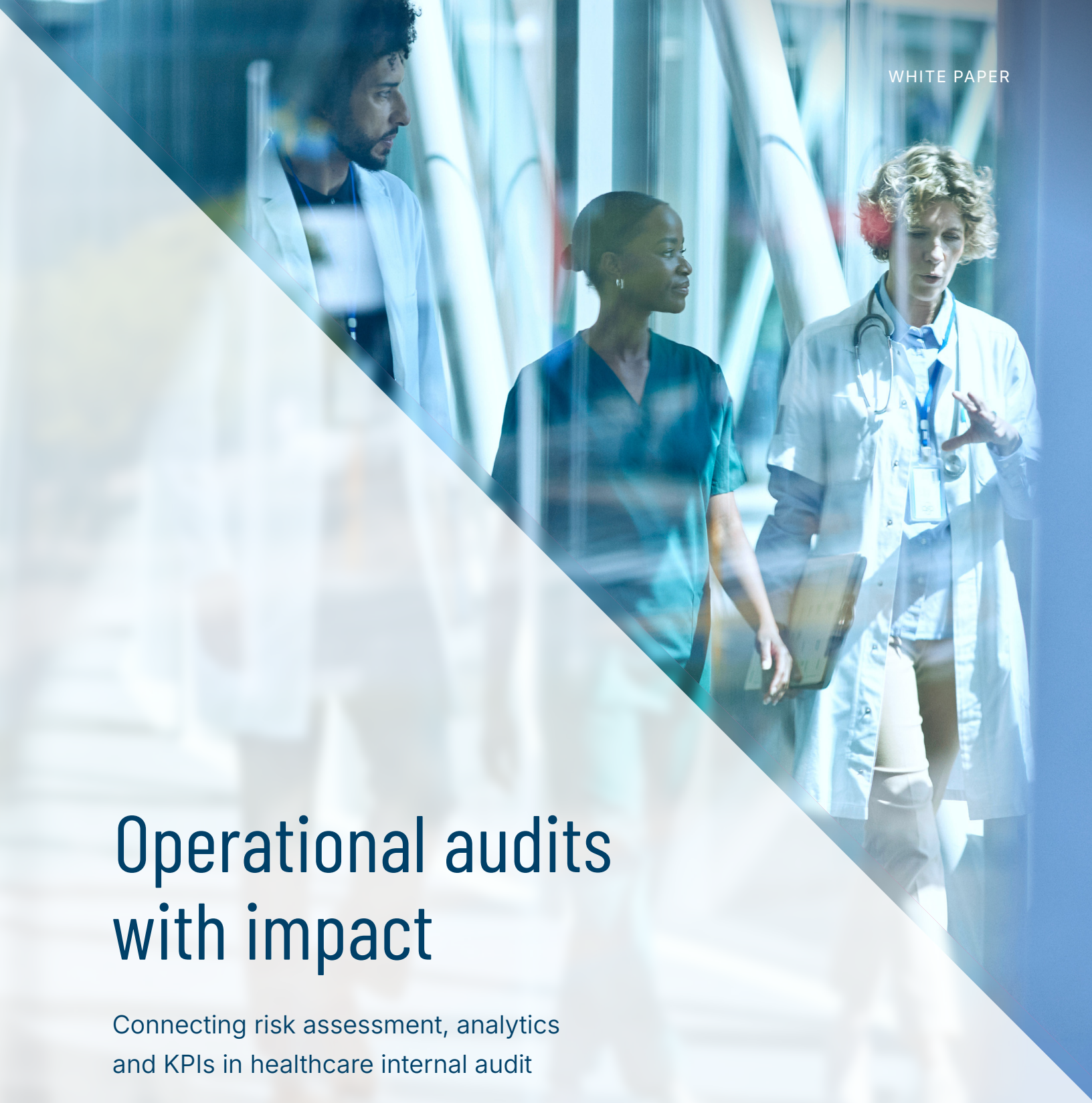


WHITE PAPER

Operational audits with impact

Connecting risk assessment, analytics and KPIs in healthcare internal audit

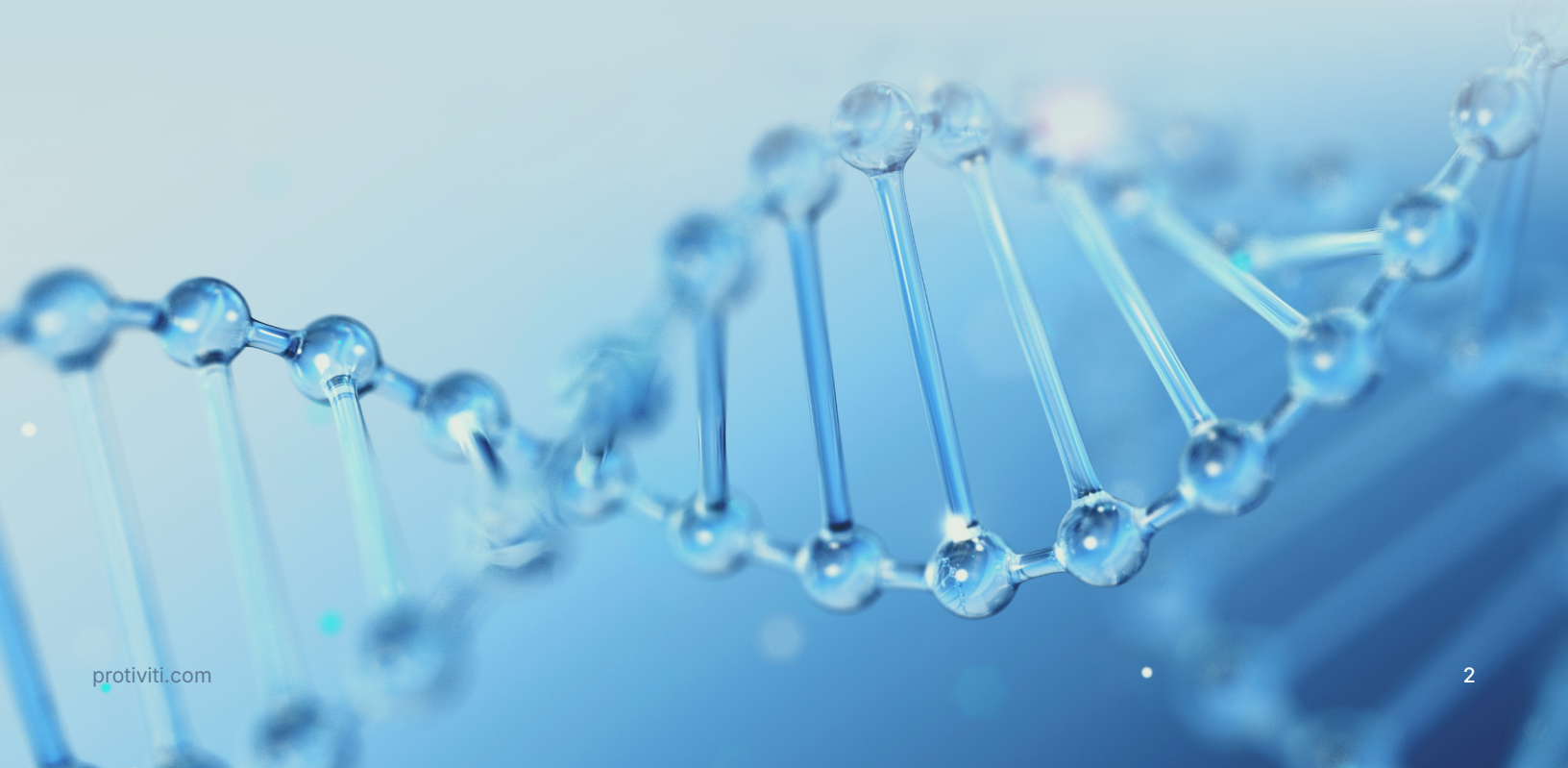
BY CAROLINE ZNANIEC, MBA, MS-HCA, CRIP, CRCR;
ZACH CHRISTIANSON, CPA; AND PAULA VASQUEZ, MHA

