ahia
Assoc. of Healthcare Internal Auditors

NEW PERSPECTIVES

on Healthcare Risk Management, Control and Governance

www.AHIA.org Journal of the Association of Healthcare Internal Auditors Vol. 45, Number 3, 2026

IT Audit for Non-IT Auditors

Understand why IT matters more than ever in healthcare

page 8

Elevating Behavioral Health Audits – Part 1

Gather insights into effective practices

page 24

Auditing Capital Projects

Take a strategic approach to mitigating risks and improving project outcomes

page 38

Face the Future with Confidence®

Turn audit into intelligence — Empower better decisions with forward-looking insight

The pace and complexity of today's healthcare environment have outgrown traditional internal audit models, requiring a more agile, proactive approach to risk management and assurance. Forward-looking insight is essential to navigate risk in real time and support confident, informed decision-making.

Protiviti's internal audit services help transform audit into a strategic driver of value by focusing on:

- **Forward-looking risk insight:** move beyond reviewing the past and deliver timely, decision-relevant risk intelligence that empowers leaders to act earlier and shape outcomes.
- **Decision intelligence enablement:** provide context, perspective and independent judgment to help leadership evaluate trade-offs and make better strategic decisions with confidence.
- **AI-driven audit transformation:** utilize AI, automation and analytics to expand coverage, accelerate audit execution and unlock deeper insights across the organization.
- **Human-centered advisory:** elevate audit's role with skilled professionals who interpret risk, engage stakeholders and deliver meaningful insights that guide the business forward.

Read more

Scan below to learn more about Protiviti Healthcare

protiviti®

Global Business Consulting

contents

Vol. 45, Number 3

FROM THE EDITOR

Auditors Just Don't Understand

By Jen Conley

"There's no need to argue, parents just don't understand" –lyrics by DJ Jazzy Jeff & The Fresh Prince

A recent LinkedIn post reminded me that internal auditors still struggle to demonstrate that they understand business, not just risks. Like teenagers who roll their eyes at out-of-touch parents, some audit clients are skeptical of auditors who don't emanate business acumen. Richard Chambers, former President and CEO of The Institute of Internal Auditors (IIA), has recounted executives' wish that internal auditors would better understand their business.

But with so much to know, how can healthcare internal auditors learn enough to placate frustrated clients without wasting hours chasing AI prompts or digging through questionable online sources? Fortunately, our *NP* contributors cut through the noise. They bring real-world experience and carefully curated insight to help auditors focus on what truly matters to audit clients.

Kenneth Brzozowski and Mary Jane Schroeder recognize that construction project teams might view audit involvement as an administrative disruption to their tight schedules. But their article walks readers through a strategic approach to setting the stage, adjusting the frame of mind, reading the signs, bridging the gap, and turning the tide toward forward-looking capital construction audits.

Jeannie O'Donnell explains why IT matters more than ever in healthcare and where non-IT auditors fit in. She recognizes that, for non-IT auditors, the goal is not to become engineers or cybersecurity specialists. The goal is to understand enough about the technology environment to ask the right questions, recognize where control weaknesses may exist, and know when to solicit additional expertise. She shows how learning the basics of IT audit improves audit quality and strengthens professional credibility.

I personally wouldn't have been ready to discuss the impact of shadow AI in healthcare before carefully reading David Sems' column on AI guardrails. But armed with his guide, I could discuss this inevitable hazard with IT and operational leaders and avoid looking like a deer in the headlights. David explains the new nomenclature that is already common to some network and security professionals (e.g., *vibe coding* and *rail types*) and offers a risk matrix example and field manual that can quickly help auditors defend their organizations.

continued on page 7

NEW PERSPECTIVES
Published by AHIA, Inc.

EDITOR:
Jen Conley
801-803-2361
Jen.ahia.np@gmail.com

EDITORIAL BOARD:
Robert Michalski, CHIAP®, CHC, CHPC, CHRC, CCE
Editorial Board Chair
University of Florida Health
Gainesville, FL
robert.michalski@ufhealth.org

Robin Cannon, CHIAP®
Wellspan Health
York, PA

Megan DeVries, CHIAP®, CIA®
AHIA Board Liaison
Corewell Health
Grand Rapids, MI

Angela B. Fearon, CIA®, CPA
Children's Wisconsin
Columbia, MO

Susan Fredrick, CIA®, CPA
Cleveland Clinic
Cleveland, OH

Amy LaBarge, CIA®, CPA, CISA
Parkland Hospital
Dallas, TX

Isaak Lerner, CISSP, CISM, CISA
Lerner Consulting
Milwaukee, WI

Jared S. Soileau, PHD, CIA®, CPA, CISA, CCSA
Louisiana State University
Baton Rouge, LA

Jay Swacker, CIA®, CPA, CHC
Dean Dorton
Lexington, KY

Scott Thompson, CHIAP®, CHC, CHPC
CommonSpirit Health
Birmingham, AL

Joshua Wallner
Stryker
Grand Rapids, MI

Jonathan West, CIA®, CISA
Intermountain Health
Salt Lake City, UT

FROM THE CHAIR

Meet the AHIA Publications Committee

By Heather Zundel

Since you're reading *New Perspectives (NP)*, I know you're already familiar with some of the Publications Committee's work. But NP is just one part of the Committee's effort to provide strategic direction for AHIA publications, helping align topics and content with member needs, AHIA Board priorities, and the association's mission. AHIA's publications are especially valuable because they provide practical insight from professionals who are actively working through many of the same challenges our members face.

The Publications Committee aligns the work of three subcommittees: the e-News Subcommittee, the Editorial Board, and the White Paper Subcommittee.

For timely, quick-access resources, e-News connects AHIA members with emerging issues, professional insights, educational opportunities, and developments affecting healthcare internal audit and the broader healthcare environment. The goal is to provide relevant, practical content that keeps members informed between the more in-depth publications and educational offerings AHIA provides.

E-News Chair, Fatimah Muhammad, explained, "e-News creates an important opportunity to highlight the expertise within our membership. It allows us to share perspectives from professionals across different areas of healthcare, bring attention to evolving risks and trends, and keep members connected to what is happening throughout the association and the profession."

While our e-News team keeps members informed with timely industry updates, the Editorial Board focuses on *NP*, AHIA's professional journal, by identifying relevant topics and authors, reviewing articles, maintaining editorial standards, and supporting the journal's refereed and peer-reviewed status. They also take on the tough but meaningful responsibility of selecting just one Article of the Year and identifying standout pieces for AZBEE award nominations.

Finally, the White Paper Subcommittee steps in when our members need a deep dive into the art and science of healthcare internal auditing. White paper categories include best practices and case studies of real-life examples, models in healthcare internal audit, and special interests.

After vetting idea submissions, this team works as a liaison to authors of white papers, providing them with timely reviews, content revisions, and publication coordination and support. So far, this year's white papers include *Generative Artificial Intelligence in Healthcare Internal Audit: A Practical Guide* and

ahia
Assoc. of Healthcare Internal Auditors

2026 BOARD OF DIRECTORS

Chair
Heather Zundel, CPA, CGMA
Presbyterian Healthcare Services
HeatherZundelcpa2022@gmail.com

Vice Chair
Cally Cass
Peace Health
CCass@peacehealth.org

Treasurer
Mary Thomas, CIA®
Main Line Health
awesomeasbury@gmail.com

Secretary/Assistant Treasurer
Evan Webber, CIA®, CFE
OSF Healthcare
evan.p.webber@osfhealthcare.org

Directors
Megan DeVries, CHIAP®, CIA®
Corewell Health
Megan.DeVries@corewellhealth.org

Alan Henton, CHIAP®, CPA (inactive), CISA, CISSP, CIPT
Vanderbilt University Medical Center
Alan.P.Henton@vumc.org

Jerod Holloway, CHIAP®, CIA®, CFE, CHC
Weaver
jerod.holloway@gmail.com

Jerry E. Lear, CHIAP®, CIA®, CISA, CHC®
Bon Secours Mercy Health
JeLear@bsmhealth.org

Darryl Rhames, CHIAP®, CFE, CHPC, CICA
University Health
Darryl.Rhames@uhs-sa.com

Shawn Stevison, CHIAP®, CPA, CHC®, CRMA, CGMA
Humana
SStevison@humana.com

Jonathan West, CIA®, CISA
Intermountain Health
Jonathan.West@imail.org

Executive Director
Julie Sutter
856-423-7222 ext 978
jsutter@talley.com

I share relevant articles with other stakeholders outside of our department as discussion starters, training resources, or examples of leading practices.

