ahia
Assoc. of Healthcare Internal Auditors

protiviti®
Global Business Consulting

Evolving Risk Landscape Refocuses Healthcare Audit Priorities

Key findings from the latest survey conducted by Protiviti and AHIA on internal audit plan priorities for provider and payer organisations

Table of Contents

03 Executive Summary

05 Cross-Segment Priorities

14 Provider-Specific Priorities

23 Payer-Specific Priorities

31 In Closing

32 About Protiviti

Executive Summary

As the healthcare industry adapts to the lasting effects of digital transformation, regulatory shifts and emerging cyber threats, organisations are encountering increasingly complex and unpredictable risks. AI-driven fraud, data privacy challenges and escalating ransomware attacks are reshaping the priorities for healthcare internal auditors. Their role remains critical in safeguarding operations, helping to ensure compliance, strengthening financial and IT controls, and addressing evolving vulnerabilities in an environment that demands resilience and strategic foresight.

The latest Healthcare Internal Audit Plan Priorities Study, conducted by Protiviti and the Association of Healthcare Internal Auditors (AHIA) reveals key areas of focus for internal auditors. This executive summary reveals key cross-segment priority focus areas for internal auditors, along with payer- and provider-specific results.

Top healthcare internal audit plan priorities

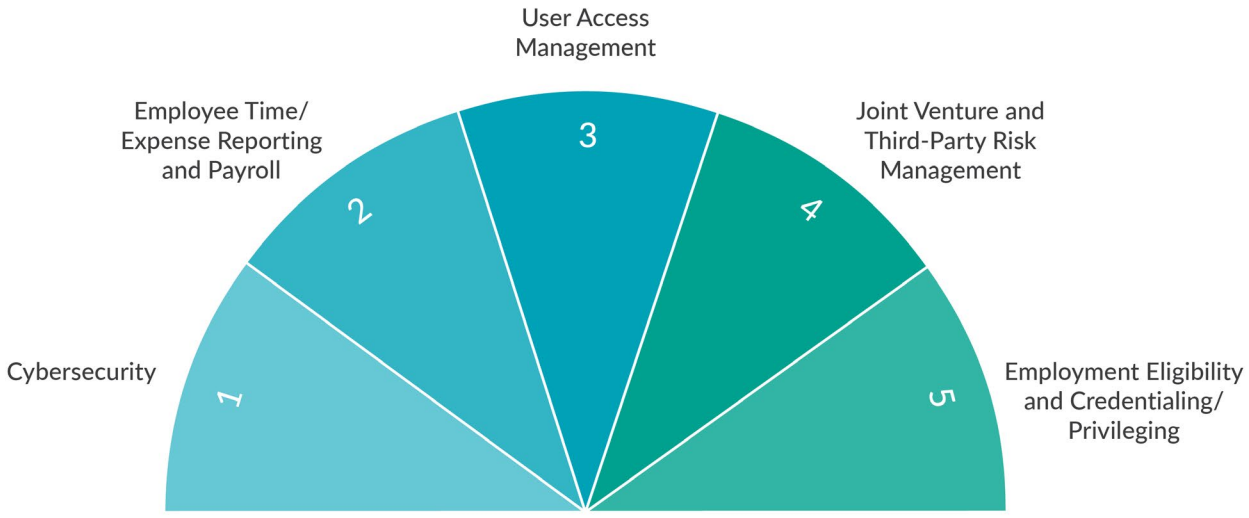
Priorities	Cross-segment	Provider	Payer
1	Cybersecurity	Fraud	Claims processing
2	Employee time/ expense reporting and payroll	Back-end revenue cycle operations	Member impact and access to care
3	User access management	Physician relationships	Provider relationships
4	Joint venture and third-party risk management	Pharmacy operations and drug distribution/ management	Product and sales
5	Employment eligibility and credentialing/ privileging	Hospital and physician clinical coding and documentation	Risk adjustment/ coding

> In today's rapidly evolving healthcare landscape, internal audit plays an essential role in protecting organisational integrity and ensuring compliance while also validating, enhancing and leveraging innovation. From cybersecurity and user access management to fraud prevention, provider relationships and the integration of advanced technology and AI, a proactive and strategic audit function enables healthcare organisations to anticipate emerging risks, strengthen resilience and deliver optimal consumer experience in the face of unprecedented challenges.

– **Richard Williams**
Global Practice Leader, Healthcare Industry

Cross-Segment Priorities

Top Five Priorities



Across the enterprise, healthcare organisations are affected by multiple challenges regardless of segment. These interconnected risks must be addressed to support organisational objectives while providing assurance and value.

01 Cybersecurity

Cybersecurity remains the top priority for internal audit in healthcare for the third consecutive year, driven by a relentless wave of cyberattacks targeting the industry. These attacks have caused prolonged system outages and network outages – sometimes lasting a month or longer – resulting in severe patient safety risks, revenue losses, operational disruptions, workforce strain, reputational damage and financial instability. Healthcare organisations must act decisively to safeguard their systems and data against these threats.

Key audit areas to consider:

- **Security programme assessment:** Evaluate the organisation's security posture using recognised frameworks such as the National Institutes of Standards Technology (NIST) Cybersecurity Framework (CSF) or the U.S. Department of Health and Human Services (HHS) Cybersecurity Performance Goals (CPG). Verify that assessments align with regulatory requirements and include adversary simulations and penetration testing to identify vulnerabilities. Confirm that risk management plans adequately address any identified weaknesses.
- **Asset and vulnerability management:** Assess how the organisation maintains a complete inventory of technology assets that access sensitive data or networks. Verify that vulnerabilities are identified and remediated promptly in accordance with established policies and best practices.
- **Incident response:** Review the organisation's incident response plans and recovery capabilities. Examine whether regular testing (e.g., drills or tabletop exercises) and thorough post-incident analyses are conducted to learn from breaches and continuously improve response processes.
- **Third-party risk management:** Analyse how third parties with access to the organisation's data or networks are vetted, monitored and managed. Confirm that risks associated with vendors and partners are effectively identified, escalated and addressed to protect the organisation's security posture.
- **Social engineering awareness:** Examine the organisation's efforts to educate and test employees on social engineering tactics such as phishing. Assess the effectiveness of training programmes, the frequency of awareness testing, and the protocols for reporting and escalating suspected social engineering attempts.