ahia
Assoc. of Healthcare Internal Auditors

protiviti®
Global Business Consulting

Contents

Executive summary	3
Introduction: The strategic shift in healthcare internal audit	5
Why operational audits matter now	8
Six components of a repeatable methodology for operational audits	9
Preserving independence: Audit-safe engagement models	17
Application across operational areas	18
Case studies: Methodology in action	20
Demonstrating value and ROI to leadership and boards	26
Conclusion	27



Executive summary

Healthcare organisations face growing pressure to connect operations, financial performance, and risk, particularly to identify opportunities to improve performance and address areas that drive cost savings or decrease revenue variability. Increasingly, they turn to internal audit for this insight, looking for a more precise view of what is working, what is exposed and what needs attention. To meet this expectation, internal audit is expanding beyond financial and compliance coverage to assess operational efficiency, effectiveness and controls across key functions. This includes increasingly becoming a strategic partner of the organisation through the use of data analytics and artificial intelligence (AI) to identify, prioritise and evaluate risk, including where weak governance and broken processes quietly leak value the organisation could recover.

BENCHMARK SIGNAL

Internal audit's future is increasingly tied to analytics and technology-enabled insight.

92%

of CAEs view data analytics as the most important technology skill for the future.

4 in 10

say they are already using generative AI in internal audit activities.

Source: **2025 North American Pulse of Internal Audit (Internal Audit Foundation/The IIA).**

Operational audits keep internal audit firmly in its assurance role, not in management's. They extend assurance by evaluating whether performance, financial outcomes and emerging technologies are governed, measured and sustainable. In doing so, they draw on internal audit's core strengths of independent evaluation, disciplined analysis and risk-based insight without shifting accountability away from management.

This white paper lays out a practical, healthcare-specific approach to operational auditing as a means of delivering operational performance assurance. It presents a repeatable methodology that integrates risk assessment, analytics and key performance indicator (KPI) monitoring from planning through follow-up to support more measurable and defensible audit insights. Recognizing that AI is reshaping how audit teams work and how provider organisations operate, this paper treats AI as both an enabler of audit insight and a growing area requiring governance.

BENCHMARK SIGNAL

Analytics and AI are reshaping healthcare internal audit.

94%
of respondents currently use AI in internal audit.

63%
are already performing AI governance engagements.

49%
use data feeds or analytics to inform their risk assessments.

The study also notes that internal audit can use analytics and AI-enabled innovation to move beyond point-in-time testing and identify operational breakdowns that create measurable financial exposure while management retains responsibility for remediation.

Source: **2026 AHIA and Protiviti Healthcare Internal Audit Plan Priorities** study.

Case studies cover the operational areas chief audit executives (CAEs) keep raising, including revenue cycle integrity, payer behaviour and clinical audits. As health systems lean harder on AI, each of these operational areas inherits a fresh set of questions about validation, monitoring and accountability that internal audit cannot ignore.

Introduction: The strategic shift in healthcare internal audit

Internal audit is playing a broader role in helping healthcare organisations understand risk, performance and financial outcomes. While financial and compliance coverage remains foundational, boards, audit committees and CAEs are increasingly expecting internal audit to identify operational risks earlier, quantify their impact and highlight where performance gaps may affect financial results.

Operational audits are not new, but the expectations around them are changing. CAEs are increasingly being asked to evaluate whether the operational drivers of performance are governed, measured and working as intended, and to connect those conclusions to financial, compliance and strategic outcomes. This aligns with the broader evolution of internal audit toward risk and decision intelligence, where internal audit provides timely, relevant risk context before decisions and outcomes are fixed.

These expectations reflect the operating environment healthcare organisations now face. Growth, system integration and changes in care delivery have introduced variations in processes, data definitions and performance measures across the enterprise.

Many organisations are still working through the effects of recent disruptions, with underlying systems and workflows that were never fully aligned. As a result, performance can be difficult to interpret. KPI monitoring may be fragmented and definitions may differ across entities. Leadership reporting may reflect inconsistency rather than true operational performance.

Operational audits help address this challenge. They evaluate efficiency, effectiveness and control across clinical, operational and administrative functions, and connect operational performance to financial impact by identifying where process breakdowns, data inconsistencies or control gaps create measurable risk.

> Operational audits are the engagement-level mechanism through which internal audit provides operational performance assurance.