Compliant and Effective AI Integration in Middle Revenue Cycle Functions.

Committee Chair Bob Michalski shared how valuable AHIA's publications are to his organization:

> My team and I use AHIA's publications to stay current on emerging issues in healthcare internal audit, compliance, risk, governance, and related areas. We use the articles in *NP* as professional reference material when researching audit topics, benchmarking practices, or developing audit plans. The articles also help support professional development for team members by deepening knowledge in evolving competencies. Reviewing articles has also helped prepare team members for the Certified Healthcare Internal Audit Professional (CHIAP®) certification. I will also share relevant articles with other stakeholders outside of our department as discussion starters, training resources, or examples of leading practices. My team members have also contributed their expertise by authoring articles.

Similarly, Valerie Mattas explained how her team uses AHIA publications:

> Our audit team leverages AHIA publications to support annual audit planning, inform project-level risk assessments and research, and share insights with stakeholders. The resources help strengthen confidence in our expertise and enhance discussions around emerging and evolving risks. It's very helpful to have healthcare-specific resources on people, process, and technology.

I encourage all members to view AHIA's publications not only as something to read, but also as an opportunity to contribute. If there is an issue, trend, innovation, or lesson learned that you believe would benefit other healthcare professionals, the Publications Committee wants to hear from you. Our publications are strongest when they reflect the collective knowledge and experiences of the AHIA community.

Why do you volunteer?

The Chairs of the Publications Committee's three subcommittees shared what inspires them to give their time and energy so generously.

Fatimah Muhammad, e-News Chair

I volunteer because I believe strongly in professional collaboration and creating opportunities for knowledge to be shared across our field. One of my favorite parts of serving with AHIA is working with professionals who bring different experiences and perspectives to the table.

I use AHIA publications as both a professional resource and a way to remain connected to emerging issues across healthcare. Given that my work intersects with compliance, financial strategy, pharmacy, reimbursement, and operational risk, I value content that brings together different perspectives and helps leaders better understand how changes in healthcare may affect their organizations.

As Chair of the e-News Subcommittee, I particularly enjoy identifying topics that are timely and meaningful and helping create a platform where members can share their expertise. There is tremendous knowledge within the AHIA community, and I enjoy helping bring more of those voices forward.

Valerie Mattas, White Paper Chair

I started volunteering for the subcommittee after authoring a white paper and saw it as an opportunity to become more engaged with AHIA. Beyond contributing to the profession, it has enabled me to build a strong network of healthcare internal audit leaders across the country—connections that provide invaluable perspectives and support as I help guide my team and organization. My advice to AHIA members: Don't be afraid to get involved, no matter how many years of experience you have.

Robert Michalski, Publications Committee and Editorial Board Chair

I volunteer because I believe AHIA's publications are one of the most important ways we support, connect, and advance the healthcare internal audit profession. It is an honor to support an award-winning professional journal like *NP* that includes such high-quality content and provides an outlet for members to share practical insights.

My favorite part of volunteering is working with talented AHIA members, authors, and colleagues who are committed to strengthening the profession. I have learned so much from the authors, the Committee and Editorial

Board members, and have made strong professional connections and personal friends from serving together.

I encourage every AHIA member—whether you've been in healthcare internal audit for decades or are brand new to the field—to engage with *NP*. Our profession is strongest when we learn from one another, and *NP* is a great tool to facilitate that learning and knowledge sharing. Keep reading, keep sharing your feedback, consider submitting an article or topic idea, and reach out if you'd like to join us behind the scenes on the Editorial Board. We'd love to have your voice and perspective helping shape the future of our journal! **NP**

Interested in volunteering?

Find AHIA committee charters and membership rosters at https://ahia.org/committees/. Learn about and respond to committee volunteer opportunities at https://community.ahia.org/new-page2/volunteer-pages-bucket.

Auditors Just Don't Understand

continued from page 4

A focus on planning activities is the key to effective behavioral health audits, as explained by Erin Panek and Cheryl Snook. Auditors must show their organizations that they can identify crucial resources, understand the regulatory environment, leverage subject matter expertise, develop an appropriate audit scope, and adjust the test plan as necessary. Erin and Cheryl outline considerations for all types of behavioral health audits as well as specific considerations for audits of involuntary holds.

In part three of her review of the seven signs of ethical collapse, Marianne Jennings calls out three signs that auditors and objective observers understand better than the operational leaders who display them. She also provides auditors with tools they can use to intervene before the signs become systemic failures.

Finally, in her Chair column, Heather Zundel shares how the Publications Committee Chair's audit team has used *NP* articles to prove their business knowledge and to proactively share information, training resources, and leading practices with audit clients and other organizational shareholders.

To gain stakeholder understanding, auditors don't need to prove that they're as experienced as the audit client. They just need to harness the right tools to show that they're knowledgeable, supportive, and ready to collaborate. **NP**

About *New Perspectives*

New Perspectives (NP) is a refereed and peer-reviewed journal that focuses on up-to-date information, trends and issues in the healthcare industry and the internal auditing profession. Practical guidance is provided on risks and controls that can be applied by internal audit professionals in their jobs.

NP is published quarterly in an electronic format. Issues are accessed by online viewing or through download. See the NP archives at https://ahia.org/new-perspectives-archive/ (login required).

For author guidelines or to submit an article, please contact Jen Conley at 801-803-2361 or Jen.ahia.np@gmail.com.

Yearly subscription rates, including postage, are $100, payable in U.S. funds. No refunds or cancellations. Send publication and subscription inquiries, address changes and other inquiries to: Association of Healthcare Internal Auditors, Inc., 19 Mantua Road, Mount Royal, NJ 08061 USA. Phone 856-554-1083 or email, *info@ahia.org*.

New Perspectives, its editors and the Association of Healthcare Internal Auditors, Inc. are not responsible for the opinions and statements of its contributors and advertisers. The authors do not necessarily reflect the official policies of AHIA nor does AHIA endorse any products. AHIA does not attest to the originality of the author's content. Reprints of any portion of *New Perspectives* may be used for educational or instructional purposes only, provided the following statement appears on each reprint: "Reprinted with permission from *New Perspectives*, Journal of the Association of Healthcare Internal Auditors, Inc. Volume/Number." Copyright 2026, Association of Healthcare Internal Auditors, Inc.

FEATURE

IT Audit for Non-IT Auditors

Understand why IT matters more than ever in healthcare

By Jeannie O'Donnell, CIA, CISA, CFE, CHC, CPC, CHIAP

Healthcare auditors rely on data for nearly every conclusion they reach, whether they are reviewing reimbursement, revenue cycle activity, compliance metrics, or operational performance. That reality makes IT audit relevant far beyond the traditional technology function. When the systems that generate, process, or transmit data are not well controlled, the reliability of audit conclusions may be at risk.

For non-IT auditors, the goal is not to become engineers or cybersecurity specialists. The goal is to understand enough about the technology environment to ask the right questions, recognize where control weaknesses may exist, and know when to bring in additional expertise. IT risks intersect with many healthcare provisions such as patient information, HIPAA safeguards, billing and reporting expectations, and complex arrangements such as a hospital's 340B Drug Pricing Program (340B) contract pharmacy relationships.

This article translates foundational IT audit concepts into practical guidance for financial, operational, and compliance auditors. It will expand on the basics: what IT audit is, why governance matters, how to define the IT universe, what to look for in access controls and change management, how to audit business continuity and disaster recovery, and why third-party and security risk assessments matter. Along the way, those concepts will be tied back to healthcare realities where data integrity is directly connected to reimbursement, compliance, and organizational credibility.

The audit environment

In today's environment, virtually every audit depends on data generated and processed by information systems. That is true for financial audits, operational reviews, compliance engagements, and investigative work. Auditors may not think of themselves as relying on IT. Yet, every download from a general ledger, billing system, payroll application, electronic medical record, or pharmacy platform depends on the design and operation of underlying technology controls.

Healthcare makes this connection even more evident. The data used to support revenue, CMS reimbursement, cost reporting, payer claims, quality measures, utilization trends, privacy monitoring, and 340B eligibility all originate in information systems. If those systems are not secure, if interfaces are incomplete, if user access is excessive, or if changes are not properly tested, the resulting data may be inaccurate or incomplete. Once that happens, the risk is no longer simply technical. It becomes financial, operational, regulatory, and reputational.