Cybersecurity attacks can cause prolonged system and network outages, impacting patient safety, causing reputational damage and financial instability, and more.

02 Employee time and expense reporting and payroll

In today's healthcare landscape, payroll and timekeeping processes carry significant compliance, financial and reputational risks. With regulations changing frequently amid mounting pressure on labour costs, healthcare organisations must be vigilant in how they manage employee compensation, time tracking and workforce documentation. Internal audit plays a vital role in spotting gaps, reinforcing controls and ensuring compliance with both federal and state labour laws.

Key audit areas to consider:

- **Wage and hour compliance:** Audit employee classifications (exempt vs. non-exempt), overtime calculations, meal/rest break tracking, and payroll deductions. Verify compliance with the Fair Labour Standards Act (FLSA) and corresponding state laws to prevent wage-and-hour litigation or regulatory investigations.
- **Timekeeping fraud:** Review timekeeping system data such as biometric time clock records, audit trails and exception reports to uncover fake punch-ins, shared logins or intentionally inflated hours, which can drive up labour costs and lead to wage law violations if left undetected.
- **Immigrant workforce compliance:** Evaluate processes around Form I-9 (Employment Eligibility Verification) documentation, work authorisation validation, visa status tracking, and payroll tax treatment for immigrant or temporary staff. Effective audits here can prevent costly fines, verify staffing complies with immigration laws, and avoid staffing disruptions due to documentation issues.
- **State-specific and multi-state regulations:** Verify that payroll systems and human resources (HR) policies reflect evolving state and local labour laws, such as sick leave mandates, pay transparency requirements and daily overtime rules. For organisations operating across multiple states, confirm that variations in laws are properly configured and/or documented to avoid noncompliance penalties.

03 User access management

Managing user access in healthcare is a complex challenge due to the diverse and dynamic population of users and systems that must be secured. The presence of outdated technologies, which often struggle to integrate with modern Identity and Access Management (IAM) solutions, exacerbates this issue. Such fragmentation can lead to inconsistent access control practices and increased risk. Notably, compromised user credentials are involved in a majority of cybersecurity breaches, making robust user access management essential for protecting sensitive information.

Key audit areas to consider:

- **User authentication:** Evaluate the effectiveness of authentication mechanisms to confirm that only legitimate users can access networks and systems. This should include strong multi-factor authentication (MFA) across all remote and privileged access, the use of secure VPNs for remote connections, and hardened authentication tokens where applicable. Assess whether these controls are consistently applied across all access points and applications.
- **Privileged access management (PAM):** Review the organisation's strategies for controlling and monitoring accounts with elevated privileges. Verify that strict policies are in place for granting, reviewing and revoking privileged access. Confirm that all privileged sessions are logged and monitored for anomalous behavior, and that high-risk actions by administrators are promptly reviewed.
- **Consumer identity protection:** Assess the measures the organisation has in place to protect the accounts of consumers, patients and members who access its digital services. This includes evaluating identity verification processes (for instance, confirming patient identities during portal registration) and the security of personal information handled through patient portals or mobile apps.
- **User access reviews:** Examine whether regular access reviews are conducted to confirm that each user's system permissions align with their current role and responsibilities. Verify that a reliable process is in place for promptly removing or adjusting access for users who no longer require it (such as terminated employees or individuals who change job positions). Verify that these reviews are documented and that any issues identified are addressed in a timely manner.

Compromised user credentials are involved in a majority of cybersecurity breaches, making robust user access management essential for protecting sensitive information.

04 Joint venture and third-party risk management

Healthcare organisations increasingly depend on external vendors and partners. High-profile incidents demonstrate that third-party failures can cripple operations, jeopardise patient safety, expose the organisation to compliance risk, threaten financial stability and damage reputations. With many organisations adding or changing vendors, robust third-party risk oversight is essential.

Key audit areas to consider:

- **Due diligence and risk assessment:** Confirm a process exists to conduct comprehensive due diligence on all vendors before engagement, especially those vendors handling sensitive patient data or critical systems. Use thorough risk identification processes that cover inherent risks and each vendor's control environment. Align assessments with the organisation's risk tolerance and update them regularly.
- **Continuous monitoring and compliance:** Continuously monitor vendor performance using defined metrics and service level agreements (SLAs), and address any areas of noncompliance or poor performance through clear reporting and remediation processes.
- **Business continuity, disaster recovery and resiliency:** Confirm that critical vendors maintain robust business continuity, disaster recovery and resilience plans that meet the organisation's requirements. Plan for vendor failures with contingency measures and/or alternate suppliers to prevent a single point of failure or operational disruption.
- **Exit strategies:** Confirm that there are clear procedures and contract terms for terminating vendor relationships. Define conditions for termination, including each party's responsibilities and requirements for transition support or service handover. Plan to shift work in-house or to another provider to minimise disruption if a contract ends.
- **Governance and oversight:** Confirm that a comprehensive third-party risk management framework exists and is in place. Define policies, procedures and roles for managing vendor relationships. Engage senior leadership or a dedicated committee in oversight, with regular third-party risk reporting to executives or the board.

Failures in third-party risk oversight can cripple operations, jeopardise patient safety, expose the organisation to compliance risk, threaten financial stability and damage reputations.

05 Employment eligibility and credentialing/privileging

Verifying employment eligibility and provider credentials is more than a routine compliance task – it is essential for mitigating legal, financial and patient safety risks. With increasing scrutiny from regulators and stakeholders, healthcare organisations must prioritise thorough verification and credentialing practices to avoid costly oversights. As regulations evolve and technology advances, internal audit teams need to confirm that hiring, credentialing and ongoing monitoring processes are robust and up to date.

