **Penetration testing and vulnerability management:** Regular scanning across environments, testing the effectiveness of controls through penetration tests and adversary simulations, and tracking remediation of identified issues
- **Incident response:** Establishing a process to identify, respond to and learn from cybersecurity incidents; having a designated response team to react quickly to threats and minimise their impact; and regularly testing the incident response plan to facilitate effectiveness in real-world scenarios

Recent high-profile cyberattacks against healthcare organisations underscore an ever-present and evolving threat landscape.

- **Social engineering awareness:** Expanding beyond phishing campaigns to include awareness of various techniques, preventive measures and proper protocols
- **Control consistency:** Ensuring adherence to organisational standards for IT controls

02 User Access Management

User access management, the second-largest risk to emerge from the study, presents a unique challenge in the healthcare environment due to its complexity: numerous protected health information (PHI) access points, diverse mix of user roles and immediate need of sensitive information due to urgency of patient care. IA departments can improve processes by continually assessing key areas, including:

- **Standard practices:** Verifying whether basic practices are working correctly, including whether access levels match business roles, changes are made only when appropriate approvals are provided, job role changes result in access changes and access is promptly terminated when necessary
- **Dispersed access management:** Evaluating groups responsible for administering access outside of standard IT teams to ensure adherence to established procedures and accurate role performance
- **User access reviews:** Examining frequency and completeness of user access reviews against policy requirements
- **Privileged access management (PAM):** Inspecting processes for identifying and securing accounts with elevated access, including whether additional controls are placed on these accounts where necessary

Cybersecurity is the top-ranked priority for internal audit leaders and teams in healthcare organisations, and nearly three out of four organisations included this on their 2024 audit plan.

06 IT Governance

The study also found IT governance continuing to increase in importance as healthcare organisations embrace emerging technologies like artificial intelligence (AI). Securing these systems and ensuring proper oversight through robust IT governance is a crucial part of mitigating risks and unplanned costs. IA departments can assess related risks by reviewing the following:

- **Strategic alignment:** Determining whether the organisation's IT strategy supports its business goals effectively and enhances performance
- **Value delivery:** Verifying that the organisation is deriving value from its IT investments by reviewing project outcomes or using metrics to measure service effectiveness
- **Risk management:** Examining how well the organisation identifies and/or manages IT-related risks through risk management frameworks, incident response plans, disaster recovery plans and regulatory compliance controls
- **Resource management:** Evaluating how efficiently IT resources are managed, including staff skills development and strategic resource utilisation
- **Performance measurement:** Determining whether the performance of the overall IT function and individual projects are regularly measured against established benchmarks or key performance indicators (KPIs)
- **IT policies and procedures:** Ensuring that policies and procedures clearly outline roles and responsibilities related to information systems and that updates are regularly applied
- **Compliance checks:** Assessing adherence to regulatory standards

Ensuring proper oversight through robust IT governance is a crucial part of mitigating risks and unplanned costs.

Financial Integrity

Financial integrity issues continue to rank in the top 10 priorities for internal audit, with accounts payable (AP) tied for third-highest concern in the 2024 study.

T03 Accounts Payable

Accounts payable departments have key functions and experience disruptive events that merit their consideration for inclusion on internal audit plans. These include changes to the ecosystem due to emerging technologies, fragmentation of people and processes due to trends in outsourcing to external parties, and interruptions such as cyberattacks or other system downtime that prevents payment for goods and services. A solid example is a major cybersecurity incident that occurred in February 2024. This cyberattack created pressure on healthcare-payer accounts payable departments to pay providers quickly, creating processing delays, errors and opportunities for fraud.

IA teams should focus on evaluating and potentially improving processes like vendor setup, invoice processing and invoice payment to help accounts payable operate efficiently and securely, both day-to-day and during critical events.

Accounts payable departments have key functions and experience disruptive events that merit their consideration for inclusion on internal audit plans.

Accounts payable also should be included on the audit plan if there's a high volume of inquiries from vendors about invoices and their related payments or if there's an invoice processing backlog that could point to inefficient or ineffective manual processes. To determine if there is a high volume of inquiries or backlog, AP due diligence should include reviewing inquiry platforms, including email, and performing an ageing of recent activity to assess timeliness of processing and payments.

IA teams should review landmarks to determine whether risks in AP are mitigated through:

- Segregation of duties (SOD) related to vendor creation, invoicing and payment processing
- Governance controls around vendor master setup
- Accurate accounts payable accrual processes and policies

05 Finance & Accounting

Healthcare organisations have a heightened need for reliable and timely financial information due to growing financial demands and reduced margins. Internal audit can collaborate with finance and accounting departments to establish a control environment that facilitates trust in the financial data while not being excessively burdensome.

Key focus areas include:

- **Revenue recognition and reserve estimate accuracy**
  - Determining whether gross revenue accurately reflects the services provided to patients by capturing all charges in the correct period
  - Assessing whether the data used in reserve estimation models are complete and accurate

Internal audit can collaborate with finance and accounting departments to establish a control environment that facilitates trust in the financial data while not being excessively burdensome.

- **Operational costs**
  - Evaluating whether supply pricing aligns with contracted rates
  - Verifying whether only authorised vendors are used for supply purchases, except as may be allowed by policy
  - Determining whether labour productivity standards meet internal and/or industry benchmarks
- **Data integrity**
  - Assessing the accuracy and completeness of data input into the organisation's information systems
  - Evaluating whether effective data management and governance processes are being followed
  - Verifying that effective controls have been established and are maintained to prevent unauthorised data modifications
- **Regulatory compliance**
  - Determining compliance with financial disclosure requirements
  - Assessing adherence to regulations governing insurance, bonds and investments

T07 Employee Time/Expense Reporting & Payroll

As healthcare organisations strive to control costs and provide accurate reporting, employee time/expense reporting and payroll processes and controls are more critical than ever.

Areas ripe for IA's consideration include:

- **Compliance and fraud prevention**
  - Determining adherence to U.S. Department of Labour and state regulations
  - Verifying compliance with shift work, mandatory breaks and overtime regulations, especially during disruptive events that create new demand for skilled labour

As healthcare organisations strive to control costs and provide accurate reporting, employee time/expense reporting and payroll processes and controls are more critical than ever.

- **Accuracy and integrity of data**
  - Assessing payroll calculations and payments accuracy
  - Evaluating data integration and integrity for financial reporting
  - Assessing segregation of duties to mitigate risks
- **Expense management**
  - Evaluating processes for employee expense reimbursements
  - Reviewing corporate credit card and purchasing card transactions
  - Determining compliance (especially with physician-related expenses) with Internal Revenue Service (IRS) guidelines and federal/state laws

One in three healthcare organisations (35%) co-source with a strategic partner or third party to perform financial and accounting audits.

Fraud Management

T03 Fraud Management, Prevention & Detection

Financial losses due to healthcare fraud amount to tens of billions of dollars each year, so it's no surprise that this is tied with accounts payable for respondents' third-highest priority. Risk exposure continues to rise as healthcare organisations face challenges to combat the evolving sophistication, frequency and types of internal and external fraud perpetuated.

Internal audit plays a critical role in fraud management, prevention and detection by helping ensure the accuracy and reliability of a healthcare organisation's financial reporting, compliance with laws and regulations, effectiveness of internal controls, and protection of assets.

Internal audit should consider the following best practices for identification and prevention of fraud:

- Leveraging analytics to proactively identify spikes, anomalies and outliers
- Performing vendor management due diligence to assess compliance with regulations, gaps in controls and alignment with strategic goals

Risk exposure continues to rise as healthcare organisations face challenges to combat the evolving sophistication, frequency and types of internal and external fraud perpetuated.

- Establishing a strong control environment designed to prevent and detect fraud
- Recruiting, screening and hiring staff who are qualified to implement financial policies and procedures and adhere to the code of conduct
- Providing ongoing education and mandatory training on fraud prevention and detection, fraud trends, applicable laws and regulations, and ethics and integrity
- Executing regular risk assessments that consider incentives and drivers of fraud and updating controls as needed
- Implementing a strong whistleblower program to report suspected fraudulent activity
- Checking periodically the List of Excluded Individuals/ Entities (LEIE) maintained by the Office of Inspector General of the Department of Health and Human Services, as well as other exclusion lists, to ensure personnel and/or vendors are not included
- Developing protocols to investigate reported or suspected fraud, taking prompt action and reporting to appropriate stakeholders
- Ensuring the board and any relevant subcommittees are routinely informed of suspected fraud and the controls in place

Internal and third-party fraud could lead to financial loss, fines and penalties, reputational damage, and business disruption. Internal audit is instrumental in developing a strong control environment designed to prevent, detect and remediate fraud.

While fraud management, prevention and detection ranks among the top IA priorities in healthcare, just 57% of providers and 58% of payers included this area on their 2024 audit plans.

Third-Party Risk Management

T07 Joint Ventures & Third-Party Risk Management

Recent events that have crippled many healthcare industry participants have drawn more attention to risks associated with increased reliance on third parties. The February 2024 healthcare cybersecurity incident highlighted the significant impact third-party vendors can have on business continuity. It also exposed categories of third parties that previously might not have been evaluated through vendor risk assessments and the like, such as claims processors and/or clearinghouses.

Internal audit departments may be asked to assess the risk of third parties to their organisation following these high-profile events. IA should confirm that the organisation has completed the following activities and has processes in place to continually update the associated outputs:

- Performing a business impact analysis to identify and determine the criticality of business processes, systems and third parties
- Creating an inventory of the complete list of third parties (including at the parent-company level)

Recent events that have crippled many healthcare industry participants have drawn more attention to risks associated with increased reliance on third parties.