IT audit is no longer a specialty to be viewed from a distance. It is a foundational competency for modern auditors. Non-IT auditors do not need to know how to build networks or configure servers. They do, however, need to understand the basics of how systems work, how data moves, where controls can fail, and how those failures affect the objectives of the process under audit.

What is IT audit?

An information technology audit, or information systems audit, is an examination of the management controls within an organization's technology infrastructure and business applications. At its core, the objective of an IT audit should be to evaluate whether systems are available when needed, information is secure and confidential, integrity is maintained, and whether outputs are accurate, reliable, and timely.

IT audit is no longer a specialty to be viewed from a distance.

That definition is broader than many auditors expect. IT audits can include review of infrastructure, applications, security, user access, vulnerabilities, interfaces, implementation controls, and governance. It may involve a targeted review of a new application, a large-scale system implementation, a data center migration, a cybersecurity program, or controls embedded within a particular business process. IT audits can be done on a standalone basis, but they are just as often performed in conjunction with financial, operational, privacy, and compliance audits.

One of the biggest mindset shifts for non-IT auditors is recognizing that IT audit is not separate from the rest of the audit universe. If an audit relies on data, it already relies on IT controls. The question is not whether technology matters. The question is whether auditors have addressed it thoughtfully enough to support their conclusions.

Why background matters

There is no single path into IT audit, and that is part of what makes the discipline accessible to non-IT auditors. Some professionals start in audit and later develop technology expertise. Others begin in information systems and later move into assurance. A background in accounting, finance, compliance, operations, or security can all be relevant, especially when paired with curiosity about how systems support business processes.

For example, my career journey began in accounting, long before IT audit became a common career destination. Over time, that accounting background intersected with hands-on experience using evolving technology, building solutions, and understanding how data is created and maintained. Later roles in hospital audit, claims audit, financial audit, IT audit, security analysis, and business continuity deepened that perspective. The progression was not from one silo to another. It was a gradual recognition that accounting, audit, technology, security, and operational resilience are all connected.

That connection matters for non-IT auditors because it underscores a practical reality: an auditor does not have to start as a technologist to become conversant in IT risk. What matters is developing enough fluency to understand how technology supports the process under review and how control failures could affect the organization.

Why auditors need the IT basics

Data is everywhere. Auditors use it to identify outliers, test transactions, analyze trends, monitor key performance indicators, assess compliance, and support investigative work. The more organizations automate, the more auditors depend on system-generated information. That makes basic IT knowledge essential, because an auditor cannot fully assess the completeness, accuracy, and integrity of data without understanding how that data is created, maintained, and protected.

In healthcare, the stakes are especially high. A flawed extract can distort a reimbursement analysis. A broken interface can affect patient charges. Weak access controls can expose protected health information (PHI). An untested change to billing rules can affect claims submissions. Weaknesses in how 340B data is tracked between a covered entity, a third-party administrator, and contract pharmacies can create diversion or duplicate discount risk.

In each case, what looks like a business, financial, or compliance issue often begins as a control issue within the technology environment.

Artificial intelligence (AI) is increasingly embedded in healthcare systems, from billing logic to clinical decision support. Even basic AI literacy helps non-IT auditors evaluate whether automated processes are reliable, transparent, and appropriately governed. Understanding concepts like training data, algorithmic bias, and model drift enables auditors to recognize when AI-generated outputs may affect reimbursement, privacy, or compliance.

This is why non-IT auditors should routinely ask a few foundational questions: Who has access to the data? How is the data generated? What systems are involved? What interfaces feed the process? What controls support completeness and accuracy? When those questions are not asked, auditors risk drawing conclusions from unreliable data.

Want to learn more about AI?

Take a closer look at these AHIA resources:

White Papers

AI in Healthcare: Navigating the Future with Governance and Innovation (2024)

Compliant and Effective AI Integration in Middle Revenue Cycle Functions (2026)

Generative Artificial Intelligence in Healthcare Internal Audit: A Practical Guide (2026)

New Perspectives

INFORMATION TECHNOLOGY: An Internal Auditor's Guide to Healthcare AI Guardrails [Vol. 45, Number 3 (2026)]

Beyond The Hype: Take a practical approach to auditing AI in healthcare [Vol. 44, Number 1 (2025)]

IT governance: Whose responsibility is it?

A common misconception is that IT governance belongs solely to the technology department. In reality, it is a shared responsibility that spans the leadership structure of the organization. Depending on the organization, responsible leaders may include, but not be limited to, the Chief Executive Officer, Chief Information Officer, Chief Information Security Officer (CISO), Chief Financial Officer, Chief Risk Officer, Chief Compliance Officer, Chief Audit Executive, and the audit committee. Each has a different role in overseeing how technology supports strategy, operations, security, compliance, and risk management.

The CISO role is particularly important because cyber-security now touches every major business process. Yet unclear accountability around security is still a recurring audit issue. In some organizations, the security officer has multiple conflicting responsibilities, performs CISO duties only part time, or lacks the authority, resources, or enterprise visibility needed to effectively manage risk. In other organizations, reporting lines do not support sufficient independence or appropriate escalation of security concerns.

For auditors, governance is not an abstract organizational chart exercise. It affects how decisions are made, how risk is escalated, how policies are enforced, and whether critical issues receive appropriate oversight. In healthcare, where privacy, security, reimbursement, and continuity of operations are deeply intertwined, weak governance can quickly become a compliance and operational problem rather than just a technology problem.

Know your universe

One of the most practical concepts in IT audit is also one of the simplest: Know your universe. That means defining the full scope of the environment under assessment. The universe includes systems, applications, devices, users, and supporting processes. It also includes people who are easy to overlook, such as contractors, temporary staff, students, and vendors with access to systems or data.

Auditors routinely identify problems when organizations do not fully understand their own environments. There may be rogue devices, incomplete application inventories, poorly tracked interfaces, or inconsistent user management practices. This can lead to uncertainty over who has access to the electronic medical record, how users are provisioned across enterprise systems, or whether transfers and terminations are reflected in all relevant applications.

This matters because you cannot effectively audit access, security, change management, privacy, or business continuity if you do not know the boundaries of the environment. Gaps in the universe become gaps in audit coverage. Taking time to define the universe can be one of the most valuable early steps in scoping an engagement.

Common areas of IT audit that often have audit plan coverage include, but are not limited to, access controls, application controls, change management, IT security, business continuity, third-party risk management, and IT security assessments.

Access controls: Often the best place to start

Access controls identify users by verifying credentials and determining what systems, functions, and data they are permitted to use. Authentication methods can include usernames, passwords, PINs, biometric factors, and security tokens. Authorization determines whether the user's level of access is appropriate for the role performed.

From an audit perspective, access controls are often quick wins because there are so many common points of failure, such as:

One of the most practical concepts in IT audit is also one of the simplest: Know your universe.

A system can appear to produce reasonable results while still having underlying design or configuration weaknesses.

- Terminated employees may retain access.
- Users who transfer roles may keep rights that are no longer needed.
- Temporary access may not be removed.
- Default passwords might not be changed.
- Shared accounts may limit accountability.
- Multiple accounts may exist for the same individual.

In healthcare, those issues affect not only security but also privacy, billing, and segregation of duties.

This is an area where non-IT auditors can add immediate value. Reviewing access listings, comparing users to HR records, validating privileged access, and asking whether access is role-based can reveal meaningful risks. In settings where PHI, reimbursement data, or controlled pharmacy information is involved, weak access controls can create exposure well beyond the IT department.

Application controls and general IT controls

Controls are the methods, policies, and procedures used to protect assets and support accurate, reliable processing. In the IT context, it is helpful to distinguish between general IT controls and application controls. General IT controls apply broadly across systems and environments. They include access management, change management, infrastructure and physical security, backup practices, and broader administrative controls such as policies, supervision, and segregation of duties.

Application controls are specific to a particular system or process. They may include validity checks, edit checks, required fields, input completeness controls, automated calculations, exception reporting, output validation, and configuration settings designed to support accurate processing. In healthcare, application controls often sit at the center of charge capture, coding workflows, billing edits, pharmacy dispensing logic, and eligibility determination.