Key audit areas to consider:

- **Employment eligibility and I-9 verification and monitoring:** Assess the methodologies for verifying new-hire eligibility (e.g., ensuring proper completion and verification of Form I-9) and for ongoing re-verification of work authorisations when they expire. Pay special attention to remote hiring practices and confirm that the organisation is complying with any flexible I-9 verification procedures, if applicable. Regular reviews of I-9 documentation processes will help prevent compliance gaps and reduce the risk of penalties.
- **Credentialing and privileging accuracy:** Validate that healthcare provider credentials (e.g., licenses, certifications, education, training, malpractice history) are being verified through primary sources. Verify that privileging decisions (i.e., granting specific clinical privileges to providers) align with the verified qualifications and documented clinical competencies of each provider. Accurate credentialing and privileging are essential for regulatory compliance, accurate billing and patient safety.
- **Continuous monitoring and license renewal tracking:** Audit the systems and processes used to track employee and contractor eligibility status, professional license renewals, board certifications, sanctions, and U.S. Department of Health and Human Services Office of Inspector General (OIG) exclusions. This includes verifying that any automated systems or AI tools being used for monitoring are functioning as intended. Check that alerts for expirations or issues are acted upon promptly and that errors or omissions in the tracking process are remediated quickly. Proactive monitoring and timely renewal verification reduce the risk of lapses in credentials and help maintain operational resilience.

Cross-Segment Priorities: Additional Areas of Focus

Privacy

The volume and complexity of data used by healthcare organisations continues to expand rapidly, driving improvements in both clinical and nonclinical outcomes. As big data fuels innovation, ensuring its protection remains critically important. The integration of advanced technologies such as AI, automation and data analytics will be instrumental in upholding privacy standards while also enhancing the quality of care. Organisations must adopt proactive strategies to harness the benefits of these technologies while safeguarding the security and confidentiality of sensitive data. Securing protected health information (PHI) and personally identifiable information (PII), ensuring appropriate use and disclosure of data (including to third parties), and adhering to the "minimum necessary" standard are fundamental to mitigating privacy risks. Effectively preventing and addressing data breaches or incidents (such as unauthorised access or snooping into medical records) is vital to maintaining patient trust, ensuring regulatory compliance and preserving the organisation's reputation.

Financial management, reporting and accounts payable

The complexity of healthcare finance creates significant risk exposure that requires ongoing oversight. Accounts payable management is vital for maintaining cash flow and preventing fraud. Comprehensive internal and external financial reporting, including cost reporting, is essential for regulatory compliance and informed decision-making. The integrity of financial data underpins the reliability of all financial processes, safeguarding the organisation's financial health and reputation. Internal audit is uniquely positioned to evaluate financial controls, detect fraud or waste, and assess the integrity of financial reporting in a rapidly changing regulatory environment. With increasing scrutiny from regulators, payers and donors, ensuring financial transparency and accountability is critical. Additionally, pressures related to thin margins, rising labour and supply costs, and the shift to value-based care models demand strong governance and informed decision-making. This focus ultimately helps protect assets, support compliance and preserve the mission of care delivery.

Human resources/workforce

HR functions in healthcare are critical to helping organisations adapt to rapid technology advancements and evolving workforce expectations. Skills development remains a top priority, especially with the rise of telemedicine, AI diagnostics and personalised care. A culture of continuous learning helps teams stay innovative and patient focused. As digital transformation reshapes healthcare, HR must redesign workflows, support flexible work models and build interdisciplinary teams to tackle complex challenges. Evolving roles demand HR strategies that foster adaptability and technical proficiency. Meanwhile, talent acquisition is increasingly competitive. To attract top talent, healthcare organisations are emphasising strong employment branding, highlighting commitments to development, diversity and meaningful careers. These efforts enhance both recruitment and retention, securing a capable, engaged workforce for the future.

Capital projects

With large-scale investments in infrastructure and technology, it is crucial to establish that capital expenditures align with an organisation's strategic goals to maximise return on investment. Healthcare systems face continuous scrutiny over spending, making effective oversight essential to prevent financial mismanagement and enhance accountability. Internal audit can support these objectives by identifying risks associated with project overruns, misallocation of funds, and noncompliance with regulatory requirements. Audit teams can also highlight opportunities for efficiency and improvement in project management. This includes driving better decision-making, improving resource allocation, and verifying that projects adhere to approved timelines and budgets. Such proactive auditing not only safeguards organisational assets but also supports sustainable growth and innovation in an evolving healthcare landscape.

System implementation/upgrades

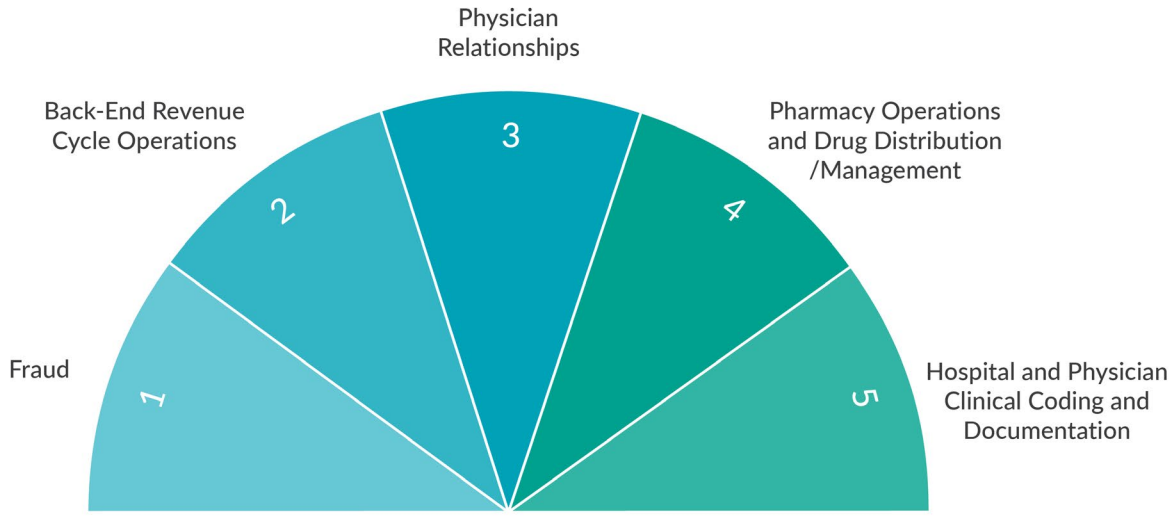
System implementations, conversions and upgrades are top priorities for healthcare organisations due to their critical role in enhancing operational efficiency, ensuring data integrity, and maintaining compliance. As technology rapidly evolves, ensuring that systems are up to date and well-integrated is essential for optimising workflows, improving patient care and effectively managing the bottom line. After the initial wave of technology modernisation over the past few years, software vendors continue to update their products, often incorporating sophisticated functionality such as AI that can significantly improve operations. Most healthcare companies will therefore continue to implement new technologies and enhance existing systems. Organisations need comprehensive strategies and strong governance to address challenges that arise during these projects. Internal audit should verify that effective project management practices are in place to implement solutions and mitigate risks associated with system downtime, data migration errors, cost overruns, or falling behind competitors due to slow technology adoption.