- Completing vendor risk assessments
- Creating business continuity plans

A framework like the Shared Assessments Vendor Risk Management Maturity Model (VRMMM) can also be used to assess the maturity of an organisation's vendor risk management program and benchmark against others in the industry. The framework consists of eight categories that make up a comprehensive program:

1. Program Governance
2. Policies, Standards & Procedures
3. Contract Development, Adherence & Management
4. Vendor Risk Assessment Process
5. Skills & Expertise
6. Communication & Information Sharing
7. Tools, Measurements & Analysis
8. Monitoring & Review

A framework like the Shared Assessments VRMMM can be used to assess the maturity of an organisation's vendor risk management program and benchmark against others in the industry.

Human Resources

09 Human Resources, Benefits, Compensation & Workforce Challenges

According to the 2024 SHRM Talent Trends Report, more than 75% of organisations have had difficulty in the last 12 months recruiting for full-time, regular positions and nearly half have had difficulties retaining these employees. While the percentage of organisations experiencing recruiting difficulties has decreased from a high of 91% in 2022, 47% of Human Resources (HR) professionals say it has been somewhat or much more difficult for their organisation to recruit compared to one year ago. For many organisations, talent (finding it, keeping it and ensuring the business has the best) is an enduring challenge.

Internal audit departments play an important role in ensuring that an organisation's talent function operates effectively and adheres to established policies and regulations. A structured and comprehensive approach to auditing the talent function includes:

- Assessing whether the organisation's recruitment strategies align with its overall business objectives
- Evaluating whether there are robust processes in place for identifying job requirements, sourcing potential candidates, conducting interviews and making hiring decisions

Internal audit departments play an important role in ensuring that an organisation's talent function operates effectively and adheres to established policies and regulations.

- Confirming compliance with laws related to nondiscrimination and data privacy during hiring processes
- Evaluating the effectiveness of partnerships with recruitment agencies and use of digital tools like applicant tracking systems, based on metrics like time-to-hire and quality-of-hire

Auditors need to determine whether talent management initiatives designed to engage and retain employees are being implemented properly. This could include:

- Reviewing performance management systems
- Analysing turnover rates across different departments or roles
- Assessing training and development programs for relevance and impact
- Evaluating rewards and recognition programs for fairness and motivational value

Succession planning is another critical area for auditors, who should assess whether a structured process is in place for identifying high-potential employees, providing them with developmental opportunities and preparing them for leadership roles. Alignment between succession plans and the organisation's long-term strategic goals needs to be evaluated, along with transparency and communication of succession plans.

Internal audit departments can provide valuable assurance on the effectiveness of these operations while also suggesting improvements where needed.

Close to half (47%) of HR professionals say it has been somewhat or much more difficult for their organisation to recruit compared to one year ago, according to the 2024 SHRM Talent Trends Report.

Revenue Cycle

10 Charge Capture & Reconciliation

Hospitals can improve their revenue cycle operations and deliver measurable returns by prioritising compliance and accuracy in the identification, capture, reporting and reconciliation of chargeable items. Ineffective processes lead to poor charge entry, negatively affecting healthcare organisations and resulting in revenue losses.

Regular audits are key to evaluating the effectiveness of charge capture processes. The Healthcare Financial Management Association (HFMA) reports that hospitals lose 1% of net revenue due to charge capture errors, which can lead to increased bad debt, denied claims, contractual disputes and regulatory scrutiny.

A comprehensive approach is beneficial, but healthcare providers should also conduct targeted audits in high-risk areas in which both automated workflows and manual charge entries heighten error risks. Key clinical areas for potential improvement include operating rooms, interventional procedures, medication administration and emergency services.

Regular audits are key to evaluating the effectiveness of charge capture processes.

Internal audit can leverage data analytics to uncover charge entry delays and discrepancies such as overlooked high-cost supplies and inconsistencies in coding between facility and professional services. This analytical approach helps auditors prioritise departments for review based on potential revenue impact and operational shortcomings.

Inaccurate charge entries carry significant financial and compliance risks. Establishing robust policies and comprehensive monitoring processes is essential for ensuring compliance, minimising rework that inflates costs and diminishes productivity, and ultimately enhancing net revenue.

A majority of internal audit functions in healthcare provider organisations (63%) included charge capture and reconciliation on their 2024 audit plans.

Additional Observations

Areas that are not included in the top 2024 audit plan priorities but appear to be priorities for 2025 include:

- Data governance, analytics & monitoring/reporting
- Billing accuracy & accounts receivable
- Supply chain
- Privacy
- EHR/ERP implementation & optimisation

The Bottom Line

Healthcare organisations will continue to face disruptions that will impact the bottom line and draw focus away from providing the highest-quality patient care. Regardless of what challenges are ahead, IA plays a key role in helping organisations safeguard against risk and address their most urgent issues, while successfully navigating the complex changes that are inherent to our industry.

Appendix A: Provider-Specific Priorities, Other Observations & Key Risks to Consider

Top Provider Internal Audit Plan Priorities

	2024 ranking	Percentage on 2024 audit plan
Cybersecurity	01	74%
User Access Management	02	66%
Charge Capture & Reconciliation	03	63%
Accounts Payable	04	62%
Employee Time/Expense Reporting & Payroll	05	60%
Billing Accuracy & Accounts Receivable	T06	57%
Fraud Management, Prevention & Detection	T06	57%
Pharmacy Operations & Drug Management	T06	57%
Finance & Accounting	T09	55%
IT Governance	T09	55%
Supply Chain	T09	55%

Other Observations: Providers

Areas that are not included in the top 2024 audit plan priorities but appear to be priorities for providers for 2025 include:

- Data governance, analytics & monitoring/reporting
- Capital spending, projects & construction
- Employee, provider & vendor verifications
- Privacy
- Emerging technologies

Key Provider-Specific Risks to Consider

Following are some top provider-specific priorities and why they should be top of mind for providers and their audit teams.

01 Billing Accuracy & Accounts Receivable

Hospital internal audit departments should focus on several key areas related to billing accuracy and accounts receivable to ensure compliance and efficiency, including:

- Billing accuracy
- Accounts receivable collections
- Cash application
- Denials and charity care
- Underpayments and overpayments/refunds
- Payer contract management
- No Surprises Act and Hospital Price Transparency Rule compliance

Analytics can be applied to identify trends in denials, underpayments and overpayments/refunds, as well as to monitor compliance with the No Surprises Act and the Hospital Price Transparency Rule.

Key provider-specific risks to consider:

- Billing accuracy & accounts receivable
- Pharmacy operations & drug management
- Physician arrangements
- Chargemaster & pricing
- Patient access

02 Pharmacy Operations and Drug Management

Recent federal and state activity is proving that the need for oversight and monitoring in the healthcare drug and pharmacy arena is as important as ever. The Federal Trade Commission (FTC) released an interim report of its three-year investigation into pharmacies and pharmacy benefits managers (PBMs) for alleged illegal business practices. The Department of Justice (DOJ) held a hospital system liable for failing to properly supervise its employees' prescribing practices. And state lawmakers are compelling drugmakers to extend 340B program discounts to contract pharmacies. IA departments auditing the risks associated with drug and pharmacy operations should focus on several key areas due to the potential risk of loss of revenue, fines, and reputational and patient harm:

- 340B retail pharmacy monitoring
- Medication reconciliation
- Drug diversion
- Inventory management
- Medication billing

03 Physician Arrangements

According to Becker's Healthcare, the DOJ is intensifying its focus on Stark Law enforcement and subsequently is seeing more complaints-in-intervention and Stark-related settlements. Additionally, the Centers for Medicare & Medicaid Services (CMS) Stark-related settlement amounts increased by a factor of 5.5 from 2021 to 2023. Because of this increase in enforcement, this area likely poses greater risk today than most organisations realise.

Important considerations for IA include:

- If your physicians have undisclosed or unmanaged financial relationships with physician-owned distributorships (PODs), financial and patient care risks can emerge. IA teams should audit annual conflict of interest forms and CMS's Open Payments Database payments to identify potential POD relationships.

- Unless a specific safe harbour or exception applies, the Stark Law prohibits physicians and other healthcare professionals from referring their Medicare and Medicaid patients to other entities for designated health services if they (or an immediate family member) have any financial relationship to the entity referred. IA teams should audit physician arrangements (and leases) for fair market value (FMV) and commercial reasonableness assessments to ensure alignment with market guidelines.
- The Anti-Kickback Statute prohibits entities from paying a physician in exchange for a referral. IA teams should audit the organisation's expenses to determine whether inappropriate gifts or entertainment are being provided to its referral sources.
- Stacked physician agreements are multiple contracts with the same physician that pay individually compliant rates but, when combined, the aggregate payment/hour total is no longer compliant. IA teams should audit the combination of a physician's arrangements for alignment with FMV individually and holistically. Additionally, physicians with multiple arrangements should have payments audited for services and payments that may overlap or be concurrent (e.g., on call for separate services at the same time), resulting in potential duplication and inappropriate stacking payments.

IA teams should audit the combination of a physician's arrangements for alignment with fair market value individually and holistically.

04 Chargemaster & Pricing

Risk considerations related to charge description master (CDM) address the accuracy, maintenance and pricing within a hospital setting. Internal audit departments should concentrate on several critical areas to maintain regulatory compliance and financial integrity:

- CDM accuracy
- CDM maintenance
- Pricing updates
- Charge capture rates
- Pricing discrepancies
- Reimbursement impact

By focusing on these key areas, objectives and attributes, internal audit departments can help hospitals uphold accurate billing practices, enhance revenue cycle performance, and mitigate risks associated with CDM accuracy, maintenance and pricing. Analytics can assist with assessing charge capture rates, identifying trends in pricing discrepancies, and monitoring the impact of CDM updates on reimbursement rates and revenue.