Auditors should not assume that accurate output means controls are working. A system can appear to produce reasonable results while still having underlying design or configuration weaknesses. For that reason, both design and operating effectiveness matter. Understanding whether the right controls exist, whether they are configured correctly, and whether they are operating consistently is essential to placing reliance on system-generated data.

Change management: Small changes, big consequences

Change management is the structured approach used to ensure that changes affecting technology services are properly documented, approved, tested, and implemented. A change can mean adding, modifying, or removing anything that affects IT services, from infrastructure updates to application configuration changes to report logic and security settings.

The basic discipline of change management usually includes documenting and approving the change, involving appropriate personnel and end users, developing an implementation plan, testing in a non-production environment, moving the change into production in a controlled manner, and maintaining a record of the change in a ticketing or service request system. When those steps are bypassed, the organization increases the risk of outages, faulty processing, security vulnerabilities, and unreliable reporting.

Healthcare examples make this concept tangible. An improperly tested change to billing edits can affect claims accuracy. A modification to a charge description master interface can disrupt charge capture. A pharmacy system configuration change can affect 340B accumulations or replenishment logic. Change management sometimes sounds procedural, but weak change control can create very real financial and compliance consequences.

IT security: Physical, administrative, and technical safeguards

A comprehensive security review looks beyond firewalls and passwords. Security includes physical security, administrative safeguards, and technical safeguards.

Physical security covers facility access, badge controls, equipment tracking, secured devices, acceptable use of business equipment, and incident response readiness. Administrative safeguards include leadership responsibility, policies and procedures, training, governance, and the broader structure used to manage security. Technical safeguards include access controls, audit controls, integrity controls, encryption, and transmission security.

For healthcare auditors, this framework should feel familiar because these categories align closely with HIPAA security expectations and broader privacy responsibilities. It also underscores why security and privacy audits are often

intertwined. Weaknesses in physical or logical access can expose PHI. Inadequate logging and monitoring can impair investigations. Weak training can lead to inappropriate use or disclosure. Poor transmission controls can expose data shared with vendors or contract pharmacy partners.

Security audits therefore require both breadth and context. The issue is not only whether the organization has a policy or tool in place, but whether the security program is appropriately designed for the organization's risk profile and whether those controls support the confidentiality, integrity, and availability of critical information.

Business continuity and disaster recovery

Business continuity refers to an organization's ability to keep operating after an interruption. Disaster recovery focuses more specifically on the technology systems that support critical business functions. Fires, natural disasters, chemical spills, power outages, cyber events, and pandemics all expose the importance of continuity planning. In healthcare, the consequences of prolonged downtime extend beyond inconvenience. They affect patient care, patient safety, privacy, scheduling, billing, and leadership decision-making.

Auditing this area requires more than confirming whether a plan exists. Auditors should look for:

- a business continuity plan
- supporting policies
- a designated business continuity officer or equivalent leadership
- a business impact analysis
- stated assumptions
- current organizational charts
- response teams and team leaders
- detailed action plans or process flows
- communication scripts
- vendor lists
- a disaster recovery plan
- consideration of backup sites
- documentation of servers, systems, and applications
- evidence of testing

Testing is where many organizations fall short. Documentation may exist, but continuity plans are not always exercised meaningfully. In healthcare, auditors should also consider downtime procedures for clinical and revenue cycle operations, the practical ability to recover data and equipment, and whether vendor dependencies have been addressed. A continuity plan that works only on paper will not support the organization during an actual disruption.

Third-party risk: Vendors extend the audit universe

A third-party risk assessment evaluates the risks introduced through relationships with vendors, service providers, software companies, and other suppliers. Those risks can be cybersecurity-related, operational, reputational, regulatory, strategic, or financial. Any third party that supports critical functions, handles sensitive data, or performs key processing on behalf of the organization becomes part of the broader control environment.

This area is especially relevant in healthcare, where organizations rely on outsourced billing services, revenue cycle vendors, cloud platforms, managed service providers, pharmacy administrators, and other specialized partners. The organization's regulatory obligations do not disappear because a third party is involved. If a vendor's controls are weak, the covered entity (i.e., an organization that is subject to HIPAA regulations, including healthcare providers, health plans, and clearinghouses) may still bear the financial, compliance, and reputational consequences.

The 340B environment illustrates this clearly. Contract pharmacy arrangements and third-party administrators can introduce complexity in eligibility tracking, split-billing logic, replenishment, claims data matching, and reconciliation. If the covered entity does not understand data flows, responsibility matrices, exception handling, and oversight controls, it may miss diversion, duplicate discount, or contract compliance risks. Third-party relationships do not transfer risk; they expand it.

Security risk assessments and control frameworks

Another major area for IT audit is the security risk assessment. These engagements involve a comprehensive review of the organization's information security posture, often measured against an established framework, checklist of best practices, or regulatory expectations.

In practice, a security assessment often begins with a document request for policies, procedures, organization charts, key management reports, and access to major

Business continuity refers to an organization's ability to keep operating after an interruption.

Building fluency in IT concepts expands the types of work you can support and the value you can bring.

applications used in the process. From there, the work typically expands to documentation review, stakeholder interviews, walk-throughs, job shadowing, and targeted testing. A control framework helps give structure to the work.

The National Institute of Standards and Technology (NIST) provides several widely used frameworks, such as NIST Special Publication 800-53, which provides detailed control guidance across a wide range of security domains. Reports from these reviews are often presented in matrix form, identifying the control, related requirements, observations, supporting policies and procedures, risk implications, risk ratings, and recommendations.

In healthcare, security assessments often intersect with privacy audit work because the two disciplines are closely linked. Auditors may need to consider not only whether access and transmission controls are in place, but also whether those controls align with organizational obligations related to PHI, incident response, vendor oversight, and operational resilience.

IT audits are not all boring

One reason it is important to broaden participation in IT audit is that the work is far more practical and varied than the label suggests. IT audit is not limited to checklists or purely technical reviews. It can involve readiness assessments, support for expert reports in data breach matters, litigation-related analysis, privacy and security work, evaluations of system implementations, and investigations that depend on technology evidence.

Healthcare examples include CMS-related readiness assessments, reviews of direct enrollment or regulatory control environments, data breach analysis, privacy and security reviews, and application-specific assessments such as access controls or System and Organization Controls (SOC)-report-related topics. (A SOC audit is an independent assessment that verifies if a service organization effectively safeguards customer data and follows stringent operational controls.) The common thread is that technology controls frequently sit underneath business, financial, legal, and regulatory issues that are highly visible to leadership.

For non-IT auditors, this is good news. Building fluency in IT concepts expands the types of work you can support and the value you can bring. It also strengthens your ability to engage credibly in cross-functional discussions about risk, controls, and accountability.

Where non-IT auditors fit in

Non-IT auditors already have many of the skills needed to contribute meaningfully in this space. They understand processes, risks, controls, documentation, governance, exceptions, and root causes. What they often need is more confidence in applying those skills to technology-supported environments. In practice, this may mean validating the source and completeness of a data set before relying on it, reviewing user access as part of an operational audit, understanding how an interface affects the process under review, or involving IT specialists earlier when a risk exceeds the team's current depth.

IT audit knowledge supports queries, analytics, security assessments, implementations, privacy reviews, and broader risk assessments. That same integration is available to any auditor willing to learn the basics. You do not need to own every technical detail. But you do need enough understanding to ask better questions and identify when technology risk is driving the business issue in front of you.

Non-IT auditors can be especially effective at the intersection of operations, compliance, finance, and systems. By connecting those domains, they help organizations move beyond siloed thinking and toward more complete assurance.

Where to go from here

For auditors interested in building this skill set, the next step is not to master everything at once. Start with the basics. Learn key terminology. Understand how access controls work. Learn the difference between general IT controls and application controls. Ask how data moves across systems. Review change management evidence. Sit in on security or privacy discussions. Participate in vendor risk assessments. Work on an IT audit, supervised by a more experienced IT audit mentor.

The more often you link technology concepts back to familiar audit objectives, the faster the subject becomes practical rather than intimidating.

Professional development can also help. Certifications such as the CIA (Certified Internal Auditor) and CISA (Certified Information Systems Auditor) provide structured ways to deepen audit and systems knowledge, and other security-related certifications may be relevant depending on the role. Just as important, however, is on-the-job exposure—such as working with IT auditors, security teams, privacy officers,

revenue cycle leaders, and operational owners to understand how technology enables and complicates the processes auditors review.