Supply chain

Healthcare supply chain professionals are increasingly tasked with reducing the cost per patient amid significant global disruptions that include tariff uncertainties, heightened cybersecurity concerns, persistent inflationary pressures and substantial labour shortages. To maintain operational efficiency under these conditions, healthcare systems should adopt connected supply-chain systems that facilitate orchestration across the multiple platforms handling complex purchasing and distribution transactions. Such an approach enables real-time spend visibility and supports proactive cost control and revenue cycle optimisation. Additionally, integrating vendor credentialing and third-party risk management (TPRM) into supply chain systems can enhance security and compliance. Connected systems, complemented by automation and real-time advanced analytics, allow for continuous monitoring of supply conditions and enable swift responses to potential issues such as supply-demand imbalances, stock shortages or price fluctuations. By implementing these strategies, healthcare organisations can build greater resilience into their supply chain operations and help to ensure continuity of care even during disruptions.

Provider-Specific Priorities

Top Five Priorities



Healthcare providers face their own unique set of risks that require internal audit teams to shift from reactive oversight to proactive leadership.

01 Fraud

Fraud remains a top concern for healthcare providers and a critical focus for internal audit. The sector's dependence on external vendors and complex supply chains heightens risks in payroll, billing and patient data handling. Improper claims billing involving government payers such as Medicare and Medicaid also poses significant fraud risk, often triggering regulatory scrutiny, False Claims Act liability, and potential exclusion from federal programmes. Internal auditors must proactively identify and mitigate these risks to prevent financial loss, legal exposure and reputational damage.

Key audit areas to consider:

- **Claims fraud monitoring:** Analyse billing trends and claims data to detect anomalies such as upcoding, phantom billing or duplicate claims, particularly those involving government payers such as Medicare or Medicaid. Align audits with HHS OIG Work Plan priorities, enforcement actions, etc.
- **Procurement and vendor management:** Review purchasing, vendor due diligence, bidding, invoicing and contract compliance to detect kickbacks, overbilling or favoritism.
- **Expense reimbursement verification:** Analyse employee expense reports for anomalies like repeated or high-value claims that may signal fraud.
- **Conflict-of-interest reviews:** Verify that disclosure processes are in place and audit for undisclosed relationships that may be influencing business and regulatory decisions.
- **Access control and user activity:** Review system access and user activity for unauthorised changes to vendor or employee data that could indicate fund diversion.
- **Payroll and benefits integrity:** Examine the payroll system for ghost employees, unauthorised overtime or irregular benefit claims. Flag patterns like multiple direct deposits or excessive overtime.
- **Inventory and asset management:** Verify that physical inventories (medical supplies, equipment, pharmaceuticals, etc.) are properly tracked and reconciled. Investigate any discrepancies that could indicate theft or diversion of assets by employees or third parties.

Internal auditors can help provider organisations prevent financial loss, legal exposure and reputational damage by proactively identifying and mitigating risks, including those related to fraud.

- **Third-party intermediaries:** Scrutinise transactions involving agents, consultants or other intermediaries who act on behalf of the company. Look for irregular contract terms, unusually high fees, or payments that coincide with new client acquisitions or regulatory approvals, as these could be red flags for bribery or kickback schemes.
- **Journal entry testing:** Conduct detailed testing of journal entries looking for timing and process anomalies, especially around revenue recognition and reserves, to uncover potential manipulation.

02 Back-end revenue cycle operations

The back end of the revenue cycle includes core functions that directly impact a provider's financial performance and compliance status. These functions span claims processing, payment posting, denial management, accounts receivable follow-up, and patient collections. Internal audit should assess not only the efficiency of these operations but also their adherence to payer contract terms, regulatory requirements and internal policies. Given heightened regulatory scrutiny in these areas (e.g., compliance with prompt refund requirements and proper handling of denials), audits must help to ensure that revenue cycle processes are both effective and compliant.

Key audit areas to consider:

- **Claims processing accuracy:** Confirm services are coded and billed correctly using appropriate CPT/HCPCS codes, diagnosis codes and modifiers, supported by documentation to reduce rework and denials.
- **Post-service revenue integrity:** Verify clinical documentation aligns with charges. Every documented procedure should have a corresponding charge to prevent missed revenue.
- **Denial management:** Assess how denials are tracked and resolved. Review root causes, appeal processes, and the use of CARC/RARC codes to support timely and accurate follow-up.
- **Payment variance and contract compliance:** Compare expected vs. actual payments. Identify under/overpayments and confirm payer contracts are correctly configured, including value-based or risk-sharing arrangements.

- **Credit balance and refund processing:** Evaluate how overpayments are identified and refunded. Assess compliance with CMS and OIG guidelines for timely resolution.
- **Patient financial services:** Review billing and collection practices for clarity, fairness, and compliance with pricing transparency and the No Surprises Act. A patient-friendly process supports both compliance and satisfaction.

03 Physician relationships

Regulatory bodies have intensified their focus on financial relationships between healthcare providers and physicians, particularly with regard to the federal Stark law and the Anti-Kickback Statute (AKS). In May 2025, the U.S. Department of Justice (DOJ) and the HHS announced they are more aggressively pursuing cases of healthcare fraud and abuse involving kickbacks and improper physician referrals. In 2024, CMS nearly doubled the total number of Voluntary Self-Referral Disclosure Protocol (SRDP) settlements, resolving 314 cases in 2024 compared to 176 cases in 2023.

With this environment, healthcare organisations must adopt proactive measures to strengthen compliance and mitigate risks associated with physician arrangements.