05 Patient Access

Patient access functions within a hospital present risks in key areas that can impact operational efficiency, compliance and positive patient experiences. Internal audit departments can help hospitals streamline patient access processes, enhance revenue cycle efficiency and improve overall patient satisfaction. Attributes that should be tested during audits in patient access may include:

- Scheduling accuracy
- Admission/registration compliance
- Insurance verification/authorisation
- Consent processes
- Patient wait times
- Data accuracy

Analytics can be beneficial in analysing registration error rates, monitoring insurance authorisation turnaround times, tracking patient wait times and identifying opportunities for process improvements.

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

Top Payer Internal Audit Plan Priorities

	2024 ranking	Percentage on 2024 audit plan
Claims Processing	01	89%
Providers/Network Management & Relations	02	78%
Cybersecurity	03	75%
Finance & Accounting	T04	67%
User Access Management	T04	67%
EHR/ERP Implementation & Optimisation	T06	58%
Fraud Management, Prevention & Detection	T06	58%
IT Governance	T06	58%
Joint Venture & Third-Party Risk Management	T06	58%
Members	T10	56%
Sales & Marketing	T10	56%

Other Observations: Payers

Areas that are not included in the 2024 audit plan but appear to be priorities for payers for 2025 include:

- Compliance/regulatory
- State reporting, CMS financial audits, capital adequacy & actuarial
- Pharmacy/PBM
- Internal/external financial reporting & cost reporting
- Business continuity, emergency management & pandemic preparedness/response

Key Payer-Specific Risks to Consider

Following are some top payer-specific priorities and why they should be top of mind for payers and their audit teams:

01 Claims Processing

With U.S. healthcare spending projected to grow from $4.8 trillion in 2023 to $7.7 trillion by 2032, claims processing/adjudication continues to be a critical area for payers. To mitigate financial loss, maintain regulatory compliance and uphold the trust of members and providers, it's crucial to use detailed auditing techniques and data analytics diligently. While automated adjudication boosts efficiency and cuts costs, improper implementation and lack of ongoing maintenance can cause expensive systemic errors. Eliminating upfront configuration errors (e.g., provider contracts, benefit coverage, fee schedules, etc.) helps streamline downstream processes and increase customer satisfaction. Real-time monitoring via dashboards aids in identifying bottlenecks and ensuring timely processing per regulatory requirements.

Key payer-specific risks to consider:

- Claims processing
- Providers/network management & relations
- Members
- Sales & marketing

Claims payment integrity necessitates collaboration across the enterprise with proactive measures such as vendor integration, partnership with the special investigation unit (SIU) and current fraud detection/prevention mechanisms. However, maintaining alignment across all stakeholders is challenging, often leading to overlapping services and waste.

Finally, claims audits, next-generation analytics and pre/post-payment edits not only help drive leading claims processing practices, but they also address growing complexities and concerns around correct member deductibles, co-pays, cost share, coordination of benefits, etc., as well as provider reimbursement.

Claims payment integrity necessitates collaboration across the enterprise with proactive measures such as vendor integration, partnership with the SIU and current fraud detection/prevention mechanisms.

02 Providers/Network Management & Relations

Given the evolving regulatory landscape and heightened scrutiny on healthcare compliance, provider credentialing processes must meticulously verify qualifications and comply with updated licencing requirements mandated by regulatory bodies. Continuous contract review is crucial to align with new healthcare laws, covering payment models, reimbursement rates and contractual obligations, to mitigate legal risks and ensure financial transparency within provider networks.

Analysing fee schedules is essential to confirm alignment with current Medicare or Medicaid reimbursement rates and address regulatory directives on cost containment. Adapting performance monitoring frameworks to integrate new quality metrics and reporting requirements mandated by regulatory agencies ensures providers adhere to clinical guidelines, enhance patient outcomes and maintain consistent care standards.

Enhanced transparency in provider relations, including disclosures of conflicts of interest and financial relationships under new laws or guidelines, is increasingly mandated. Upholding integrity in provider interactions and ensuring compliance with evolving regulatory standards are critical for effective management of provider and network operations amid dynamic regulatory environments.

03 Members

The focus on member experience remains a vital concern with a rise in legislative reform and scrutiny around utilisation management. CMS has implemented new rules to streamline the prior-authorisation process and increase transparency. These regulations mandate quicker processing times for requests and require health plans to provide metrics and specific denial rationale. Over 90 reform bills across 30 states show a nationwide focus on this movement toward enhancing patient access while reducing administrative complexity.

Denials management remains crucial as denial rates continue to rise due to stricter authorisations and coding inaccuracies. Proper audit measures should be implemented to ensure that denials are continuously monitored and instances of error are managed to avoid member abrasion.

Star Ratings related to member satisfaction play a crucial role in the evaluation of health plan payers, with at least 33% of Star Ratings based on the member experience performance of a contract. Higher Star Ratings are strongly associated with better member satisfaction scores, suggesting that improving service quality by providing flexible communication channels and continuous support, ensuring quick issue resolution, and offering personalised experiences contribute to a better member experience. Enrollment experience is also critical to both attracting new members and retaining existing ones. Errors or delays can lead to decreased satisfaction, potential disenrollment and regulatory scrutiny.

04 Sales and Marketing

The landscape of sales and marketing for Medicare Advantage is evolving rapidly with new regulations such as the CMS 2024 and 2025 Final Rules. CMS continues to focus on beneficiary protections, including around sales and marketing, especially as Medicare Advantage plans have grown to cover more than half of the Medicare-eligible population.

A key sales aspect of these rules is ensuring that advertising is clear and plan-specific and is not misleading. Additionally, new agent and broker compensation regulations setting a clear, fixed payment amount will reduce loopholes that can result in anti-competitive and anti-consumer steering incentives for plans which may not align with members' best interests.

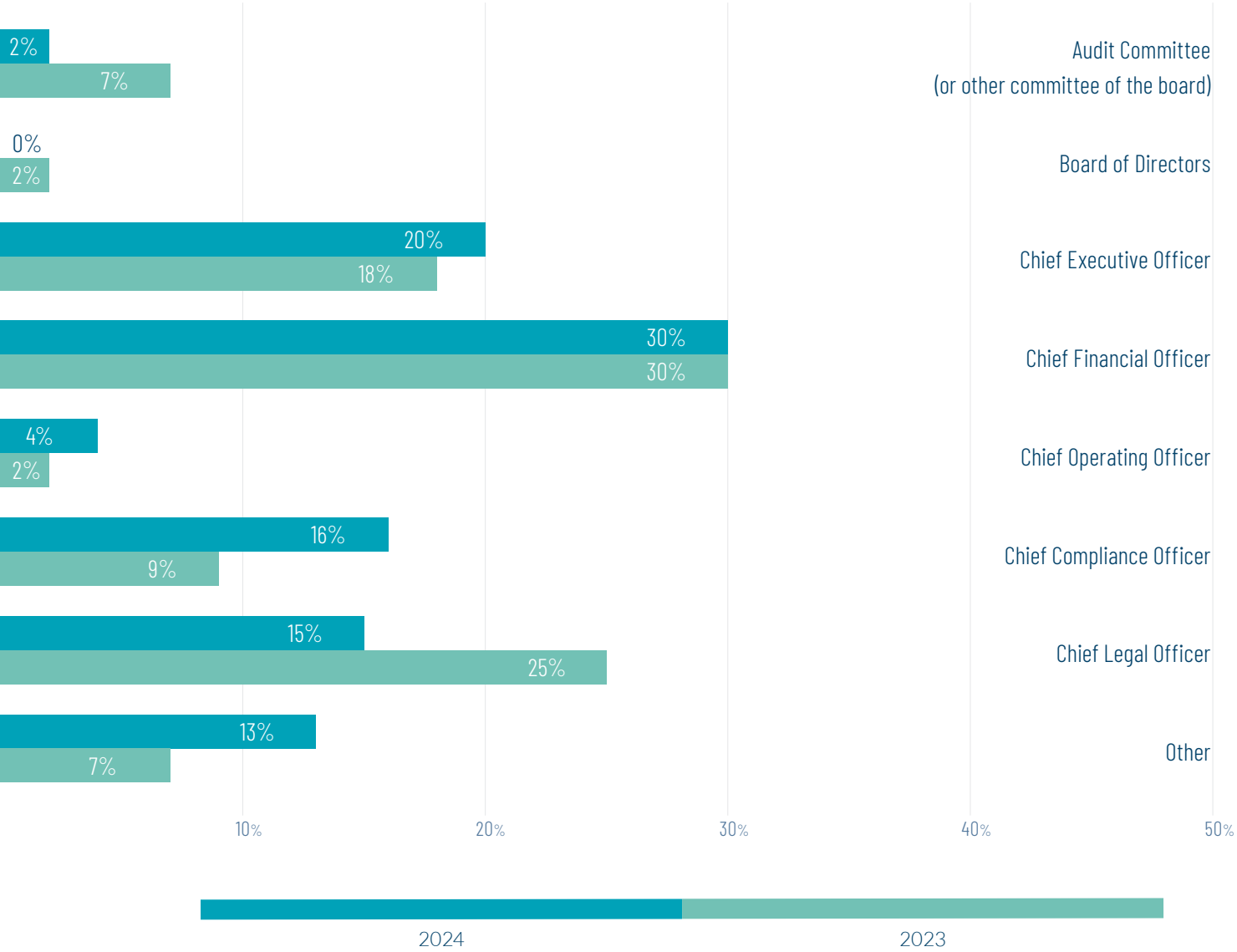
CMS is also requiring transparency around the use of utilisation management criteria and committee makeup, including posting information to be publicly available on the plan's website.