None of this changes internal audit's core role of providing independent assurance over governance, risk management and control processes while delivering insight that helps the organisation create, protect and sustain value. Operational audits bring clarity to complex operating environments by validating KPI definitions, tracing data across systems and identifying where performance variation reflects real exposure. Data analytics and AI support this work by enabling broader testing, faster identification of anomalies and more focused evaluation of risk areas, while judgement and conclusions remain with the auditor.

Used well, analytics and AI do more than accelerate traditional audit procedures. They expand internal audit's ability to connect operational performance, financial outcomes and risk in a way that is more measurable and actionable. The following graphic illustrates how that shift broadens internal audit's contribution from assurance alone to a more value-focused role.

BENCHMARK SIGNAL

Analytics is becoming the engine behind internal audit's shift to measurable impact.

From control & compliance → to value & impact

92% of CAEs say data analytics is crucial to internal audit's future.

28% rate their function's data capabilities as high or advanced.

Key focus areas

- Revenue integrity
- Clinical operations
- 340B compliance

Metrics tracked

- Cost savings
- Cash recoveries
- Denial reductions

Common outcomes

- Margin unlocked
- Reduced write-offs
- Improved governance

Reporting to stakeholders

- ROI analysis
- KPI dashboards
- Board-level insights

Source: **2025 North American Pulse of Internal Audit (Internal Audit Foundation/The IIA).**

This white paper offers a practitioner's view of how to design and execute operational audits, while clearly communicating the value of operational audits to leadership and boards. It covers five key questions that CAEs are asking right now:

Five questions CAEs are asking

- Which operational risks actually matter, and how do we prioritise coverage when resources are limited?
- How do analytics and KPI monitoring make audits more rigorous, more continuous and more credible to leadership?
- How do we demonstrate measurable impact while preserving independence and objectivity?
- How do we collaborate across compliance, revenue cycle integrity, operations and finance while staying in an assurance role?
- How should internal audit use AI and automation to improve its own performance while also providing assurance over the organisation's AI-enabled processes?

Why operational audits matter now

Healthcare organisations have less tolerance for operational inefficiency. Labour costs, supply chain pressures, payer dynamics, denial activity, compliance requirements and technology investments all originate in operational processes and ultimately affect financial performance.

BENCHMARK SIGNAL

Internal audit's focus extends beyond financial audits.

18% *of internal audit time budgeted by audit area is to financial or accounting audits (the rest are IT and cyber, operational, compliance, etc.).*

Source: **2026 AHIA and Protiviti Healthcare Internal Audit Plan Priorities study.**

As a result, audit committees and CAEs are increasingly expecting internal audit to have greater visibility into how operations are designed and performed. This includes earlier involvement in areas where strategy, transformation and technology investments shape performance, so that risks, assumptions and controls are understood before issues surface.

Internal audit provides an independent view on whether processes, controls and technology investments are producing measurable and sustainable results.

Three forces are driving this shift:

1. **Margin recovery has become an enterprise priority.** Chief financial officers (CFOs) and operating leaders are looking for unlocked margin everywhere. Internal audit can support that effort by identifying where governance gaps, control weaknesses, process variation or data issues are limiting value realisation.

2. **Data is increasingly more usable at scale.** Electronic health record (EHR) platforms, enterprise resource planning (ERP) systems and analytics tooling allow internal audit to analyse entire populations instead of testing a few samples from the population, benchmark internally and externally, and monitor KPIs continuously. AI accelerates pattern recognition, exception triage and synthesis on datasets that have outgrown manual review.

3. **Stakeholders expect impact, not just findings.** Boards and audit committees want outcomes, dollars and forward-looking insight, not just another list of control gaps. As AI spreads, that expectation grows to include assurance on whether new technology is improving performance in a controlled, quantifiable and explainable way.

The opportunity is real, and it comes with a fair question: How does internal audit deliver this without sliding into management's role? The methodology that follows is designed with that line in mind.

Six components of a repeatable methodology for operational audits

A strong operational audit program rests on a methodology that is repeatable and explicit about how risks, analytics and KPI monitoring reinforce one another. The six components below outline a framework that starts with planning all the way through to follow-up, and which scales from a single audit to a full annual internal audit plan. Together, these components help internal audit move from periodic operational review toward operational performance assurance that is more continuous, data-supported and useful to leadership's decision-making.

Table 1. Operational audits framework

Methodology component	What it delivers
Operational risk universe	A single enterprisewide view of where risks actually live, including coordination with other risk management functions, so audit coverage targets real exposures instead of last year's topics
Risk scoring and heat mapping	A repeatable, defensible way to rank risks that makes concentrations and blind spots visible instead of debatable
Controls self-assessment	Earlier warning on emerging risks, and a risk view that process owners validate frequently rather than internal audit validating after the fact
Stakeholder interviews and subject-matter expert (SME) integration	Sharper scoping and faster root cause identification, with credibility that comes from reading the workflow the way operators do
Data analytics and benchmarking	Risks and opportunities sized in dollars, days, denials or defects, with full-population analysis and peer benchmark comparison in place of sample testing
KPI monitoring and continuous auditing	Near real-time visibility showing improvement over time and letting the team reprioritise before a risk becomes a finding

Connecting risk assessments, analytics and KPI monitoring is at the heart of this methodology. Treated as one system rather than three separate disciplines, each reinforces the others. Risk assessments help determine which analytics matter, analytics quantify the risks and the opportunities, and KPI monitoring creates the ongoing visibility needed to support continuous auditing. Anchored in well-governed data and clear audit objectives, AI can tighten that loop, helping the team synthesise faster and see patterns sooner. The sections that follow walk through each of the six components in turn, grounded in the realities healthcare provider organisations face.

1. Operational risk universe

The risk universe is the starting point for operational auditing. It defines where risks exist across the organisation in a structured way, rather than as a list of audit topics.

Internal audit brings together key inputs including strategic and operating plans, enterprise risk assessments, quality and compliance priorities, regulatory and payer changes, KPI dashboards and prior audit results. The process is most effective when coordinated with other risk management functions, including compliance, enterprise risk management, legal, privacy, information security and quality, allowing internal audit to leverage existing risk insights, identify areas of overlap or emerging exposure, and align assurance coverage across the organization. These inputs are used to identify where performance varies, where risks are emerging and where control effectiveness may be uncertain.