Key audit areas to consider:

- **Physician arrangements:** Regularly audit financial relationships and agreements between the organisation and its physicians by confirming that each arrangement meets a Stark law exception and/or AKS safe harbor, and that compensation is consistent with fair market value (FMV) for the services provided, and not tied to the volume or value of referrals.
- **Referral pattern analysis:** Analyse physician referral patterns for any anomalies that could indicate potential kickback arrangements or self-referral issues. For example, examine whether certain high-referring physicians have financial ties to the organisation or whether there are abrupt changes in referral volumes surrounding new financial agreements.
- **High-risk relationship monitoring:** Prioritise scrutiny of inherently high-risk arrangements. This includes contracts involving complex compensation formulas, physician ownership or investment in entities the hospital does business with, and relationships with physicians who are in a position to generate substantial referral business. These situations warrant deeper auditing due to greater regulatory risk.

Financial relationships between healthcare providers and physicians face greater scrutiny from regulatory bodies, increasing the urgency to strengthen compliance and mitigate risk proactively.

- **Conflict-of-interest disclosures:** Review the processes for physician conflict-of-interest disclosure and compare disclosed information to payments or ownership interests reported in external databases (such as CMS's Open Payments database). Verify the organisation has a robust programme to review, escalate and address any conflicts identified, and that any required reporting to regulators is completed accurately and timely.

04 Pharmacy operations and drug distribution/management

Healthcare executives are increasingly focused on pharmacy operations and drug distribution management due to their impact on compliance, efficiency, financial integrity and patient safety. Emerging risks in these areas are shaped by technological advances, regulatory shifts and market dynamics.

Key audits areas to consider:

- **Regulatory compliance:** Pharmacy operations and medication distribution are critical areas for healthcare providers, carrying significant compliance, financial and patient safety implications. This area is heavily regulated by agencies such as the U.S. Food and Drug Administration (FDA), the U.S. Drug Enforcement Administration (DEA), and the Centers for Medicare and Medicaid Services (CMS). Internal audit should focus on evaluating adherence to the following areas to prevent penalties, fines or loss of licensure:
  - **Controlled substances:** Confirm proper handling, tracking, storage and reporting of controlled substances to prevent diversion or misuse and to comply with DEA regulations.
  - **Medicare and Medicaid billing compliance:** Validate accurate billing for medications and services.
  - **Licensing requirements:** Verify that pharmacies and pharmacists meet state and federal licensing standards.
- **Financial risks:** Drug distribution and pharmacy operations involve significant financial transactions, including purchasing, inventory management and billing. Audit areas include:
  - **Fraud prevention:** Identify and mitigate risks of fraudulent activities such as overbilling or kickbacks.
  - **Cost control:** Verify proper pricing and reimbursement practices to avoid financial losses.

- **Patient safety:** Errors in pharmacy operations, such as incorrect dispensing or failure to manage drug interactions, can have life-threatening consequences. Consider audits around:
  - **Medication errors:** Determine if robust systems are in place to minimise errors in prescribing, dispensing and administering drugs.
  - **Quality control:** Monitor the integrity and safety of medications throughout the supply chain in compliance with the Drug Supply Chain Security Act (DSCSA).
- **Operational efficiency:** Inefficiencies in pharmacy operations can lead to delays in patient care and increased costs. Internal audit commonly evaluates:
  - **Supply chain management:** Verify adequate stock levels and prevent disruptions in drug availability.
  - **Technology use:** Review the implementation of automated systems for accuracy and efficiency.

Emerging risks in pharmacy operations and drug distribution management can impact compliance, efficiency, financial integrity and patient safety.

05 Hospital and physician clinical coding and documentation

Accurate clinical documentation and coding are essential for quality patient care and revenue integrity. According to the American Health Information Management Association (AHIMA), a significant portion of healthcare revenue is lost due to claim denials and delays caused by documentation or coding errors. Internal audit plays a critical role in ensuring compliance, alignment with industry standards, and accuracy in clinical documentation and coding. Regular audits help improve documentation quality and accurate reimbursement while reducing compliance risk.

Key audits areas to consider:

- **Behavioral health services documentation:** Review the completeness and accuracy of documentation for mental health and substance abuse services. Verify that therapy duration, treatment plans and progress notes support billed codes. Documentation must justify diagnoses and treatments to meet clinical and payer requirements.
- **Use of AI in coding:** If using computer-assisted coding (CAC) or AI tools, assess their performance and controls. Confirm that AI-generated codes are reviewed by qualified professionals and enhance accuracy rather than introduce errors. Audit samples should compare AI-generated codes to actual documentation.

- **Diagnosis-related group (DRG) accuracy:** For inpatient stays, verify that assigned DRGs are supported by medical records. Inaccurate DRGs can result in overpayments (compliance risk) or underpayments (lost revenue). Confirm physicians document all relevant comorbidities and complications, and coders capture them correctly.
- **Evaluation and management (E/M) and CPT coding:** Audit physician coding, especially for E/M services and high-risk CPT codes like prolonged services or complexity add-ons (e.g., G2211). Confirm that documentation supports the billed service level and that coders follow current guidelines. Errors can lead to disallowed charges, audits or repayments.

Provider-Specific Priorities: Additional Areas of Focus

Revenue cycle compliance

Revenue cycle compliance remains a top priority amid increasing regulatory scrutiny. Internal audit should focus on adherence to the No Surprises Act and its Good Faith Estimates component, proper notice and consent for out-of-network services, and required disclosures. Compliance with Hospital Price Transparency rules is also key, including accurate, accessible machine-readable files (MRFs) and correct display of payer-specific negotiated rates. As automation expands, audits should assess data integrity across electronic health records (EHRs), billing systems and payer portals to detect misbilling or control gaps. Oversight of outsourced vendors handling coding, billing or patient communications should also be evaluated. By prioritising these compliance areas, internal audit can help the organisation mitigate regulatory risks, maintain patient and payer trust, and uphold the integrity of the organisation's billing practices.

Charge capture

Accurate charge capture is essential for optimising reimbursement and minimising revenue leakage. Internal audit should focus on validating that services provided to patients are properly documented and billed. This involves auditing clinical departments to see that procedures, treatments and supplies used are recorded in the medical record and reflected on the bill. Common issues to look for include missed charges (services provided but not billed), incorrect charge codes, and inconsistent documentation that could lead to billing errors. By pinpointing discrepancies or inefficiencies in the charge capture process, internal audit can identify opportunities for process improvements. Strengthening charge capture controls and workflows will help increase the organisation's revenue (through more complete billing) and reduce the incidence of claim denials related to billing errors.