Under these new regulations, there's a clear emphasis on consumer protections and maintaining fair competition. Failure to comply could result in severe penalties, damaging both reputation and financial stability. Plans should conduct regular oversight to monitor agent and broker activity and the plan's commission payments, and to ensure members receive accurate information about their coverage.

Appendix C: Additional Healthcare Study Insights

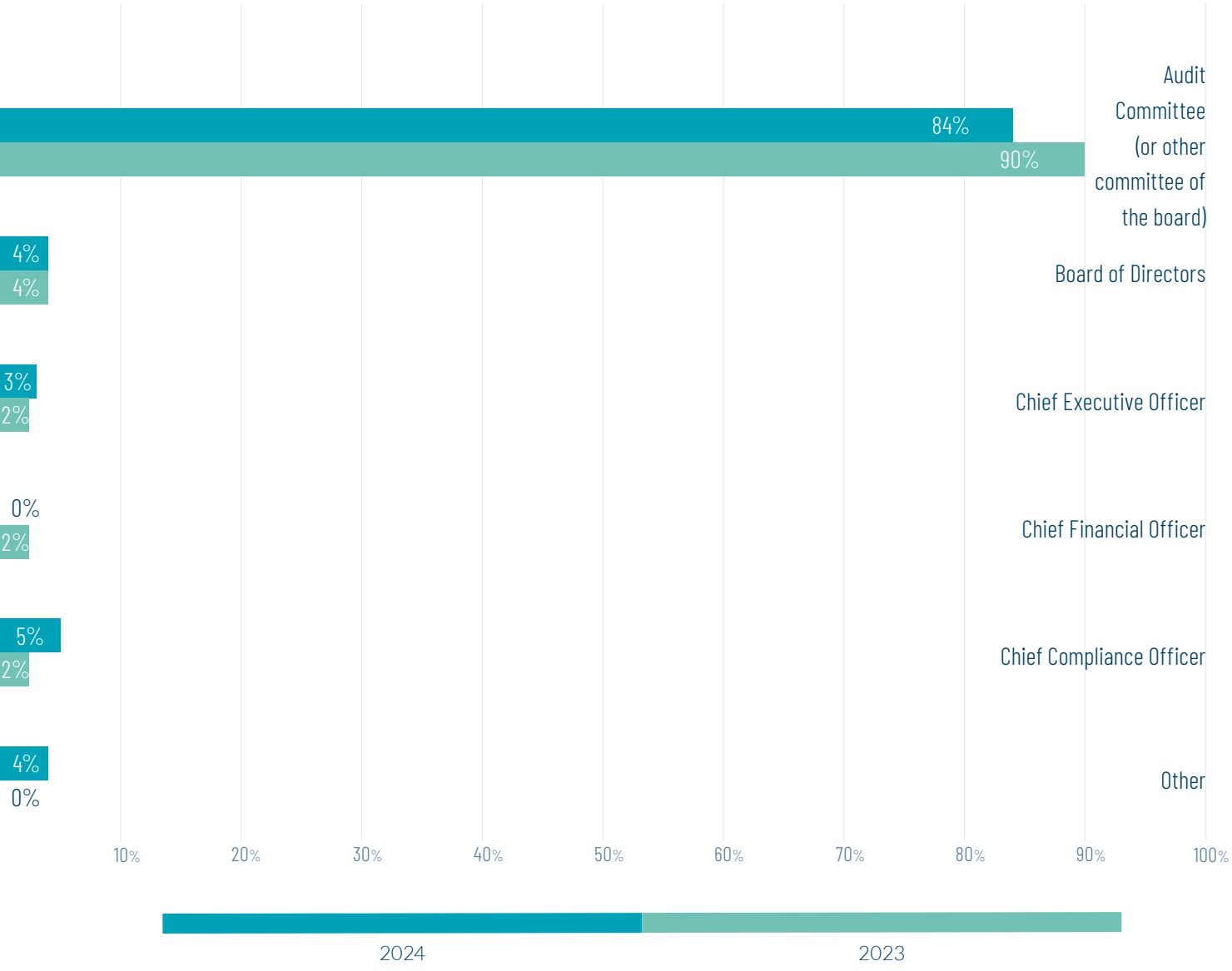
Who does the internal audit function report to?

Administratively (day-to-day)

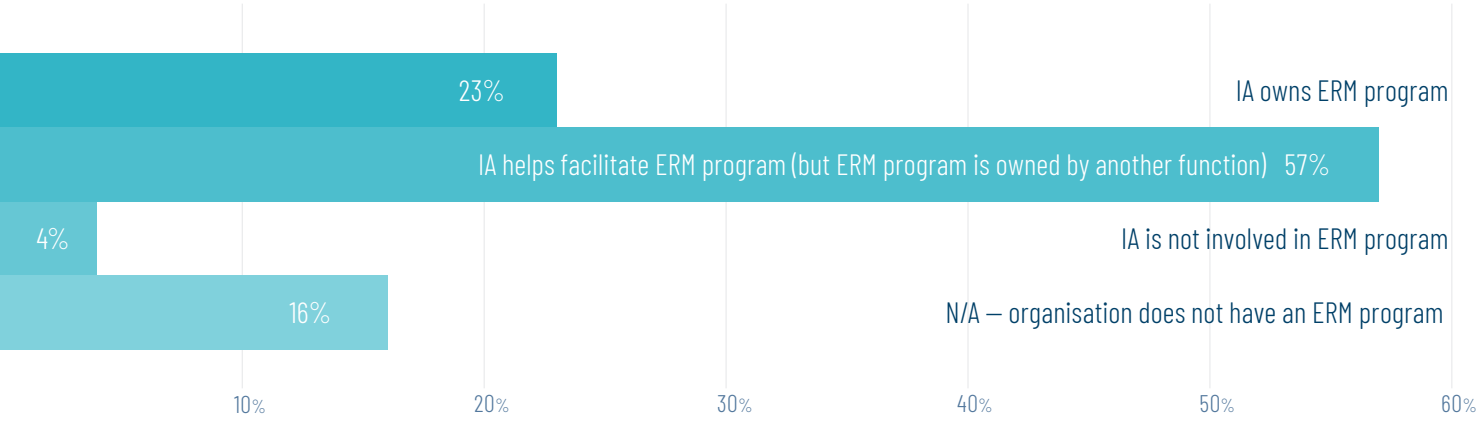


Who does the internal audit function report to?