From there, risks are organised into a consistent structure across major domains such as revenue cycle, clinical operations, workforce, supply chain and technology-enabled processes. This allows internal audit to compare risks across the enterprise and align coverage to what matters most.

The universe is refreshed on a defined cadence through reassessment of these same inputs, along with ongoing monitoring of KPI trends and operational changes. As technology becomes more embedded in workflows, this includes identifying where tools such as AI and automation are influencing decisions, performance or reporting, and ensuring those areas are visible within the risk landscape.

2. Risk scoring and heat mapping

Scoring is valuable when it is data-driven and transparent. A sound approach weighs likelihood and impact, velocity (how quickly the risk could materialise), how much it amplifies other risks, and how well management already covers it. A heat map then visualises risk concentrations and brings underweighted areas into focus, creating a consistent view for operating leaders and the audit committee to compare risks and set coverage priorities.

3. Controls self-assessment

A controls self-assessment (CSA) brings process owners in as risk partners and gives internal audit a sharper read on risk. Where a standard annual risk assessment asks what could go wrong, CSAs ask how risks are handled right now, including the controls, ownership and day-to-day practises that decide whether mitigation is working. A CSA run as a design-thinking workshop or a structured survey allows internal audit to validate the risk universe, test whether controls operate as intended and identify emerging risks earlier than the annual cycle ever could.

A CSA works best when everyone starts with a shared vocabulary. Operational leaders rarely think in audit terms, and what they call a control may differ from what internal audit documents into a risk-and-control matrix (RCM). A structured survey across operating leaders, paired with a short workshop to align terminology, gives internal audit a faster and truer picture of the control environment than annual interviews alone. Internal audit can vet the responses with management, confirming what is operating as designed, surfacing where intent and practise part ways, and identifying risks before they ever reach a heat map. The discipline is collaborative, not adversarial; it trades sampling-in-a-vacuum for an ongoing dialogue at ground level.

That pays off where AI sits in the workflow. In those conversations, process owners often name the AI tool itself as the control. However, the controls that matter usually sit around the AI — data quality, human review of the output, the ability to override, escalation when something looks wrong and ongoing monitoring. The ambient documentation case study in this white paper (page 23) is a concrete example of this distinction.



4. Stakeholder interviews and SME integration

Stakeholder interviews and having the correct subject-matter expertise can sharpen the credibility and effectiveness of operational audits, especially in clinically complex or heavily regulated areas. Pairing structured interviews with targeted clinical and regulatory expertise allows the team to ask sharper questions and interpret workflow realities accurately, all while maintaining independence and objectivity.

This matters most with AI. A stakeholder may rely on an AI tool every day without it ever appearing in a policy, a standard operating procedure (SOP) or a process map, so the documentation gives no sign the AI tool is shaping operational processes. The only reliable way to find out if the tool is in use and to understand how it affects accuracy, decisions and controls is to talk to the clinicians, operators, data teams and compliance leaders closest to it.

BENCHMARK SIGNAL

Credible assurance increasingly rests on specialised expertise.

96% *of respondents agreed that experienced auditors will need to strengthen their skills, including their technological knowledge, to remain relevant and audit new and emerging risks.*

Source: Internal Audit: Vision 2035 — Creating Our Future Together (Internal Audit Foundation/The IIA).

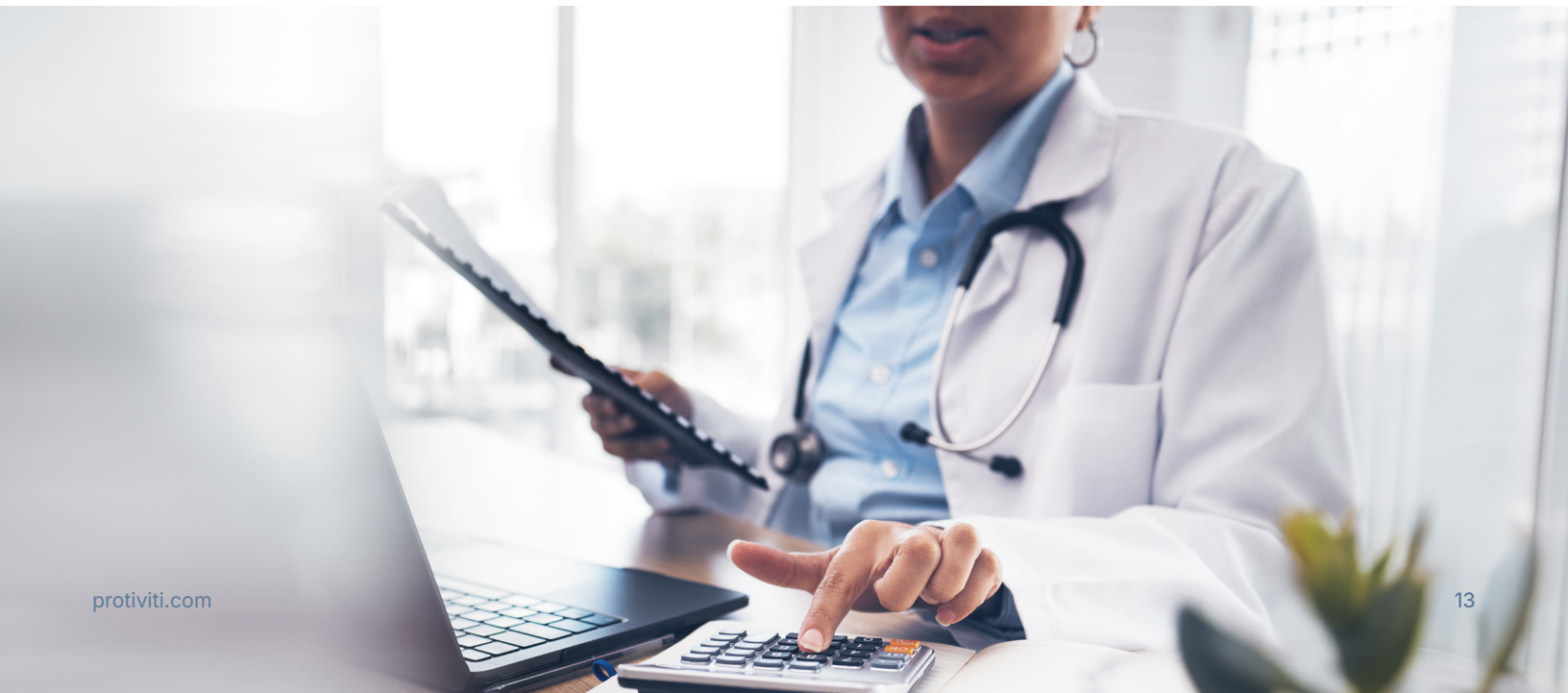


5. Data analytics and benchmarking

Analytics in planning and execution

Most healthcare organisations already hold the data they need for analytics-enabled operational auditing. The challenge is rarely access. Rather, it is architecture, reconciliation and auditability. Internal audit's role includes leveraging source data, governed reporting layers and external benchmarks to support defensible conclusions, maintain consistent KPI definitions and enable repeatable testing across the enterprise. Internally, these sources fall into two groups: clinical and operational reporting, and enterprise finance and revenue cycle systems.