Medical management

Internal audit can enhance value by assessing whether medical management processes help to ensure appropriate care while controlling costs. This includes reviewing management processes like pre-authorisations, inpatient admissions, and post-acute referrals for compliance with evidence-based guidelines and Medicare/Medicaid rules. Audits should confirm that service denials are clinically justified and documented. Case and disease management programmes should be evaluated for effectiveness in identifying high-risk patients and coordinating care. Reviews of inpatient length of stay and readmissions should confirm efficient discharge planning and identify trends using data analytics. Lastly, performance reports on utilisation metrics should be regularly reviewed and acted upon, especially when avoidable readmissions exceed benchmarks. These audits help mitigate financial and regulatory risks tied to overutilisation or underutilisation.

Medical device security

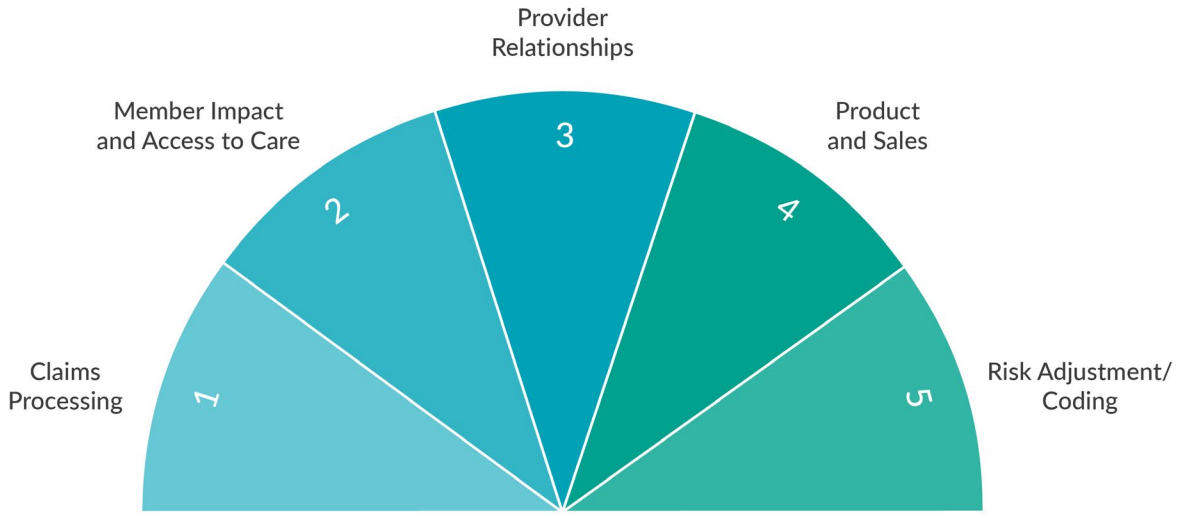
Medical devices like infusion pumps and heart monitors are vital to patient care but pose significant cybersecurity risks. Many operate on outdated systems, lack strong security controls, and are network-connected, making them vulnerable to attacks. A compromised device can endanger patients, disrupt operations and/or expose sensitive data. Organisations must verify these devices are secure and functioning properly through regular security assessments, including vulnerability scans and timely software patching. Internal audit should verify that network segmentation is in place to contain breaches and that an up-to-date inventory tracks each device's security status. Proactive governance, testing and mitigation planning are essential to protect patient safety and maintain trust.

Patient access

Patient access is the gateway to the revenue cycle, directly impacting patient experience and financial outcomes. Internal audit should assess the efficiency, accuracy and compliance of key functions like scheduling, registration, insurance verification and financial counseling. Focus areas include ensuring accurate entry of patient and insurance data to prevent billing errors; verifying insurance eligibility before or at the time of service; confirming consistent, secure point-of-service collections; and maintaining compliance with regulations such as Medicare Secondary Payer rules and the No Surprises Act. Teams should stay current on payer policy changes and adjust processes accordingly. Optimising patient access reduces downstream issues and enhances transparency and trust.

Payer-Specific Priorities

Top Five Priorities



The top priorities of payer organisations demand an internal audit function focused on foresight, ability and building trust at scale.

01 Claims processing

Claims processing is a critical function in payer operations, involving steps from claim intake and adjudication to payment and communication with providers and members. Efficient systems are essential for financial stability and regulatory compliance. They must support coordination of benefits (COB), Medicare Secondary Payer (MSP) rules, integration with third-party administrators (TPAs), and much more. Payers must minimise risks such as improper payments, inefficiencies and noncompliance, while ensuring transparency and accuracy.

Key audit areas to consider:

- **End-to-end data review:** Evaluate the full data flow from claim receipt to payment and explanation of benefits (EOB) issuance. Critical areas of data review should include enrollment, provider contracting and credentialing, utilisation management (UM) and finance. Review IT general controls (ITGCs) and data governance to confirm data completeness, accuracy and compliance with standards like HIPAA.
- **Claims processing quality and efficiency:** Assess how performance is continuously monitored. Key metrics include auto-adjudication rates, processing time, payment accuracy and denial rates. Review quality assurance processes and the effectiveness of fraud detection and payment integrity functions.
- **Internal control structure:** Examine controls over claims processing, including segregation of duties, approval thresholds and manual processing checks. Verify changes to rules or policies follow proper change management and comply with regulations such as prompt payment laws.
- **Technology integration and automation:** Review how well systems are integrated (e.g., enrollment, provider contracting, medical management) to reduce errors. Identify manual bottlenecks and explore automation opportunities, such as Optical Character Recognition (OCR) for paper claims or AI for fraud detection.

Efficient and accurate claims processing is essential for financial health, compliance and patient trust, helping reduce waste and improving transparency across the reimbursement cycle.

02 Member impact and access to care

Maintaining a positive member experience and access to care is critical for payers. Two key areas are (1) enrollment and eligibility processes, and (2) handling appeals and grievances. Accurate enrollment processes prevent coverage errors, claims issues, revenue misalignment and member abrasion. A strong process facilitates correct premiums, proper claims payment, compliance with regulatory requirements, and financial stability.