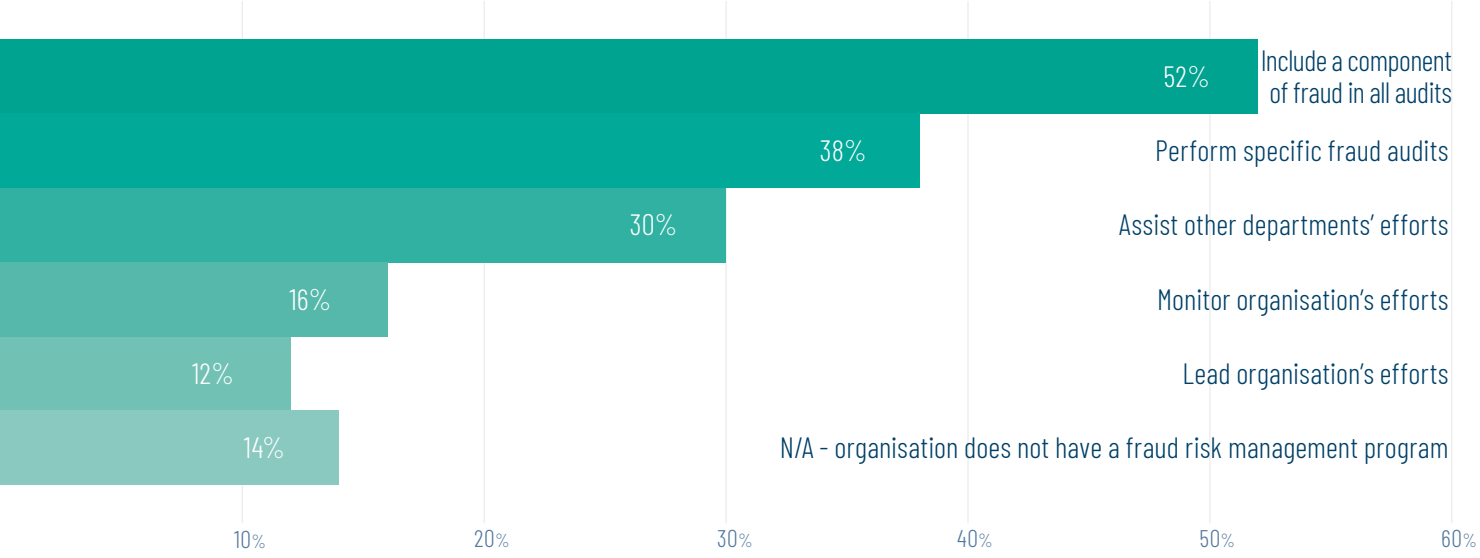
Functionally



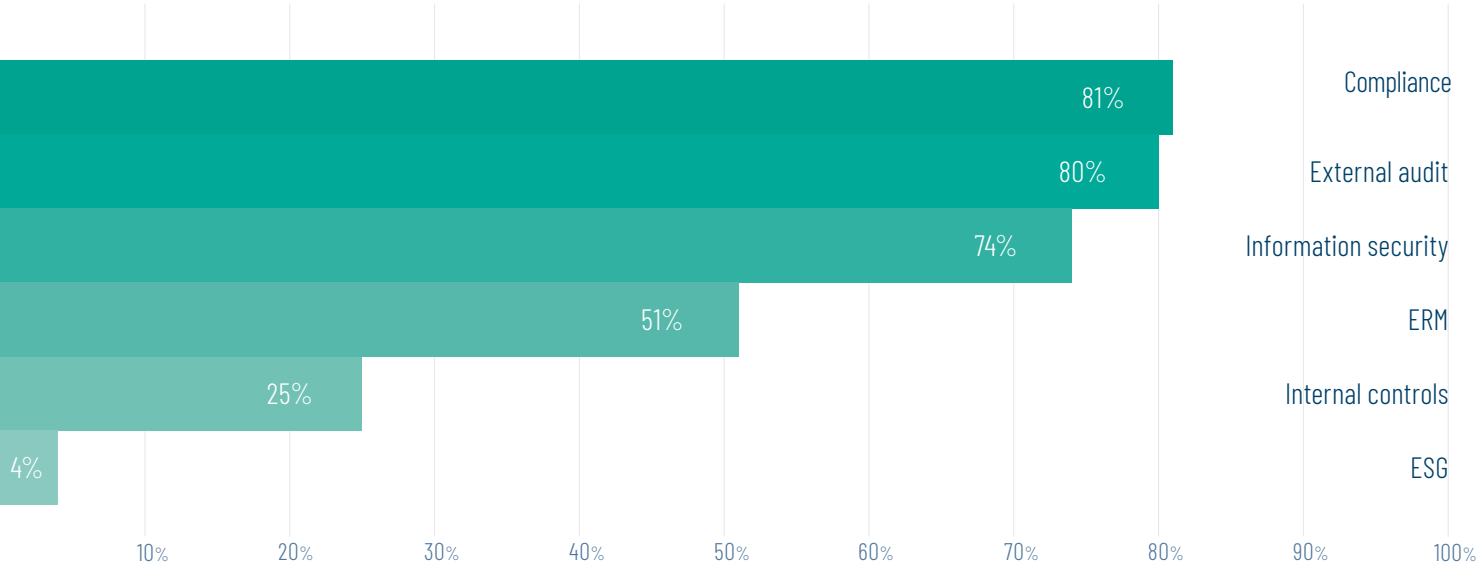
What role, if any, does internal audit play in your organisation's Enterprise Risk Management (ERM) process?



What role, if any, does internal audit play in your organisation's fraud risk management process? *Multiple responses permitted.*

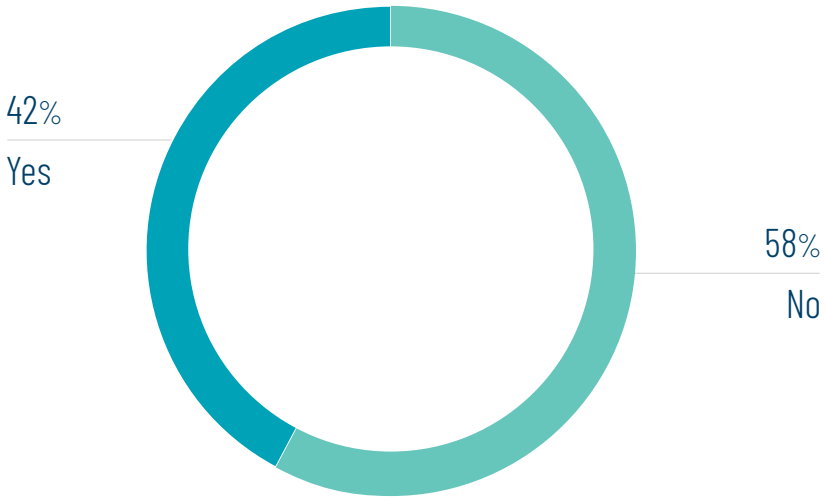


Does your Audit Committee have responsibility for and/or receive reports from any of the following functions other than IA?* *Multiple responses permitted.*



*Not shown: "Other" and "None of the above" responses.

Does the internal audit function perform audits on behalf of compliance?

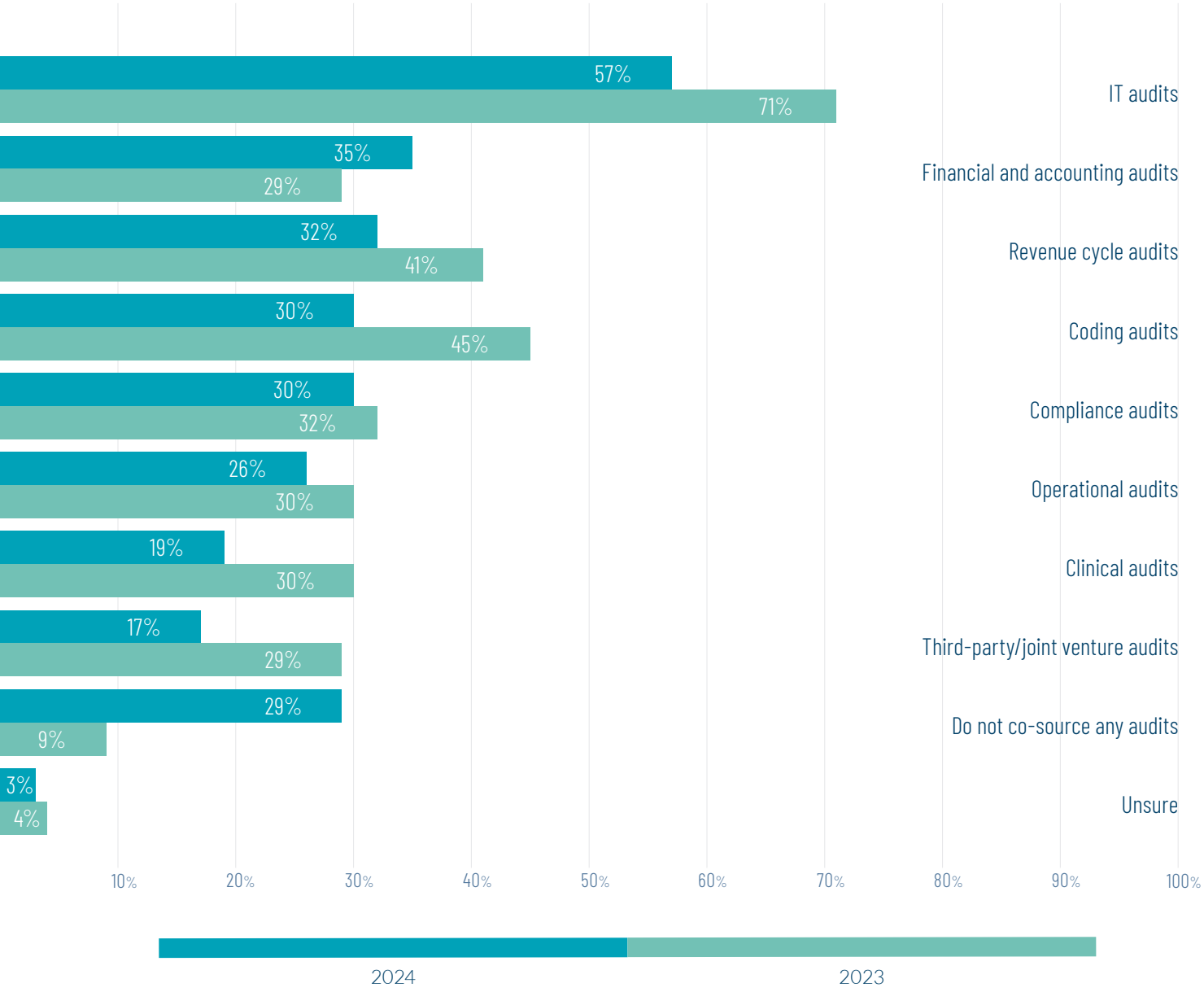


With which other functions, if any, does the internal audit function coordinate activities related to each of the following areas?

Multiple responses permitted.