On the clinical and operational side, stakeholders often rely on built-in reports in source systems, such as the EHR, for day-to-day monitoring, then turn to an enterprise data warehouse for further analysis, where they evaluate the full population, track trends and compare facilities. These sources matter most when operational audits need to connect care delivery and patient flow to performance and financial impact, through measures such as utilisation management and level-of-care decisions (including observation versus inpatient status), length of stay, throughput and patient access, case mix index, and readmissions. This is also where inconsistent definitions surface, such as how length of stay or service lines are calculated from one facility to the next, which can distort enterprise-level KPIs much the way cost centre or payer hierarchy issues do on the financial side. For internal audit, an enterprise data warehouse is a better starting point because it gives standardised data pulls, clearer logic, and reporting that can be traced and reproduced, while one-off queries alone cannot. AI adds value by accelerating summarisation, flagging anomalies and grouping recurring exceptions.



On the finance and revenue cycle side, enterprise finance and revenue cycle systems hold the system of record for general ledger activity, budgeting, forecasting, management reporting, labour data and cost allocation inputs. These data sources are critical when operational audits need to connect workflow performance to financial impact. In revenue cycle, this may include measures such as denial rate, net revenue yield, accounts receivable (AR) ageing, write-offs or throughput-related margin effects. In workforce-focused reviews, it may include labour productivity, premium pay usage, contract labour dependency, staffing-to-volume alignment or cost per adjusted discharge. In supply chain, it may include purchase price variance, inventory turnover, stockouts, expired supplies, backorder trends, item master consistency, or the alignment between supply utilisation, documentation and downstream charge capture.

These systems are also where internal audit often finds structural issues that can distort performance reporting. Examples include cost centres mapped differently across facilities, service line attribution that is not applied consistently, payer hierarchies that roll up differently by business unit, or supply categories that are not standardised across purchasing and clinical systems. These issues may not appear material at the transaction level, but they can materially affect KPI reliability and management reporting once data is aggregated across the enterprise. Where AI is introduced into these environments, its most practical contribution is often faster variance analysis, pattern recognition and triage of exceptions for review.

These issues in underlying data also underscore why data confidence matters before analytics or AI can be scaled responsibly. Protiviti's AI Pulse survey, *When AI Readiness Meets ROI Reckoning*, found that data quality, accessibility, governance and literacy are foundational to trustworthy AI, and that organisations where AI ROI significantly exceeds expectations nearly always (97%) report confidence in their data capabilities. For internal audit, the implication is practical. Analytics and AI can accelerate insight, but only when the underlying data can be reconciled, governed and explained.

PRO TIP

What data-enabled delivery looks like in practise

A strong analytics approach combines internal system data with independent views of claims submissions and payer remittance activity. Comparing what was billed to how it was adjudicated provides a more complete and objective view of revenue cycle performance. It highlights denial trends, underpayments and variation in coding or billing that internal reporting alone may not fully capture.

This becomes increasingly important as both payers and providers expand their use of AI in claims review and prior authorization, which can introduce new patterns of variation and risk.

For internal audit, the value is not the dashboard itself, but the insight it provides. This type of analysis helps focus attention on measurable exposures and supports more dynamic monitoring by identifying where payer behaviour is shifting and where performance or compliance risk may be increasing.

Benchmarking

Benchmarking gives internal data context. It helps internal audit determine whether observed performance differences reflect true variation or are driven by inconsistent definitions, reporting logic or organisational structure. This is most effective once metrics have been normalised across facilities. Without that step, benchmarking can confuse interpretation rather than clarify it.

When applied appropriately, benchmarking turns observations into actionable insights. It highlights where performance differs in a meaningful way and where further review is warranted. This is especially relevant in areas such as revenue cycle performance (e.g., denial rates, AR days, write-offs), clinical operations (e.g., length of stay, throughput, readmissions) and workforce performance (e.g., productivity, staffing efficiency, alignment to quality and value outcomes).

External benchmarks, such as published industry data along with internal cross-facility comparisons, provide additional context and credibility. For internal audit, these comparisons strengthen conclusions and support more focused and defensible recommendations.



PRO TIP

Putting the audit library to work

Internal audit teams are increasingly building audit libraries that include prior plans, work programs, test results and reports. AI-powered search and summarisation allow internal audit to quickly identify what has been reviewed; what did and did not have exceptions; themes of issues over years, across facilities, etc.; and where additional action may be most valuable.

This reduces time spent on retrieval and allows audit teams to focus on higher-value activities, including evaluating results, identifying patterns across audits, and reporting insights that inform decision-making.

6. KPI monitoring and continuous auditing

KPI monitoring turns audit insights into a sustained operating discipline. The most effective internal audit functions partner with operational leaders to settle on a short list of KPIs per audit area, automate the data feed where possible and review trends on a set cadence. Over time, that grows into continuous auditing — recurring tests of controls and KPI thresholds that flag issues between formal audits.

Continuous monitoring is also what keeps coverage aligned to risks as they move. Healthcare risks evolve faster than annual plans, so a mature programme builds in elements such as periodic reprioritisation throughout the year, flexible resource allocation, and a feedback loop that runs from monitoring outputs back into the audit plan. The result is an audit plan that flexes when a payer rewrites a denial policy midyear, when a major IT system goes live, or when a state regulator opens an inquiry that pulls audit attention to a specific service line. AI-driven processes raise the same need. A new use case, a changed model or a moving governance bar can create assurance needs not prioritised during annual planning.