Appeals and grievances are equally important. How a payer handles member dissatisfaction directly affects trust and access to care, which is compounded by intense regulatory scrutiny on improper denials. Appropriate grievance and appeal resolutions improve satisfaction and help to ensure compliance with regulatory standards, including timeliness and completeness. These processes also influence quality ratings like Medicare Star Ratings, which can impact enrollment and revenue over the long term.

Key audit areas to consider:

- **Appeal-decision appropriateness:** Review appeal samples for accuracy, timeliness and proper review procedures including appropriate clinical review when necessary. Confirm decisions are effectuated timely when appeals favor members and that notifications meet regulatory standards.
- **Grievance classification and resolution:** Validate complaints are correctly categorised as grievances and resolved within required timeframes, and that any quality-of-care issues are addressed appropriately. Audit responses for compliance with internal policies and regulatory requirements including completeness, clarity and timely communication.
- **Trend analysis of appeals and grievances:** Evaluate how trends in appeals and grievances are tracked and reported. Confirm processes that are in place to identify root causes and implement corrective actions for systemic issues are functioning as intended.
- **Enrollment and eligibility verification:** Test the accuracy of enrollment changes and communications. Confirm controls verify active coverage and compliance with federal and state rules, including CMS reconciliation.
- **Enrollment data and financial reporting:** Assess how membership data informs financial reporting. Validate that discrepancies between systems are reconciled and finance is alerted to changes affecting revenue.

03 Provider relationships

Strong provider networks are fundamental to a payer's success. Good relationships with healthcare providers help manage costs, maintain high quality of care, and enhance member satisfaction by offering adequate access to services. Poorly managed or inadequate provider networks can lead to compliance violations, higher fraud risk, operational inefficiencies and member dissatisfaction. Recent regulations, including CMS mandates on provider directory accuracy and network adequacy, underscore the critical need for robust oversight. Additionally, as payers transition to value-based care (VBC) models, strong provider relationships are essential for achieving performance benchmarks, reducing costs and helping to ensure optimal patient outcomes. Failure to manage these relationships effectively jeopardises organisational integrity and competitive positioning in the healthcare marketplace.

Key audit areas to consider:

- **Provider credentialing and compliance:** Assess the effectiveness of credentialing processes to verify all providers meet regulatory and organisational standards, minimising risks of fraud, noncompliance and patient safety concerns.
- **Provider directory accuracy:** Evaluate the accuracy and timeliness of provider directory data, assessing compliance with regulatory requirements and reducing member grievances related to access to care and network adequacy.
- **Contract configuration and payment integrity:** Review provider arrangements to determine alignment with contractual terms, accurate claims processing, and adherence to VBC performance metrics. Also, confirm that systems prevent paying claims at non-contracted rates for out-of-network providers unless authorised, and that any anomalies in payments (over payments or underpayments) are identified and rectified.
- **Provider network performance and adequacy:** Examine the oversight of provider networks, including monitoring performance benchmarks, network adequacy, and cost-effectiveness (potentially comparing pricing, leveraging the No Suprises Act machine-readable files), to support organisational goals and member satisfaction. Internal audit should verify that the provider network management team is proactively addressing any gaps in network adequacy or performance issues with providers.

Strong provider relationships are essential for a payer's success, including achieving performance benchmarks, reducing costs and helping to ensure optimal patient outcomes.

04 Product and sales

Payers must manage risks tied to products and sales strategies amid rising regulatory scrutiny and economic pressure. Key areas include agent and broker oversight and product-specific financial performance. Regulators like CMS are increasing scrutiny of agent marketing and enrollment practices, commission payments and monitoring of agents and brokers to validate compliance and protect consumers. Oversight of distinct product lines' financial performance, such as medical loss ratio (MLR), is essential for the payer's financial health and efficient operations, while helping to ensure that members receive quality care.

Key audit areas to consider:

- **Agent/broker oversight and commissions:** Review oversight processes for agents and brokers, verifying proper licensing, compliance training and adherence to marketing regulations (e.g., CMS rules for Medicare Advantage). Audit commission structures to confirm alignment with contracts and regulatory limits. For Medicare Advantage and Part D, verify that administrative payments comply with CMS guidelines and do not exceed fair market value, as well as avoid prohibited inducements for enrollment.
- **Agent/broker performance and compliance monitoring:** Assess whether the payer tracks agent performance metrics such as rapid disenrollment rates, complaints or enrollment errors. Verify a process is in place to identify and address inappropriate or fraudulent behavior. Confirm the existence of a formal audit or quality review programme, especially for high-volume agents.
- **Product MLR calculation accuracy:** Evaluate the accuracy of MLR calculation by auditing a sample of source data for premium revenue, claims expenses, quality improvement expenses and administrative costs. Compare MLR performance against industry benchmarks and competitors to identify potential areas for improvement.
- **Quality improvement and administrative expense validation:** Review processes for defining and tracking quality improvement and administrative costs and validate consistent application of guidance provided to staff regarding these expense types. Confirm processes are in place to evaluate existing and potential quality-improvement activities to improve member health outcomes and provision of appropriate care.

05 Risk adjustment/coding

Risk adjustment — especially the Hierarchical Condition Category (HCC) model used in Medicare Advantage and some Exchange plans — remains under intense regulatory scrutiny. Agencies like CMS and the OIG are actively auditing to identify unsupported diagnosis codes, which can lead to overpayments. CMS has intensified its Risk Adjustment Data Validation (RADV) audits and now has authority to extrapolate findings across a payer's population, potentially resulting in significant recoupments; OIG risk-adjustment audit findings may also now be extrapolated. Conversely, undercoding can reduce payments, potentially impact member care and hurt revenue. Accurate coding is essential for compliance, appropriate clinical care and financial integrity.

Key audit areas to consider:

- **Risk adjustment process controls:** Evaluate end-to-end processes, including deletion of unsupported diagnoses within CMS's 60-day window, reconciliation of diagnoses accepted by CMS, and oversight committee involvement. Verify provider education and feedback mechanisms are in place.
- **Accuracy of risk adjustment coding:** Independently review member medical records to confirm submitted diagnoses are supported by the documentation. Focus on high-risk conditions flagged by the OIG and use tools like the OIG High-Risk Diagnosis Codes Toolkit. Watch for red flags like one-time diagnoses without follow-up care and unlikely codes such as a cerebrovascular accident coded at a provider's office.
- **RADV and OIG audit readiness:** Assess preparedness for RADV or OIG audits. Confirm the existence of sufficient team resources, retrieval protocols for medical records, and access to external coding or legal experts. Validate past audit findings have been addressed and that a strategy is in place to respond to any findings and extrapolated penalty amounts.