	Compliance and privacy	Information technology (IT)/security	Legal	Quality	Risk management	Public accounting firm
Advisory	45%	41%	32%	26%	38%	13%
Audits	62%	61%	45%	38%	32%	41%
Enterprise risk management	36%	23%	20%	14%	46%	4%
Internal controls over financial reporting (e.g., SOX, MAR, etc.)	7%	16%	3%	4%	6%	32%
Risk assessment	55%	49%	35%	30%	48%	16%
None	25%	19%	32%	43%	26%	33%

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



Internal audit staff size — by annual revenue of organisation

Annual revenue (billions)							
Number of staff	Less than $0.499	$0.5 to $0.999	$1 to $4.99	$5 to $9.99	$10 to $19.99	More than $20	Unsure
20 or more			3%	15%	50%	75%	
15 to 19	14%		3%	8%	25%		25%
10 to 14	14%	14%	7%	15%		25%	
6 to 9			24%	31%			50%
3 to 5	14%	14%	50%	23%			
1 to 2	58%	72%	3%				25%
0 or fully outsourced			10%	8%	25%		
Study respondents %	**10%**	**10%**	**43%**	**19%**	**6%**	**6%**	**6%**

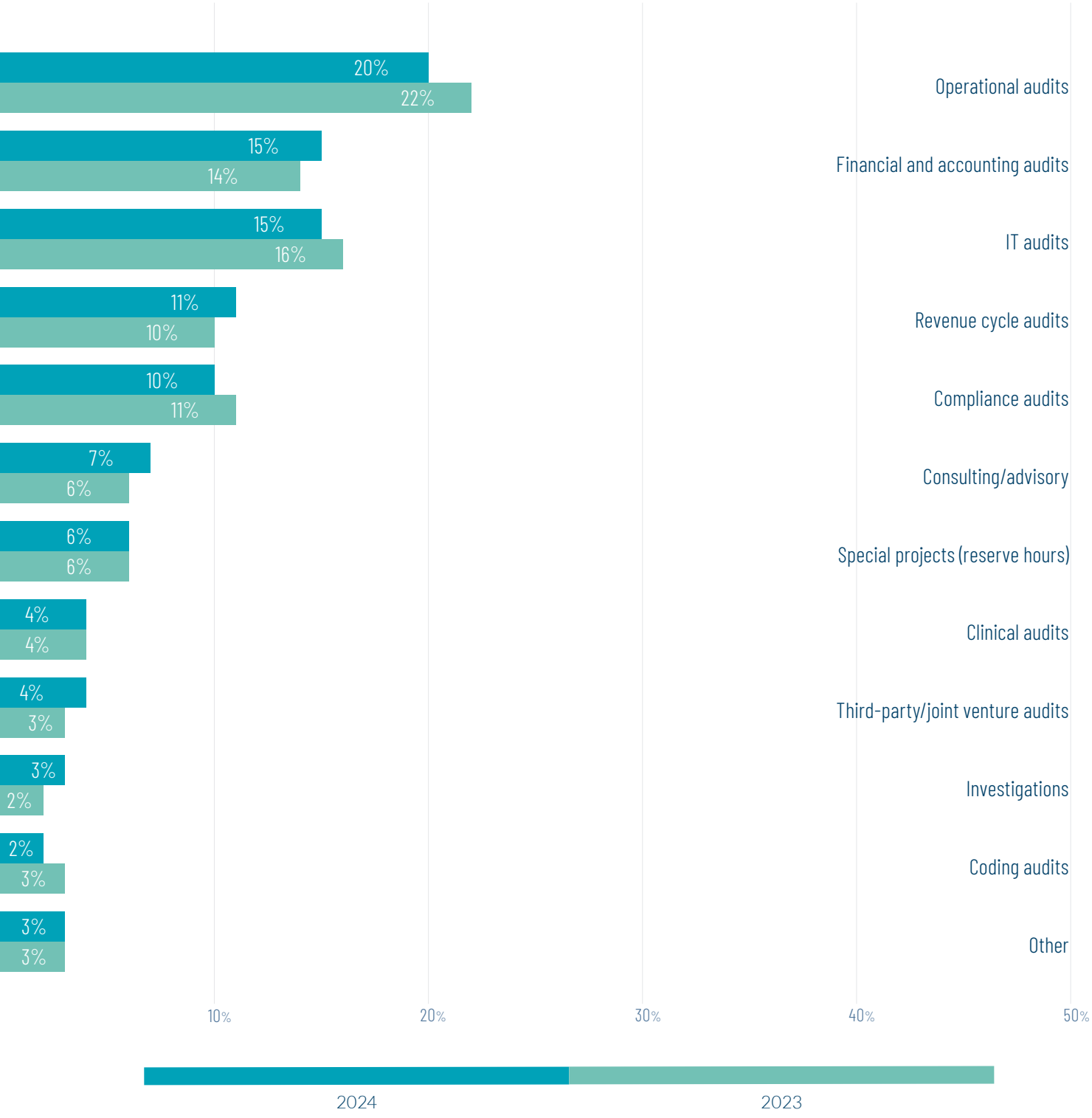
Budget for annual internal audit plan — by annual revenue of organisation

Annual revenue (billions)							
Annual IA budget (millions)	**Less than $0.499**	**$0.5 to $0.999**	**$1 to $4.99**	**$5 to $9.99**	**$10 to $19.99**	**More than $20**	**Unsure**
Greater than $3			3%	15%	50%	75%	
$2 to $2.9			10%	15%			
$1.5 to $1.999		14%	7%	15%	25%		
$1.25 to $1.499			7%	8%			
$1 to $1.249			13%	15%			
$0.75 to $0.999			30%	8%			
$0.5 to $0.749	14%	29%	20%				
$0.25 to $0.499	57%	43%	7%	8%	25%		
Less than $0.249	29%	14%					50%
Unsure			3%	16%		25%	50%
Study respondents %	**10%**	**10%**	**43%**	**19%**	**6%**	**6%**	**6%**

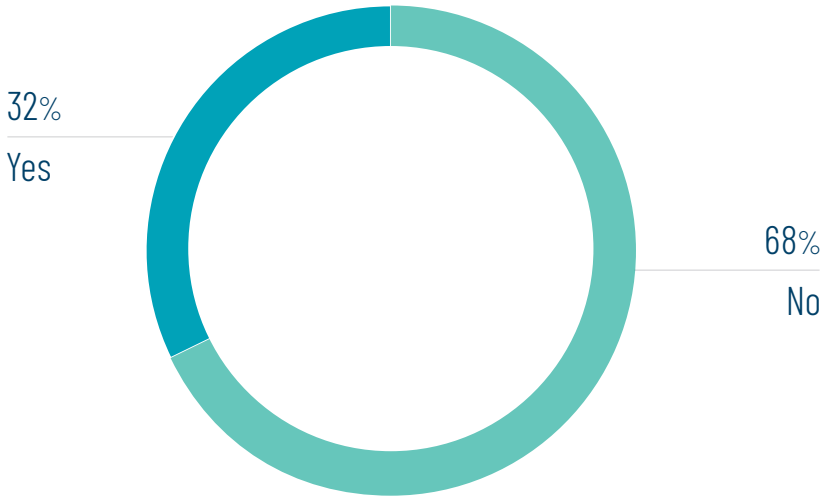
Hours for annual internal audit plan — by annual revenue of organisation

	Annual revenue (billions)						
Annual IA plan hours	**Less than $0.499**	**$0.5 to $0.999**	**$1 to $4.99**	**$5 to $9.99**	**$10 to $19.99**	**More than $20**	**Unsure**
15,000 or more			10%	22%	75%	50%	
10,000 to 14,999	14%		13%	31%		50%	25%
7,500 to 9,999		14%	17%				
4,000 to 7,499	29%		40%	31%			
2,000 to 3,999	29%	43%	17%	8%	25%		
1,000 to 1,999	14%	43%	3%	8%			75%
Fewer than 1,000	14%						
Study respondents %	**10%**	**10%**	**43%**	**19%**	**6%**	**6%**	**6%**

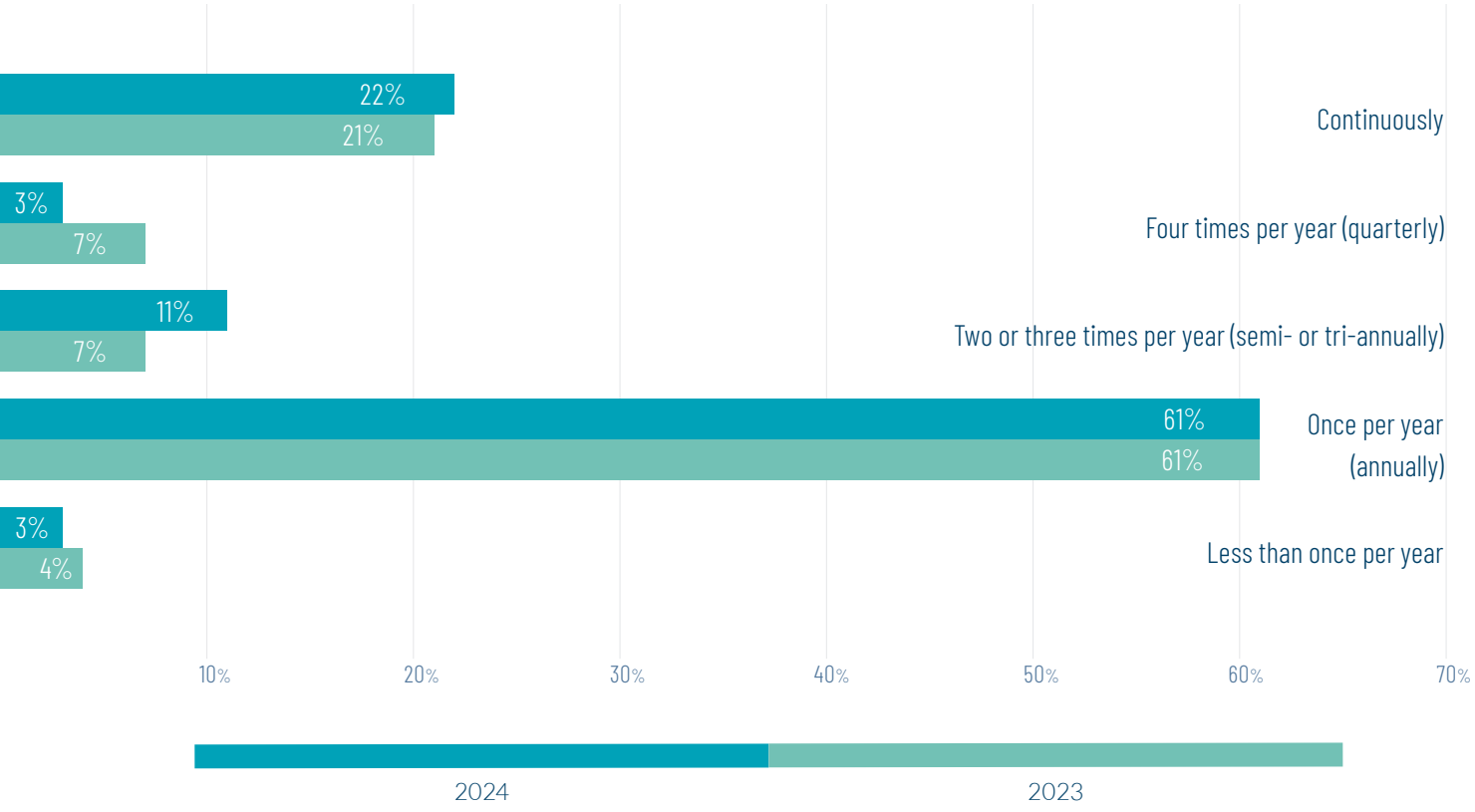
What percentage of the annual internal audit (non-administrative) time budgeted is allocated to the categories below?