Used together, these techniques close the gap between a point-in-time finding and the operational reality leaders manage every day. They also move internal audit closer to the point of decision, giving leaders risk context while outcomes can still be influenced rather than after the fact.

PRO TIP

Watching KPI outliers at scale

Trending data alone does not identify where action is needed. It shows what is changing, but not why it changed, why the change matters or what to do next.

Once a KPI feed is automated, AI can help close that gap. It can flag outliers, summarise what is driving them and route exceptions to the appropriate owner.

This allows human judgement to focus faster. Internal audit still evaluates the results, determines significance and drives conclusions so the audit itself remains with the auditor.

Preserving independence: Audit-safe engagement models

Operational audits succeed only if they preserve internal audit's independence and objectivity. CAEs are right to push back on engagement models that drift toward co-management, as audit committees are watching closely. The good news is that independence and impact coexist when an engagement is layered and phased deliberately.

Internal audit brings an enterprise view and board-level visibility that operational functions often lack. Framed as assurance over risk, performance and controls, it can help leaders prioritise margin and return on investment (ROI) while keeping ownership and decision-making with management. Three principles guide audit-safe engagements:

01

Layered scope

Keep assurance and advisory separate in scope, deliverables and reporting. When advisory follows assurance, close and document the assurance scope before the advisory phase begins.

02

Phased delivery

Sequence the work so the same team doesn't re-audit its own recommendations without a safeguard such as rotation, peer review or external assurance.

03

Transparent governance

Document the independence considerations into the engagement charter, surface them to the audit committee and revisit them annually as the scope evolves.

Disciplined scoping matters just as much. Before fieldwork starts, internal audit should use focused scoping discussions to pinpoint where the real exposure sits, where management already suspects a problem, where operational data shows meaningful variances, and where leadership has lost visibility. Concentrating audit efforts on these areas, rather than distributing them thinly across lower-value topics, keeps the work focused and high-impact. With AI-enabled workflows, scoping should spell out whether the audit is assessing the model itself, the processes around it, the data feeding it, the decisions it drives, or all four of these areas.

Used consistently, these practises allow internal audit to engage high-impact areas including revenue cycle integrity, payer behaviour and operational improvement initiatives without compromising the standards that give its voice weight.

Application across operational areas

The six methodology components listed previously apply across the operational areas CAEs continue to raise as concerns. Table 2 on the following page provides examples of how the audit lens, analytics and focus on KPI monitoring can translate across domains. The case studies that follow illustrate the methodology in action.

As these approaches mature, AI becomes a natural extension of the process. It is most relevant where it supports workflow design, decision support or reporting logic by helping identify patterns, prioritise exceptions and accelerate analysis, while leaving judgement and conclusions with the auditor.

Operational risk rarely respects functional boundaries. A denial trend is at once a revenue cycle integrity issue, a potential compliance issue, an operational breakdown and a financial exposure, which is why credible operational auditing depends on working across compliance, revenue cycle integrity, operations and finance rather than treating any single function as the sole owner. Internal audit's role is deliberate. It convenes these functions, reconciles their data and competing definitions, and tests the controls between them. The case studies that follow show the pattern. In each, internal audit surfaced and quantified the risk, while the functions it engaged retained accountability for acting on what the data and auditor surfaced. That separation is what lets collaboration sharpen an audit's insight without eroding its independence.



Table 2. How internal audit evaluates operational risks and enables value

Operational area	What internal audit evaluates	What it enables
Revenue cycle integrity and charge capture[1,2]	Workflows, controls and data that drive billing accuracy, denials, timely filing, timely appeals and reimbursement outcomes	More consistent reimbursement, reduced leakage and stronger governance
Clinical and operational performance	Care delivery and patient flow (e.g., utilisation management and readmissions), and KPI definitions for length of stay and throughput as well as the data behind them	Improved efficiency, reduced variation, and clearer links between clinical performance and financial outcomes
Provider coding and documentation[3]	Coding accuracy, documentation support for billed services, diagnosis specificity, modifier usage and alignment between clinical documentation and coded claims	Quantified recovery opportunities, reduced compliance exposure and audit-ready governance
Pharmacy, 340B and program integrity[4]	Reimbursement accuracy, program compliance, payer behaviour and reporting reliability for high-risk pharmacy-related areas such as 340B	Quantified recovery opportunities, reduced compliance exposure and stronger program oversight
Workforce and productivity	Alignment of staffing, productivity and performance metrics to operational outcomes	Better alignment of resources to demand, and improved efficiency and sustainability
Technology-enabled processes (ERP, EHR)[3]	System configuration, workflow adoption and control design supporting operational performance	Improved data reliability, reduced manual work and stronger return on technology investments

1 *Refer to case study 1: From workqueue governance audit to cash optimization*

2 *Refer to case study 2: From denials analytics to enterprise revenue recovery*

3 *Refer to case study 3: Ambient documentation review*

4 *Refer to case study 4: 340B underpayment identification and recovery*

Case studies: Methodology in action

The case studies on the following pages are not intended to highlight specific outcomes as much as they illustrate how the methodology can be applied across different operational and risk domains. Each example demonstrates how internal audit used risk assessment, analytics, stakeholder engagement and/or KPI monitoring to evaluate risks, develop assurance insights and help management better understand operational and financial exposures. The examples vary by subject matter, but the underlying approach remains consistent.

Case study 1:



From workqueue governance audit to cash optimization

Case study 2:



From denials analytics to enterprise revenue recovery

Case study 3:



Ambient documentation review

Case study 4:



340B underpayment identification and recovery

Case study 1: From workqueue governance audit to cash optimization

Internal audit evaluated governance over accounts approaching timely-filing and timely-appeal deadlines. The central question was whether oversight, prioritisation and monitoring controls were designed and operating effectively to prevent avoidable write-offs and keep reimbursement on schedule.

The audit found that competing priorities, limited staff bandwidth and a lack of system prioritisation meant accounts were not being worked in order of filing urgency. As a result, the organisation carried the greatest financial exposure on precisely the accounts that needed the earliest intervention.