As government organisations actively audit to identify unsupported diagnosis codes, provider organisations continue to face intense regulatory scrutiny, making accurate coding essential.

Payer-Specific Priorities: Additional Areas of Focus

Medical management

Medical management helps payers control costs while facilitating appropriate care. Key areas include utilisation review, case and disease management, and wellness programmes. Internal audit should verify that utilisation review practices like pre-authorisations post-service reviews are functioning correctly to confirm the appropriateness of care and optimise resource utilisation. Review case and disease management programmes for effectiveness in identifying and supporting high-risk members and reducing redundant or unnecessary services. Assess strategies for proactive health management and preventive measures – such as annual wellness visits, vaccines and medication adherence programmes – to reduce costly long-term treatments. Evaluate how success is measured (e.g., reduced ER visits) and confirm monitoring of key metrics. By employing appropriate medical management techniques, payers can facilitate the delivery of timely and appropriate care to members, ultimately reducing expensive long-term healthcare expenditures.

Benefit configuration

Accurate benefit configuration in claims systems is critical to prevent improper payments and member dissatisfaction. Internal audit should assess how insurance product designs (e.g., copays, deductibles, covered services, exclusions, out-of-pocket maximums) are translated into the claims adjudication system. Misconfigurations can result in overpayments, underpayments or denial of covered services – leading to compliance risks and financial loss. Auditors should test sample benefit scenarios, such as verifying that preventive services are paid at 100% or that no cost sharing applies after the out-of-pocket maximum is met. Additionally, verify that member materials (e.g., Evidences of Coverage, benefit summaries) align with system configurations. Discrepancies can cause member abrasion and regulatory complaints. Pay special attention to recent benefit changes or new products, as these are more prone to setup errors. Benefit configuration is key to ensuring accurate coverage and cost-sharing amounts while reducing financial leakage.

Utilisation management/behavioral health

Utilisation management (UM) and behavioral healthcare management are under regulatory scrutiny to prevent inappropriate delays or denials and help to ensure equitable access to care. Internal audit should confirm that UM decisions align with nationally recognised guidelines and that MA plans follow traditional Medicare coverage policies. Confirm that AI use in UM processes includes human input when necessary, that decisions are appropriate, and that no algorithmic bias exists. For behavioral health, confirm compliance with parity laws – limits must not be more restrictive than for medical/surgical care – by comparing prior authorisation and denial rates across behavioral and medical services. Also, confirm that UM practices don't inappropriately restrict access, such as denying preauthorised services as not medically necessary. Lastly, verify that UM policies do not discriminate based on age, race, disability or mental health status. Effective UM and behavioral health practices help increase member satisfaction and help to ensure the provision of medically necessary care.

Delegation oversight

Payers often delegate functions (e.g., network management, UM, claims, pharmacy benefits) to specialised vendors, provider groups, or other First-Tier, Downstream and Related entities (FDR). While this can enhance efficiency, the payer remains accountable for delegates' actions. Internal audit should assess the payer's oversight practices for its delegates to confirm they include a review of delegate agreements for contractual obligations (e.g., reporting, performance) and evaluation of compliance with regulatory requirements for both compliance programmes and operations via sample review. Confirm the delegation oversight programme reviews data security measures and the delegates' HIPAA privacy protections, possibly via SOC reports or security audits. Verify adherence to performance reporting requirements (e.g., claims timeliness, call stats) and that the payer reviews and enforces contractual standards, including corrective actions and penalties when warranted. Effective oversight helps detect issues early and mitigates risks such as regulatory penalties or service failures

Pharmacy benefit manager (PBM) oversight

PBMs manage prescription drug benefits and can significantly affect costs and member experience. Their contracts are complex, involving pricing guarantees, rebates and clinical programmes. Internal audit should assess PBM oversight, starting with contract compliance – confirming pricing guarantees and rebate sharing are transparent and accurate – and compliance with regulatory requirements. Coverage determinations should be audited for correct application of cost sharing and rules like quantity limits and transition fills. Review formulary management to confirm changes and prior authorisations are properly implemented and compliant. Evaluate fraud, waste and abuse programmes for effectiveness in detecting misuse. Lastly, confirm the payer receives and uses key performance metrics (e.g., generic dispensing rates, adherence, call center performance). Poor PBM oversight can lead to financial loss, compliance issues and member dissatisfaction. A strong audit framework helps to ensure value delivery and regulatory alignment

In Closing

“

While the absence of artificial intelligence from the top internal audit priorities may raise eyebrows, it's not an oversight — it's a reflection of reality. Despite 90% of respondents reporting AI usage, only 11% claim high proficiency, signaling a wide maturity gap across healthcare provider and payer organisations. Internal audit teams are beginning to explore AI use cases for their own operations, but few have yet placed it firmly on their internal audit plans. This moment presents both a challenge and an opportunity.

As AI adoption accelerates, so too must internal audit's role in ensuring responsible use. It's time to shift from passive observation to active governance. Internal auditors must not only harness AI to enhance their own capabilities but also scrutinise how their organisations are managing the risks and ethics of this transformative technology. Furthermore, according to Protiviti's recent AI Pulse Survey, most companies interested in AI are in the exploration or testing stage. Fewer than 11% of organisations have achieved full transformation.[1] However, the momentum is only going to continue to grow, and the pace of that growth is rapidly increasing. The future of internal audit in healthcare will be shaped not just by what we examine, but also the manner in which we are able to keep pace with our organisation's transformative initiatives.

– **Matt Jackson**
Healthcare Internal Audit Leader

Additional insights coming soon

Be on the lookout for the release of the second piece of this study soon that will highlight a variety of internal audit benchmarking insights.

[1] *From Exploration to Transformation — What AI Success Looks Like*, Protiviti, July 2025: www.protiviti.com/us-en/survey/ai-pulse.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collabouration 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 11th 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 collabourative, 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.

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

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

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

THE AMERICAS

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

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

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®