The objective is not to turn every auditor into a specialist. It is to ensure that auditors can engage thoughtfully with technology risk in a world where nearly every risk has an information systems component.

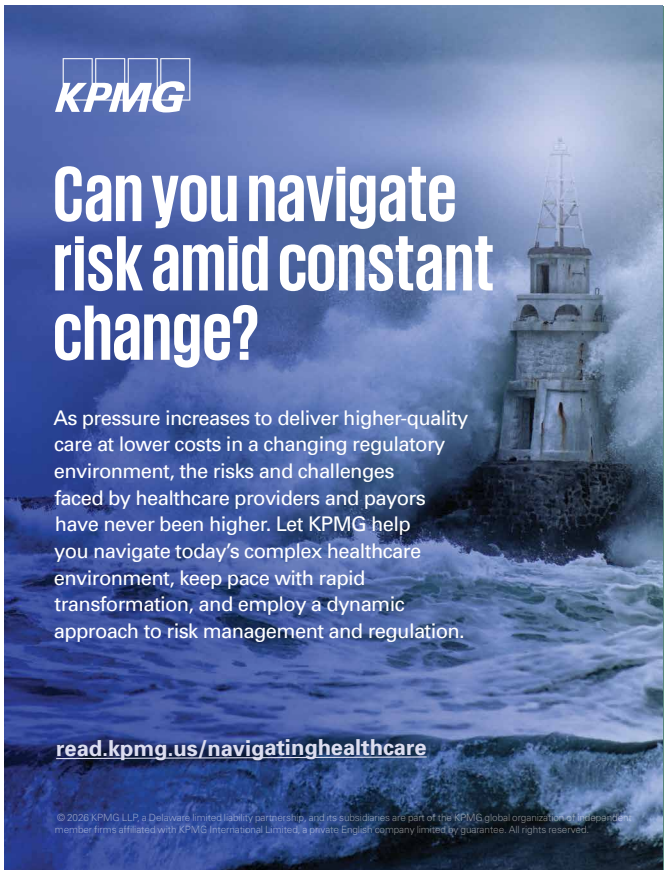
Conclusion

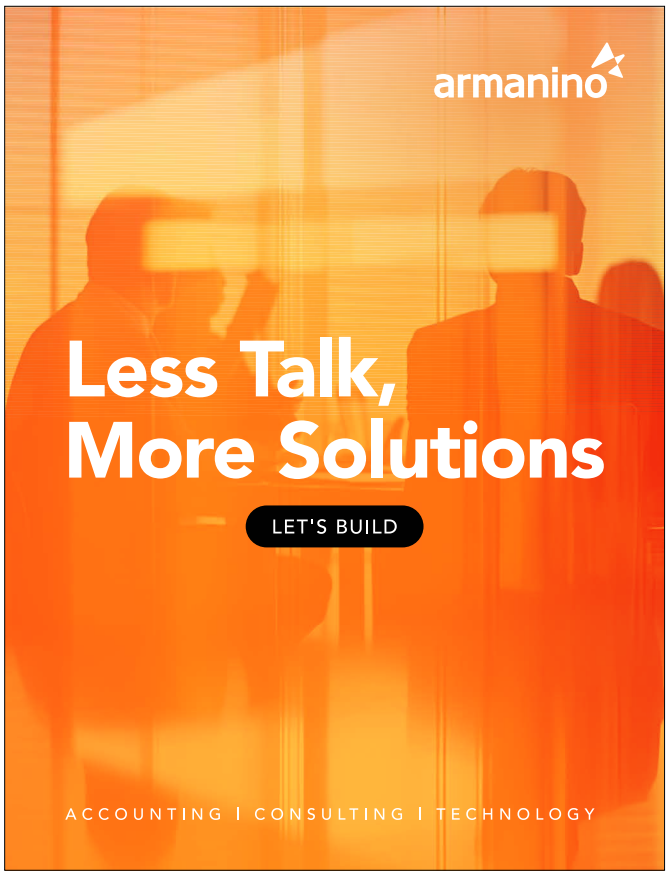
IT audit matters more than ever because organizations are increasingly data-driven, interconnected, and dependent on complex systems to support mission-critical functions. As emerging technologies continue to evolve, IT and cybersecurity risks are expanding in scale and complexity. In healthcare, the implications are immediate: Reimbursement, privacy, patient care operations, compliance, and third-party oversight all depend on reliable systems and well-designed controls.

For non-IT auditors, learning the basics of IT audit improves audit quality and strengthens professional credibility. It enables auditors to better evaluate the completeness and accuracy of data, recognize when a business issue is really a systems issue, and collaborate more effectively with specialists when technical depth is needed. Most importantly, it allows auditors to provide deeper, more practical insight to leadership.

If you rely on data, you are already relying on IT controls. The more clearly auditors understand that truth, the stronger their work and their value to the organization will be. **NP**

Jeannie O'Donnell, CIA, CISA, CFE, CHC, CPC, CHIAP®, is a Director in Healthcare Forensics at BDO, USA, P.C. and resides in Milton, Delaware. She specializes in forensic accounting, fraud investigations, monitorships, corporate integrity agreements, business continuity, and privacy & security. Jeannie can be reached at 980-253-0808 and jodonnell@bdo.com.

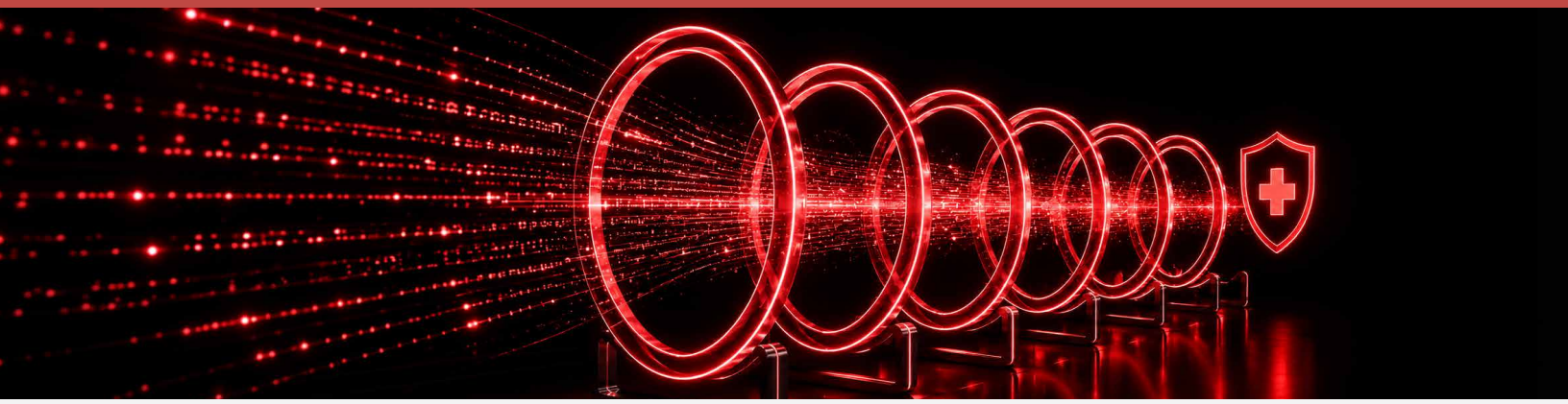




An Internal Auditor's Guide to Healthcare AI Guardrails

Tame the shadow

By David E. Sems, CPA, CITP, CFF



Picture the scenario: A well-meaning clinician, buried in prior authorization denials and behind on documentation, opens a free consumer chatbot on a phone and pastes in three paragraphs of a patient's history to draft an appeal letter. Instantly, the work is done, but also within seconds, Protected Health Information has left the secure hospital perimeter, with no Business Associate Agreement in place, no assurance about where that data is retained or how it might be used to train the next model, and no way for the organization to ever really get it back.

This likely-to-occur scenario is "Shadow AI" in healthcare—the unauthorized, unmonitored use of generative AI tools, browser extensions, and application programming interfaces (APIs) by hospital staff trying to optimize an impossible workload.