Internal audit identified a set of targeted, practical improvements:

- **Earlier visibility:** Leverage Epic dashboards to flag at-risk accounts before deadlines become critical.
- **Data integrity:** Maintain accurate payer filing and appeal deadlines within the system.
- **Stronger governance:** Tighten prioritisation and escalation controls for high-risk queues.

The audit also surfaced adjacent opportunities in denial workflows, operational efficiency and process standardization. As a longer-term measure, recommendations included structured staff training and fuller use of system capabilities, so the system routes staff to the highest-dollar, highest-risk accounts first rather than leaving that judgement to an individual's discretion.

Over the trailing 12 months, the audit delivered measurable gains in cash and control:

- **1,632% ROI** delivered through improved prioritisation, timely follow-up and stronger oversight of deadline-sensitive accounts.
- **Approximately 175 to 200 at-risk accounts per week** actively managed, amounting to $4 million in gross revenue, a running measure of the exposure being controlled.
- **Internal audit's collaboration with the organisation expanded** from a point-in-time audit into ongoing advisory and oversight for cash optimization, now extending into denial prevention and revenue recovery.

This is an audit-led pathway in its clearest form. Internal audit identified the risk, used system data and workflow observation to pinpoint where reimbursement was leaking, and recommended governance and process improvements that delivered immediate and ongoing financial benefit. The audit then evolved into a clearly defined advisory support model focused not only on recovering at-risk accounts and appeals before timely-filing deadlines, but also on identifying opportunities to leverage Epic capabilities to automate work prioritisation, improve workqueue management and strengthen workflow efficiency. By combining targeted recovery efforts with technology-enabled process improvements, the organisation is reducing manual effort, improving operational consistency and building a more sustainable revenue cycle. This illustrates how an operational audit moves beyond point-in-time control testing to become a catalyst for financial impact, technology optimization, steadier operations and stronger revenue cycle governance.

Case study 2: From denials analytics to enterprise revenue recovery

Facing margin pressure following the rollout of a new EHR, a large, multi-facility health system engaged internal audit to evaluate high-volume denial areas and identify opportunities to standardise denial management and strengthen revenue recovery. Internal audit analysed claim and remittance data alongside write-off adjustment reporting to target areas for detailed review. What began at the request of facility leadership expanded into an enterprisewide review of systemic denial root causes.

To size the exposure and trace denials to their root causes, internal audit examined denial trends and payer behaviour, aged follow-up inventory, accounts with conflicting system statuses, inpatient-to-observation rebill activity and emergency department level-of-care downgrades across roughly $100 billion in patient charges.

The review surfaced several sources of denial exposure:

- **$66 million in aged patient receivables**, representing nearly 50,000 accounts requiring additional oversight.
- **$80 million in accounts with conflicting system statuses**, where ownership gaps created risk of delayed or missed follow-up.
- **$367,000 across 21 accounts where inpatient claims were flagged for rebill** as observation or outpatient but were never subsequently rebilled.
- **Identified emergency department level-of-care denials** that pointed to potential charge-calculation and documentation-logic issues requiring reconciliation against the Epic charge calculator logs.

This case shows how internal audit can use enterprise-scale analytics to move a health system from facility-by-facility denial firefighting to systemic root-cause remediation. By quantifying exposure across aged receivables, conflicting system statuses, rebill gaps and level-of-care denials, the review gave leadership a clearer view of where revenue was at risk and where accountability needed to be strengthened. It also demonstrated the value of connecting claims, remittance and write-off data to identify patterns that standard reporting may miss. Most importantly, the work preserved internal audit's assurance role while providing management with the information needed to standardise denial management, prioritise recovery efforts and strengthen revenue cycle governance.

Case study 3: Ambient documentation review

One of the nation's largest public safety-net health systems had recently rolled out ambient listening technology to ease the documentation load on providers across its ambulatory practises. As adoption grew, compliance and revenue cycle leaders began to question whether the AI-generated documentation supported the codes being billed.

The internal audit team assessed the coding and billing risks by auditing professional-fee encounters before and after the tool's rollout, reviewing evaluation and management (E/M) level selection, Current Procedural Terminology (CPT) modifiers, and International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM) diagnosis coding against the underlying medical record.

The review identified meaningful discrepancies between what the tool captured and what providers ultimately coded, especially on the diagnosis side. In particular, providers were:

- Carrying forward problem-list conditions that were not actively addressed.
- Missing combination codes that required greater specificity.
- Coding resolved conditions as active rather than as personal history.
- Allowing extraneous conversational detail in the generated note to appear clinically significant.

Beyond identifying the risk, the team worked with providers to translate the findings into practical changes. Targeted education reinforced documentation and physician coding expectations in an ambient listening environment, including reviewing each AI-generated note before signature, capturing medications and time spent that the tool may not infer, coding only conditions monitored or treated during the visit and applying personal history codes only where appropriate.

The review also gave management a more structured way to monitor performance going forward. By clarifying where coding risk was most likely to emerge, the review helped the organisation define more practical oversight expectations for provider note review, coding validation, and ongoing monitoring of documentation quality and coding accuracy after implementation. In that way, the work did not stop at identifying variance. It helped management build a more durable control process around the use of the technology.

- **E/M accuracy improved from 72.7% to 78.1%** after implementation.
- The analysis showed the tool potentially **reduced E/M error rates and associated compliance exposure by approximately $769,000** annually.
- The review produced a **roadmap to protect revenue, strengthen compliance and continue scaling ambient listening** with confidence.

This case shows internal audit meeting emerging technology risk in a practical, measurable way. Rather than treating AI-generated documentation as a black box, internal audit used encounter-level testing to pinpoint where coding accuracy was diverging from the medical record, then helped providers convert those findings into more disciplined documentation and coding practises.

The case illustrates how an operational audit can move beyond point-in-time control testing and become a catalyst for stronger compliance, protected revenue and more responsible adoption of new technology.



Case study 4: 340B underpayment identification and recovery

A focused 340B underpayment review set out to quantify reimbursement risk in a domain that sits where financial performance, regulatory compliance and operations overlap. The work centred on identifying discrepancies between expected reimbursement for 340B-acquired drugs and the amounts that commercial and Medicare Advantage plans actually paid.