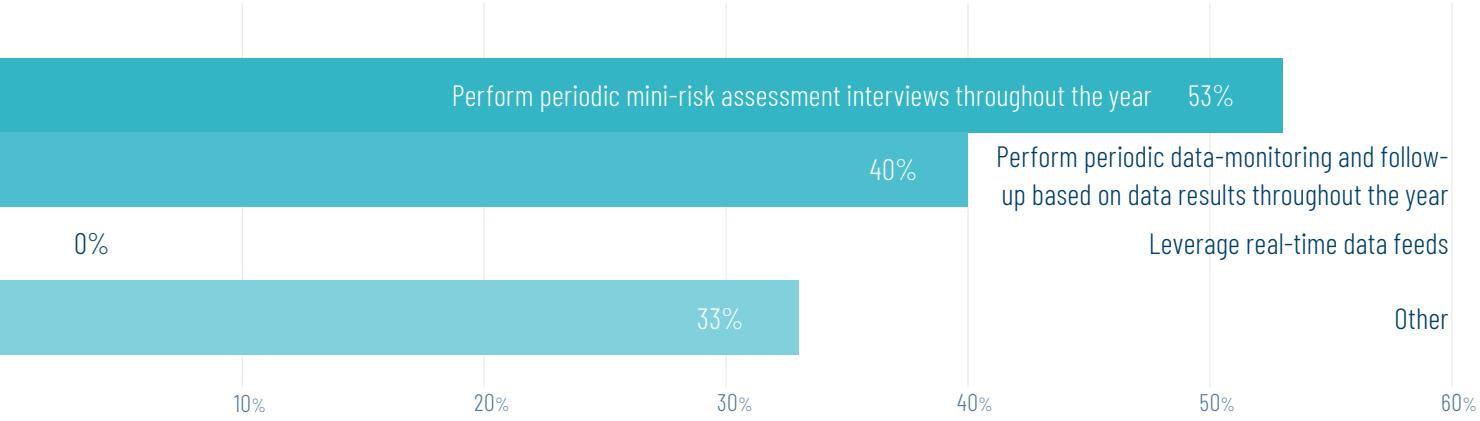
Have you updated your internal audit charter to align with the new model internal audit charter as issued by The IIA in March 2024?



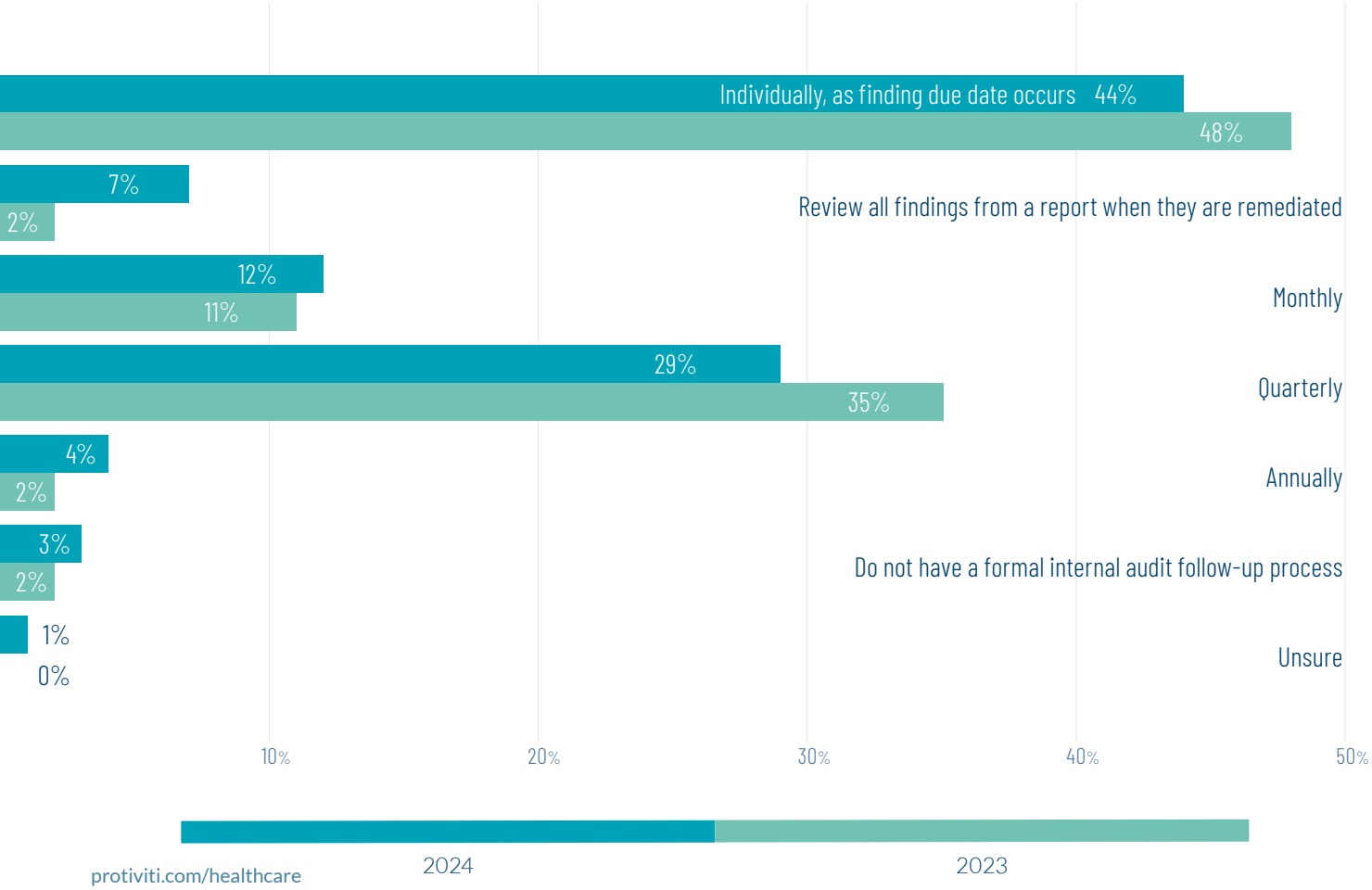
How often, if at all, is the risk assessment process performed and/or refreshed?



How does your internal audit function perform risk assessments continuously? *Sample: Those who answered "Continuously" for frequency of risk assessment. Multiple responses permitted.*

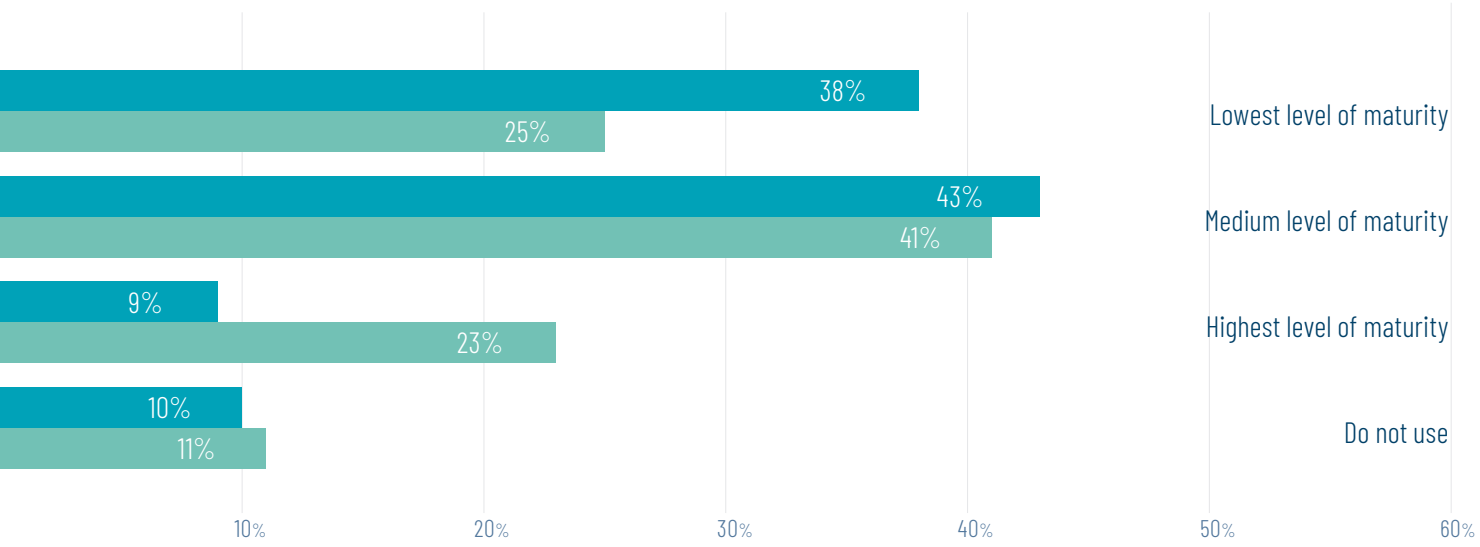


How often, if at all, do you follow up on outstanding internal audit findings?