It is no longer fringe behavior. A Wolters Kluwer Health survey published in early 2026 found that more than 40% of medical workers and administrators were aware of colleagues using unapproved AI products, while nearly one in five admitted to using an unauthorized tool themselves. These are clinicians who already log one to two hours of EHR charting for every hour spent with a patient, who are not going to wait for a 12-month procurement cycle to catch up.

This creates an audit dilemma. Traditional static network firewalls and blanket "no AI" policies fail for the same reason Dropbox slipped past IT a decade ago: the tool is one browser tab away, and the productivity gain feels too good to give up. A ban pushes the behavior onto a personal phone, off the corporate network, and out of any log an auditor could ever review. That creates severe HIPAA compliance vulnerabilities, significant data leakage risk, and medical liability exposure when an AI-generated summary quietly introduces an error into a clinical record.

With any new technology, the first response can be something like "just say no" or "it is too risky." I see how this is easy for those whose role is to help mitigate the risk.

More than 40% of medical workers and administrators were aware of colleagues using unapproved AI products.

Traditional static network firewalls and blanket "no AI" policies fail for the same reason Dropbox once slipped past IT.

But the objective of this article is to help auditors understand the technology and the risks associated with AI to help your organization adopt AI safely.

Technology has always been a fast-moving area, but the introduction of AI has moved that pace into hyper speed. It requires learning a new vocabulary of AI gateways, runtime guardrails, and model observability well enough to ask a vendor a pointed question instead of nodding along to a sales deck. Let's shed some light on how these tools actually work.

Translating the standards for healthcare

Two frameworks dominate the conversation right now: ISO/IEC 42001 and the NIST AI Risk Management Framework (RMF). EY, PwC, and Deloitte have each published internal-audit-specific guidance mapping ISO/IEC 42001 and the NIST AI RMF onto healthcare risk programs; KPMG, notably, became one of the first Big Four firms to earn ISO 42001 certification itself.

ISO/IEC 42001, published in 2023, is essentially the AI management system sibling of ISO 27001 (the best-known standard for information security management systems). It follows the same structure, leadership commitment, risk assessment, controls, internal audit, and management review that any organization already running an ISO 27001 program will recognize. Still, it swaps 38 AI-specific controls for the 93 general information security controls.

It is also certifiable: a third party-accredited body conducts a two-stage audit. It issues a three-year certificate, which gives healthcare compliance teams something concrete to hand to a regulator or a plaintiff's attorney.

NIST AI RMF, by contrast, is voluntary and framework-based rather than certifiable, organized around four functions: Govern, Map, Measure, and Manage. Healthcare organizations have increasingly used it as the connective tissue between existing HIPAA obligations and newer AI-specific risks, mapping RMF controls directly onto protected health information (PHI) handling requirements.

HHS itself signaled the direction of travel with a Request for Information on AI adoption in February 2026. Neither framework carries the force of law today, but the pattern in every other regulated industry has been the same: voluntary guidance today, examination checklist tomorrow.

> In a previous article about Shadow IT (*New Perspectives*, Spring 2018), I borrowed the vigilante "The Shadow" to describe how employees quietly build their own IT solutions when sanctioned tools feel too slow or too limited. At that time, I was talking about Dropbox folders and rogue wireless access points. Well, the Shadow has grown a new limb since then, and this one writes full documents, drafts insurance appeals, and summarizes patient charts faster than any of us can keep an audit trail on it. It has a new name as well—AI.

When it comes to the internal audit lifecycle, AI isn't that different from other technology areas. It follows the familiar pattern of (1) discovery/inventory, (2) risk assessment/classification, (3) continuous monitoring.

With discovery, the emphasis should be on making sure this is a dynamic system rather than a static spreadsheet. As I mentioned earlier, the hyper speed of AI requires a faster, more dynamic approach. Auditors need to distinguish between risk levels and understand the difference between grammar-checking assistants and AI for analyzing diagnostic images.

One of the hardest aspects to implement is moving toward continuous monitoring. But this closes the loop, shifting audit away from the annual snapshot test and toward real-time, built-in systematic logging that can catch or stop violations before they happen.

Understanding commercial AI guardrail options

Once an organization accepts that Shadow AI cannot be eliminated as a risk, the conversation turns to which products can be used to address it. As of the writing of this article, I found that commercial guardrail products currently fall into three categories:

1. Network and security web gateways
2. Traditional infrastructure and firewalls
3. Dedicated AI trust, safety, and governance platforms

Each of these is worth exploring to determine whether existing platforms can be expanded to support AI workflows or whether new products are needed.

Network and security web gateways

Products like Netskope One AI Guardrails and Cloudflare AI Gateway sit at the hospital network edge and intercept traffic before an AI prompt ever reaches an outside AI model's servers. Netskope's platform can inspect requests and responses in real time. It can check for something called prompt injection while filtering, while also filtering against a defined set of risk-based words or concepts.

Prompt injection is a type of attack in which someone writes text into an AI chatbot (a prompt) to trick an AI system into ignoring its original approved instructions and performing unintended actions, such as revealing sensitive data or bypassing security measures and safety rules. Cloudflare's AI Gateway takes a similar approach to a middleman or proxy, by scanning prompts and responses for personally identifiable information (PII), financial data, and healthcare-specific patterns.

Auditors and IT security should be asking questions like the following:

- Can the gateway dynamically redact PHI before it leaves the network, rather than simply logging the violation after the fact?
- Does it support granular, role-based access so a policy does not identically govern a billing clerk and an attending physician?

Traditional infrastructure and firewalls

This category extends the web application firewalls that many hospitals already run but expands the use case to cover AI-related network traffic. Examples include F5 AI Guardrails and Akamai's Firewall for AI. Similar to the above-discussed solution, both sit between an application and its model, inspecting both the inbound prompt and the outbound response.

F5 claims built-in "Day 1" compliance controls for PII leakage and PHI protection. Of course, marketing materials and actual functionality need to be tested to ensure they align. F5 also claims that audit-ready logging traces every enforcement action back to a specific policy. Akamai's product does equivalent work at the network edge, filtering for toxic or hallucinogenic output. It also adds an element of data loss prevention by checking for unauthorized disclosure.

The auditor's checklist should confirm whether the vendor ships pre-built HIPAA compliance templates out of the box, or whether the hospital's own team will need to build that mapping from scratch. Auditors should also verify that the tool has been independently tested against adversarial prompt-injection attacks rather than relying on the vendor's marketing claims.

Dedicated AI trust, safety, and governance platforms

This tool category is the newest but also the most volatile. It deserves an extra note of caution if your organization wants to build a long-term control environment around it. It would not surprise me in the least if some of these tools were built quickly using AI to test AI, which could increase risk.

The tool Galileo built its reputation on deep evaluation of model outputs, catching hallucinations, bias, and policy violations before they reach a user. Another product, Obsidian Security, has carved out a niche in discovering shadow AI agents and unauthorized Model Context Protocol (MCP) connections hiding inside software as a service (SaaS) applications that the hospital already trusts.

What is vibe coding?

Vibe coding is a new approach to programming where you collaborate with AI to build software using plain language. Instead of writing every line of code yourself, you describe what you want the program to do, and the AI generates the code for you.

The pattern in every other regulated industry has been the same: voluntary guidance today, examination checklist tomorrow.

Auditors need to distinguish between risk levels and understand the difference between grammar-checking assistants and AI for analyzing diagnostic images.

Both do work that neither of the first two categories can fully replicate. But Galileo's acquisition by Cisco, which was completed in April 2026, and the subsequent folding of this tech into the Splunk Observability Cloud is worth flagging as a live example of what I described in the Spring 2018 Shadow IT article as the "going concern risk." In the era of vibe coding, this risk only increases.

A niche vendor can disappear from a larger platform's roadmap overnight. Auditors need to ask not just how a tool logs compliance violations for the audit trail today, but also what contractual protections exist if that vendor's ownership, pricing, or product direction changes months from now.

I've also recently had the privilege to view the new Darktrace Secure AI platform. Darktrace is known for its AI-driven cybersecurity that learns an organization's normal behavior to detect and autonomously respond to emerging threats in real time. They have applied that same level of defense to AI usage in the organization.

Specifically, they have some unique features that I am excited to see help healthcare organizations. First, their solution analyzes what users discuss in their chats and compares it to users' expected or authorized behavior.