The gap mattered because the Centers for Medicare & Medicaid Services (CMS) remedy for the 340B payment policy only reached traditional fee-for-service Medicare and did not automatically extend to other payers that align to Medicare methodologies. As a result, many organisations faced a meaningful but difficult-to-quantify risk that their 340B claims outside of traditional Medicare had been underpaid. This was especially acute where core systems could not produce clean 340B reporting on their own, leaving management without a reliable way to check payer behaviour or size the exposure internally.

The review combined claims submission data and payer remittance data with an expected-payment model built from Medicare pricing documentation and payer-specific billing rules. Comparing expected to actual reimbursement at the claim level isolated populations that appeared underpaid and gave leadership a more objective view of 340B reimbursement performance.

The work extended beyond identification. Internal audit brought together revenue cycle, contracting, compliance and legal stakeholders to validate findings, refine the expected-payment model and build an actionable claim population for recovery. In practise, this included supporting payer communication and, where needed, payment reprocessing requests or arbitration activity. The result was not just an analytical insight, but a structured path to operational action.

- The review identified **approximately $8.8 million of potential 340B underpayments** across multiple Medicare Advantage plans by evaluating payment accuracy against CMS guidance.
- The underpayments were determined to be financially significant, representing a **potential positive impact on operating income and 140% of the CMS remedy payment** the organisation received for traditional Medicare claims.
- The analysis provided leadership with a **quantified recovery opportunity and actionable claim population**, enabling coordination among revenue cycle, contracting, compliance, legal and external stakeholders to pursue reimbursement recovery efforts.

This study illustrates how an operational audit and targeted analytics move a leadership team from “We think we’re losing money here” to a quantified, actionable number where management knows how much money has been lost and is actively working to recoup it. Instead of trusting internal system reporting alone, the review used independent claims and remittance data to show how 340B-related claims were adjudicated and where payer payment variances were occurring. The case illustrates how a focused, analytics-led review produced measurable value while remaining firmly within an assurance and risk-based framework.

Demonstrating value and ROI to leadership and boards

Operational audits earn their place on the audit plan when their impact is visible. The most effective internal audit functions report more than findings and remediation status; they report enterprise impact in dollars, days, denials or defects, tracked over time. The goal is not simply to report what happened, but to give leadership risk context early enough to support better decisions and improve outcomes.

This extends to how the broader operating model is performing, including where AI is embedded. Boards increasingly expect to understand whether these capabilities are improving performance in a measurable, governed and explainable way.

Reporting practises that work include:

- A standing audit committee dashboard that pairs audit results with leading and lagging operational KPIs.
- ROI summaries that translate audit outcomes into measurable financial and operational impact, supported by clear methodology and attribution.
- A forward-looking risk lens that shows how the audit plan is shifting as operational risk moves.
- Independence and objectivity disclosures alongside any engagement that has both assurance and advisory components.

Reporting this way strengthens internal audit's independence rather than diluting it. Boards trust the functions that show their work.



Conclusion

Healthcare organisations are increasingly managing complexities associated with operational data, performance metrics and technology-enabled processes. As a result, many of the risks that matter most to boards and executives are no longer found solely in financial controls or regulatory requirements; they are embedded in the processes, decisions and performance indicators that drive organisational outcomes every day.

This creates an opportunity for internal audit to expand its assurance lens while remaining firmly grounded in its core role. By integrating risk assessment, analytics, KPI monitoring and stakeholder insight, internal audit can provide assurance not only over whether controls exist, but also whether critical operational processes are performing as intended, risks are being managed effectively and performance information can be relied upon for decision-making. In doing so, internal audit helps strengthen the organization's ability to create, protect and sustain value while preserving its independence and objectivity.

The examples in this paper demonstrate that the greatest opportunity is not simply performing more operational audits. It is providing assurance over the operational drivers of performance, whether in revenue cycle, clinical operations, workforce management, technology-enabled processes or emerging areas such as AI. The methodology may evolve, the technologies will certainly change and new risks will continue to emerge. What should remain constant is internal audit's ability to bring an independent, enterprisewide perspective on whether the systems, processes and governance structures that leaders rely upon are positioned to achieve their intended outcomes.

For CAEs and audit committees, the question is no longer whether operational performance warrants assurance attention. It is whether internal audit is equipped with the data, methodologies, partnerships and skills necessary to provide that assurance credibly, consistently and at the pace modern healthcare organisations require.

About the authors



Caroline Znaniec, MBA, MS-HCA, CRIP, CRCR
Managing Director, Protiviti

Caroline leads Revenue and Operational Improvement, including revenue integrity and revenue cycle transformation, clinical operations and excellence, and supply chain operations and resilience. She advises healthcare internal audit teams on operational and performance-focused audits that improve efficiency, effectiveness and control across clinical and business functions. Caroline regularly presents on operational auditing in healthcare and helps organisations apply risk-based methods, analytics and KPI monitoring to prioritise audits and demonstrate value.



Zach Christianson, CPA
Senior Manager, Protiviti

Zach brings more than 10 years of accounting, assurance and healthcare transaction advisory experience. He has supported health systems and physician practises on a range of financial, operational and strategic priorities. He helps healthcare leaders assess risk, improve processes and navigate complex business and integration challenges through practical analysis, actionable insights and tailored reporting.



Paula Vasquez, MHA
Manager, Protiviti

Paula brings approximately 10 years of healthcare internal audit experience and supports leading operational and compliance-focused engagements. Paula is experienced in coordinating cross-functional working groups, in layered and phased assurance and advisory settings, and translating findings into clear, actionable next steps for leaders and process owners.

About Protiviti

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

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

About AHIA

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge, and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network, www.ahia.org. AHIA white papers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. By providing healthcare-specific information and education, white papers can help practitioners evaluate risks, develop priorities, and design audit approaches. They are meant to help readers understand an issue, solve a problem, or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content clearly related to healthcare internal auditing that does not promote commercial products or services. **Interested? Contact a member of the AHIA White Paper Subcommittee.**

Subcommittee:

Valerie Mattas, White Paper Chair
valerie.mattas@sharp.com

Alan Henton
alan.p.henton@vumc.org

Debi Weatherford
debi.weatherford@piedmont.org

Laura L. Sak-Castellano
laura.sak-castellano@aah.org

Face the Future with Confidence®

© 2026 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. 1126-IZ-EN

ahia
Assoc. of Healthcare Internal Auditors

protiviti®
Global Business Consulting