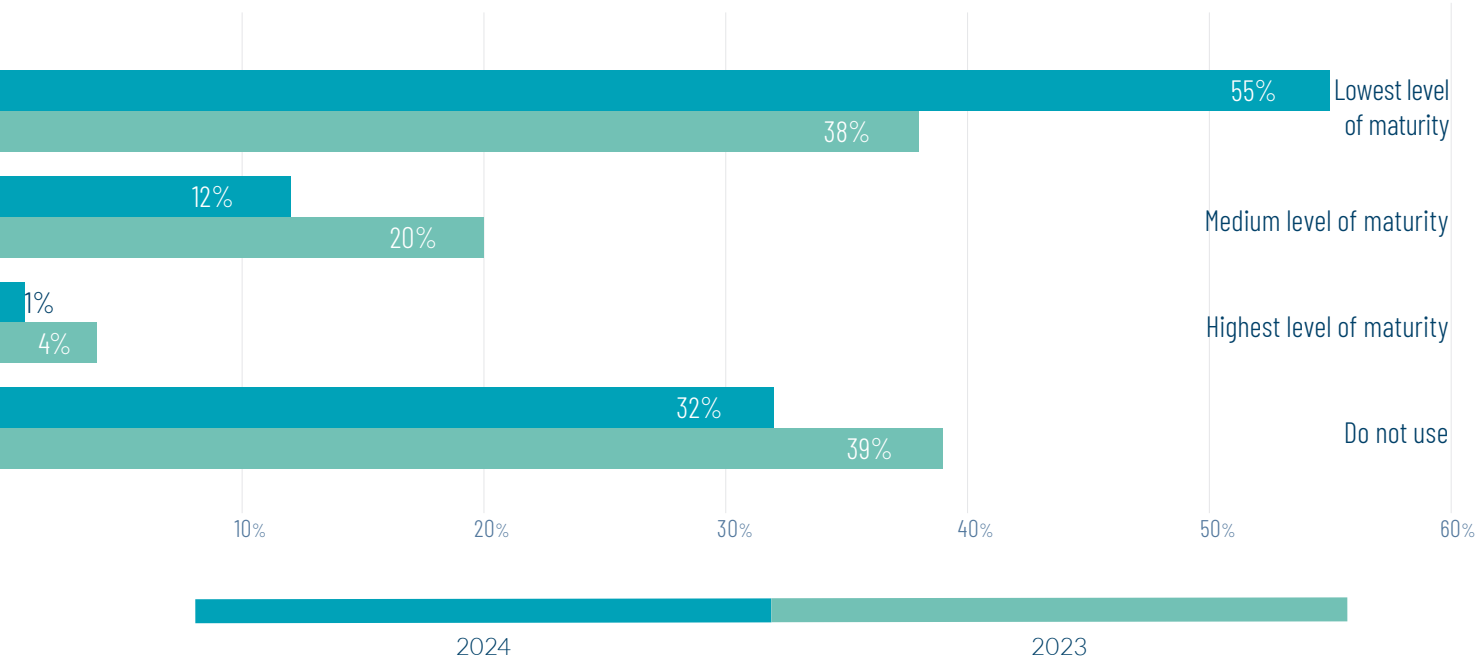


Please rate the current level of proficiency with each of the following areas within your internal audit function.

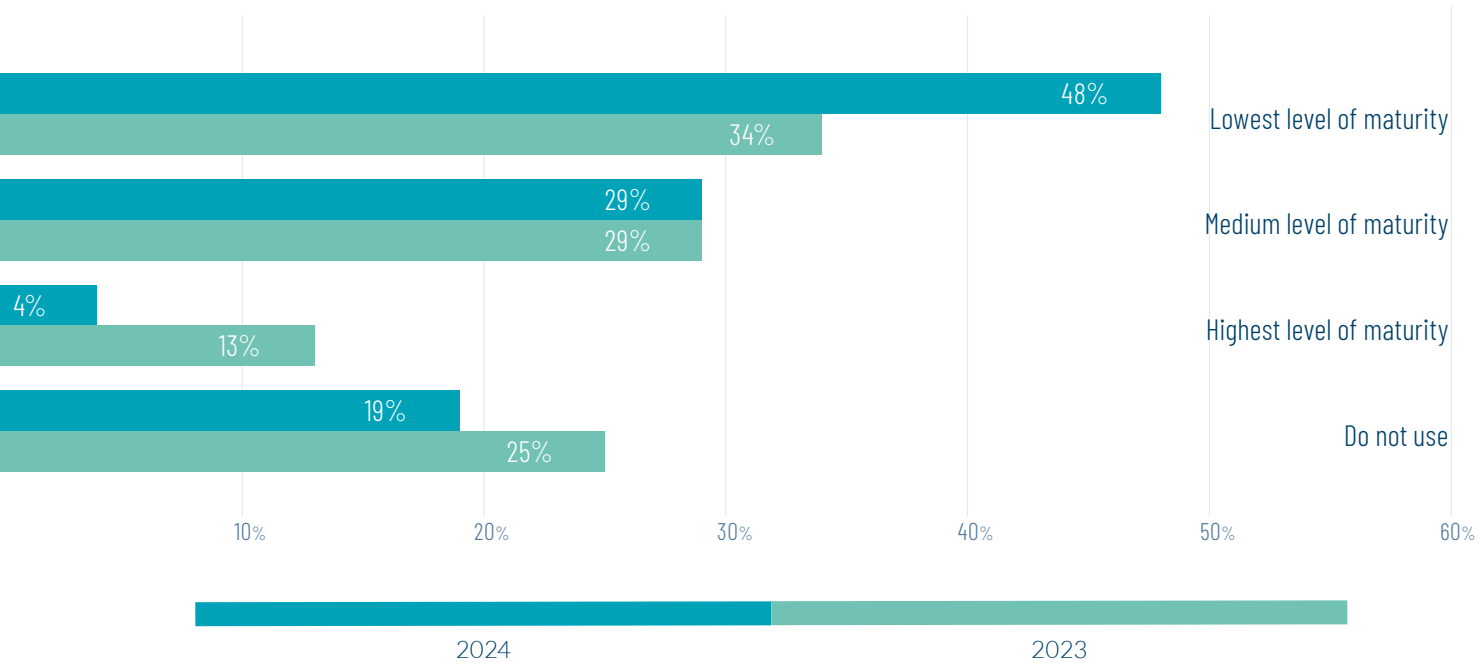
Advanced Analytics



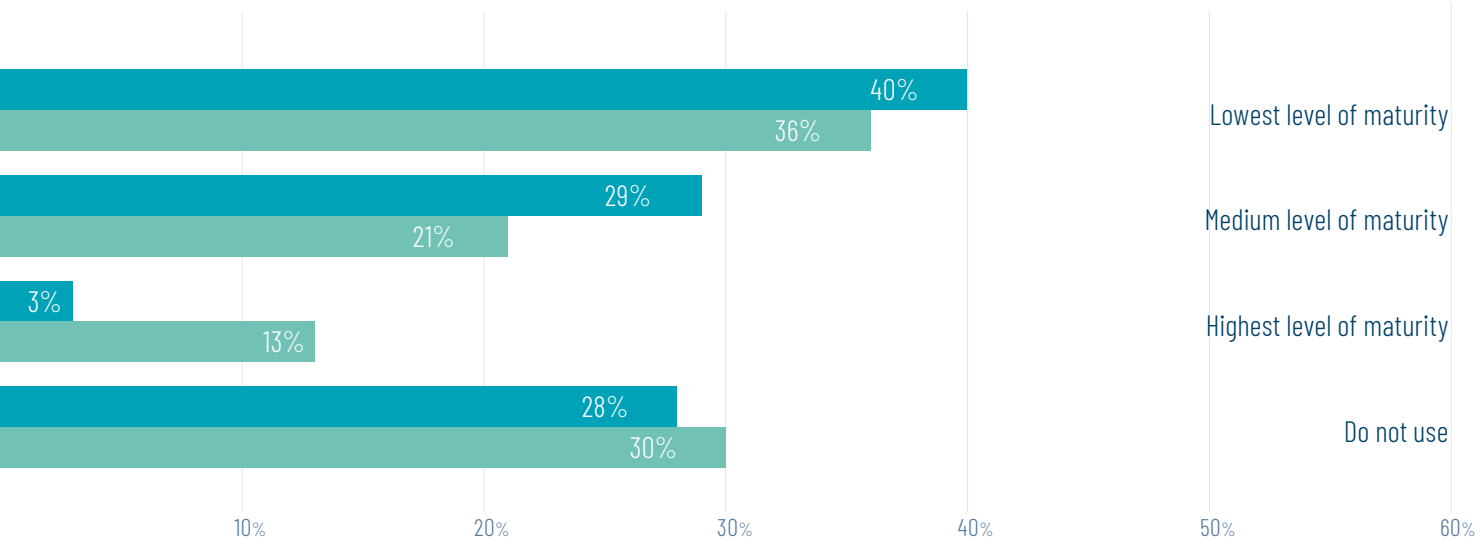
Artificial Intelligence



Automation



Process Mining



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, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 10th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).

Our Healthcare Internal Audit Solutions

Healthcare organisations today are faced with myriad challenges and many are underutilising 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 organisations 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 organisation 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®