Secondly, they specifically identify Shadow AI to determine which AI platforms are in use across the organization. This has multiple benefits, both in identifying what is being used and in helping shape AI adoption by knowing what platforms are preferred by the users. Like their other offerings, they provide an intuitive, single-pane-of-glass user interface that supports rapid decision-making.

Open-source alternatives

I am a big fan of open-source models for two main reasons: (1) one can see what the solution is actually doing, and (2) there are typically lower entry costs.

Not every hospital system has the budget for an enterprise gateway license. Other IT leaders also emphasize data sovereignty, wanting every byte of patient data to remain within their own server clusters rather than transit a third-party vendor's cloud. That has pushed a wave of open-source projects into serious consideration by hospital IT departments that would previously never have looked twice at open-source options.

What is an open-source large language model?

Large language models (LLMs) are foundation models that use AI, deep learning, and massive data sets to generate text, translate between languages, and write many types of content (i.e., generative AI models).

- Proprietary LLMs are owned by a company and can only be used by customers that purchase a license.
- Open-source LLM code and underlying architecture are accessible to the public, meaning developers and researchers are free to use, improve, or otherwise modify the model.

One of the tools I've spent some time looking at is LiteLLM. This has become a default choice for many as a proxy for a localized model. Like the commercial tools, it sits in front of more than 100 LLM APIs, providing a hospital with a single OpenAI-compatible endpoint while handling authentication, per-project spend tracking, and budget enforcement across the models a department has been approved to use.

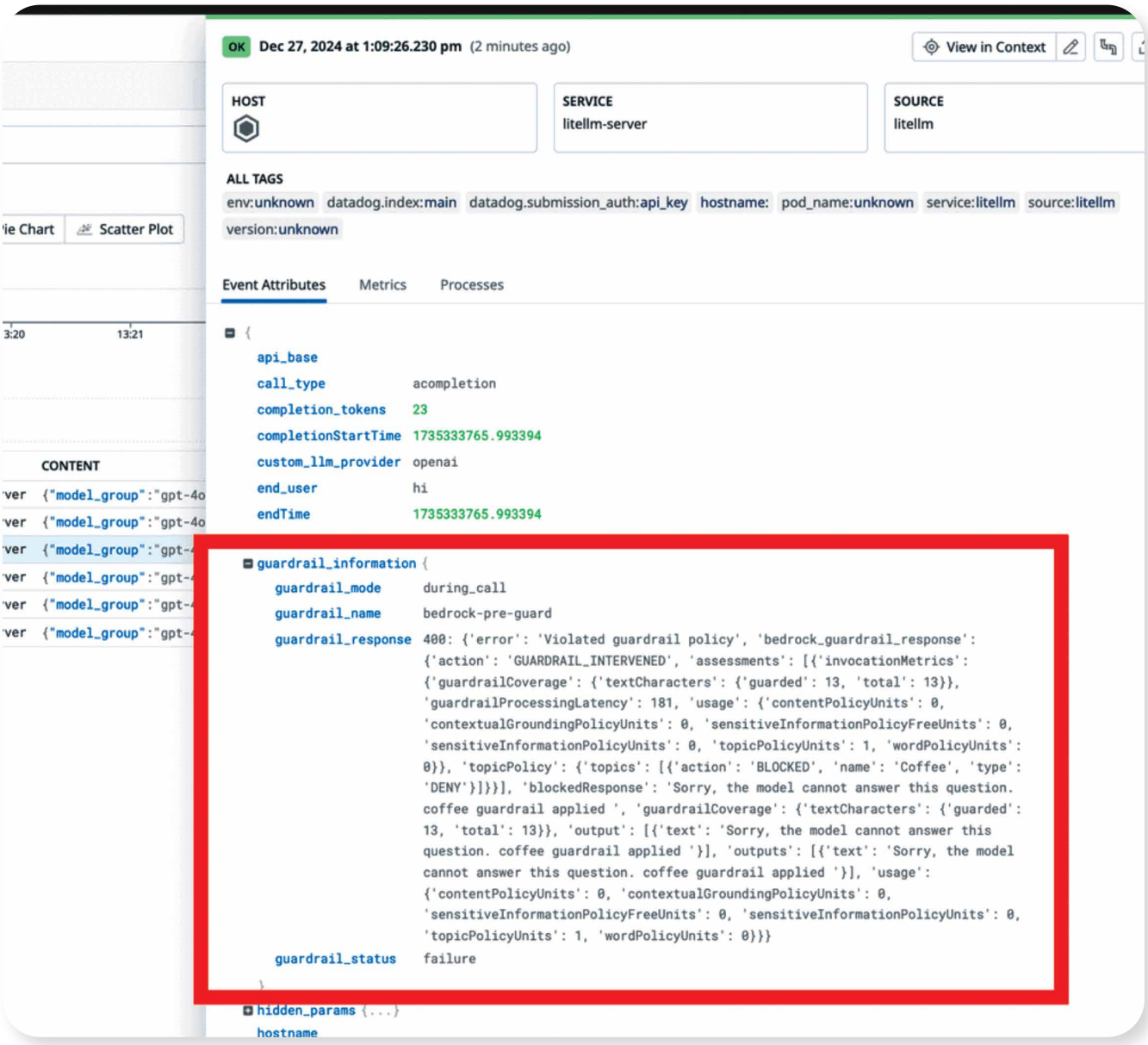
Exhibit 1 is a screenshot of the LiteLLM Guardrail rule being violated, and the response shows that "the model cannot answer this question" Auditors should expect this kind of default message when controls are designed to intercept and block disallowed queries before the model generates a response.

LiteLLM is genuinely useful and free, but it also carries the same risks that all software faces, especially in open-source projects. In March 2026, two published versions of the LiteLLM package on Python Package Index (PyPI),

versions 1.82.7 and 1.82.8, were compromised in a supply-chain attack. Organizations using an earlier release were unaffected, but those who updated had a compromised vulnerability added straight into their AI proxy layer. That is not a hypothetical maintenance-overhead concern for an audit work program; it is a documented event.

Many recognize NVIDIA as the world's leading maker of AI hardware (e.g., computer chips), but it also places strong emphasis on the software and systems that support that infrastructure. A lot of what it does is open source. An example is NVIDIA's NeMo Guardrails, which takes a different approach, using a purpose-built scripting language

Exhibit 1
https://docs.litellm.ai/docs/proxy/guardrails/quick_start



Not every hospital system has the budget for an enterprise gateway license.

For smaller, leaner hospital IT teams without a dedicated AI security engineer, open-source AI Guardrail solutions come with risks.

called Colang to define exactly what a model can and cannot talk about.

Rather than a single filter, it applies five separate guardrail types: input, dialog, retrieval, execution, and output. This allows an organization, for example, to block a clinical chatbot from ever providing medication dosage advice outside its intended scope, regardless of how the conversation evolves. It is Apache 2.0-licensed and actively maintained by NVIDIA, so at this point, there is some risk mitigation around the question of who patches this next year compared with a smaller community project.

Meta's Llama Guard is not a self-contained tool but rather an open-source model (LLM) that is safety-tuned to evaluate both the incoming prompt and the outgoing response. This can be used to flag content as safe or unsafe and cite the violated category. The current generation, Llama Guard 3, runs as an eight-billion-parameter model, supports eight languages, and is commonly paired with NVIDIA's NeMo Guardrails (mentioned above) as one of its community-model integrations rather than deployed on its own.

Auditors should note Meta's own published caveat: Input filtering catches more genuine risk but can also increase the false-refusal rate, leading legitimate clinical questions to be blocked alongside harmful ones. Auditors should be aware of and ensure that these types of models are fully tested in real-world settings.

HealthClaw Guardrails is an open-source, MIT-licensed reference implementation that sits as a vendor-neutral security layer between AI agents and Fast Healthcare Interoperability Resources (FHIR)-compliant clinical data servers. FHIR is a modern Health Level Seven international standard for exchanging healthcare data between systems in a consistent, API-friendly way. FHIR standardized how health data is structured, and Model Context Protocol (MCP) is the de facto way AI connects to resources and tools. HealthClaw aims to bring those two things together.

Every request passing through the proxy is subject to PHI redaction (truncating names, masking identifiers, stripping addresses). It also has an immutable audit log that records every read and write. It can also enforce human-in-the-loop confirmation before clinical data is written to the data servers.

There is a Quick Start guide that gives one a 10-minute demo using popular chat programs. I ran this demo with Claud.AI, and it helped me understand the Guardrail concept. If you want to try it yourself, use this link: https://github.com/aks129/HealthClawGuardrails/blob/main/docs/quickstarts/README.md

An example of the chat output is included in Exhibit 2. I recommend that you, at a minimum, take a look at this demo to further enhance your understanding of the concepts discussed in this article.

Risk matrix example

As with many software tools, organizations should not treat the above-mentioned or any commercial tool as fully interchangeable, or treat "open source" as a single risk category. Each one carries a different licensing model, a different maintenance burden, and a different path to a support contract when something breaks, or no support contract at all.

Exhibit 3 is an example of a risk analysis and comparison that an auditor could use to document, tool by tool, what the organization is accepting when it adopts each one, and what compensating control needs to sit alongside it.

By organizing the data this way, a few things stand out when the four tools are side by side:

- LiteLLM and Guardrails AI both offer a commercial escalation path.
- LiteLLM Enterprise and Guardrails Pro give an auditor something concrete to recommend if the organization wants open-source flexibility without giving up a support contract entirely.

Exhibit 2 - HealthClaw Demo in Claude.AI

Guardrail Conformance Result: Grade B (6/7 properties passing)

Property	Result
PHI Redaction	✅ Pass — names, SSNs, phone, address all properly masked
Immutable Audit Trail	✅ Pass — access is logged, no raw SSN leakage
Step-Up Authorization	✅ Pass — writes without a step-up token are correctly rejected (401)
Human-in-the-Loop	✅ Pass — clinical writes without human confirmation are blocked (428)
Tenant Isolation	✅ Pass — cross-tenant reads are rejected
Medical Disclaimers	✅ Pass — clinical reads carry the disclaimer
Error Fidelity	❌ **Fail — Grade F**

The one failure — Error Fidelity — is what's dragging the overall grade down from an A. In plain terms: the server isn't correctly rejecting malformed requests. Specifically:

- Sending an **unknown/unsupported search parameter** should get rejected outright but instead returns status 200 (success) — it's silently accepting garbage input rather than erroring.
- The **audit trail isn't recording these bad requests as failures** — so if something malformed slipped through, there'd be no trace of it having been a problem.
- **Unsupported search modifiers** aren't being rejected either (also returns 200 across the board).

This isn't a PHI leak or access-control hole — those six categories are solid — but it means the FHIR API is too permissive about malformed queries and the audit log won't reliably reflect that leniency. That's a real fix-it item for whoever maintains this HealthClaw deployment, not something you as the data user need to act on directly.

Want me to check `fhir_subscription_topics` or dig further into any one of these categories?

- NeMo Guardrails has no paid support tier of its own outside NVIDIA's broader AI Enterprise subscription, which is priced and sold at a scale most single-hospital IT departments will find hard to justify.
- Llama Guard sits in a different category: it is a model, not a managed service, distributed under Meta's own license rather than a standard open-source license, and it has no support channel beyond the community and the vendor hosting it.

For smaller, leaner hospital IT teams without a dedicated AI security engineer, open-source AI Guardrail solutions come with risks. A matrix like Exhibit 3 can help an organization

Exhibit 3 – Risk Matrix

Tool	License / Maintainer	Maintenance Overhead	Enterprise Support Path	Implementation Complexity	Auditor Note
LiteLLM	MIT (core); enterprise directory separately licensed and maintained by BerriAI.	High – near-daily releases; no Long-Term Servicing Branch to pin against.	Some guardrail management/UI features are gated to the Enterprise license, not the free proxy. Enterprise – commercial managed tier with custom support service level agreement (SLA).	Low-moderate. Single proxy config; broad model support (100+ LLM APIs).	March 2026 PyPI supply-chain compromise (v1.82.7/ 1.82.8). Verify Software Bill of Materials (SBOM), require commit pinning, and confirm patch process before routing PHI through it.
NVIDIA NeMo Guardrails	Apache 2.0. Maintained by NVIDIA.	Moderate – actively maintained, structured release cadence.	No dedicated paid tier; support only via NVIDIA AI Enterprise subscription (sales-gated, priced per Graphics Processing Units [GPU]/node).	High. Requires learning Colang scripting; five separate rail types (input, dialog, retrieval, execution, output).	Sends anonymous usage telemetry to NVIDIA by default (config/ provider names, active rail categories). Confirm telemetry settings before deploying in a PHI environment.
Meta Llama Guard 3	Llama Community License (Meta) – open-weight, not an OSI-approved open-source license; usage restrictions apply.	Low as a standalone classifier, but no formal patch/ support channel; community-driven only.	None direct. Typically requires pairing with a separate inference host or vendor for any SLA.	Moderate. Needs its own GPU inference hosting; usually deployed alongside NeMo Guardrails rather than standalone.	Meta's own documentation flags an elevated false-refusal rate on input filtering. Validate against real clinical prompt samples before go-live.
Guardrails AI (guardrails-genai)	Apache 2.0 (core). Maintained by Guardrails AI.	Moderate – active project; dual open-core/ commercial model.	Guardrails Pro – commercial managed tier with hosted validation, observability, and support SLA.	Low-moderate. Validator-based; checks pulled from the community Guardrails Hub.	Hub validators are community-contributed and vary in the depth of their reviews. Treat each validator as a separate third-party component requiring its own review before use with PHI.

By 2030, more than 40% of enterprises are expected to experience a security or compliance incident tied to unauthorized Shadow AI usage.

leaning on LiteLLM or Guardrails AI in production to budget for the commercial tier as compensating controls, even if the initial pilot runs on the free version.

An organization deploying NeMo Guardrails or Llama Guard without NVIDIA or Meta support behind them should treat internal prompt-engineering expertise as a named, retained skill on the IT roster, not a nice-to-have, because there is no vendor to fall back on if that person leaves.

Auditor's field manual: Building the work program

All of this architecture is only as good as the testing program built around it, so here is what a starter work program might look like for a healthcare internal audit function tackling Shadow AI for the first time.

1. *Verify the AI inventory first.* Cross-reference the IT department's approved AI tool purchases and license lists against what is actually flowing through your organization's network. The gap between those two lists is your starting risk universe, and you might be surprised as to what you find. There is likely a lot of Shadow AI occurring.
2. *Evaluate the gatekeeper's effectiveness* using a red-team approach. A red-team approach involves a trusted group deliberately acting like an attacker to test and improve an organization's defenses. Rather than trusting the vendor's data sheet, send a controlled, realistic, but entirely fabricated PHI (e.g., a fake patient name, medical record number, and diagnosis) through the corporate network to a consumer AI endpoint (ChatGPS, Perplexity, Gemini, etc.), and confirm the guardrail actually catches and masks it, rather than trusting the vendor's data sheet.
3. *Assess model telemetry* (i.e., automated collection and transmission of data from remote locations to a central system) by auditing the guardrail platform's own log files, not just the underlying AI tool's log files. Confirm the logs comprehensively capture blocked prompts, system access, and, critically, any manual overrides an employee may have attempted to use to push a blocked request through. As with all logs, a log with no entries is a red flag, not a clean bill of health.
4. *Finally, review autonomous agent governance* as AI tools move from drafting text to taking action (i.e., "agentic AI"). Inside clinical data workflows, look for tasks such as scheduling follow-up appointments, submitting prior authorization requests, and updating a medication list. Auditors need to confirm that any of these automated processes have logic loops requiring human sign-off before a decision is finalized.

Gartner's own research puts the stakes in plain numbers: By 2030, more than 40% of enterprises are expected to experience a security or compliance incident tied to unauthorized Shadow AI usage, and separate research from IBM found that Shadow AI added roughly $670,000 to the average cost of a data breach when it was part of the breach vector. That is not a rounding error on next year's audit budget, and it is not a risk that annual routine control testing will catch in time.

Conclusion

Shadow AI is inevitably driven by genuine clinical demand for efficiency. Today, trying to fully restrict AI is about as effective as last decade's attempt to ban Dropbox to keep files off personal laptops.

What internal audit can and should do is advocate for the technical runtime guardrails, commercial or open source, that let organizations confidently protect patient data while still empowering the innovation that clinicians are reaching for anyway. The shadow is not going away. Your job is to make sure it stays in the light long enough for someone to look at what is in it. **NP**

David E. Sems, CPA, CITP, CFF, is a recognized expert in cybersecurity and digital forensics, with over 20 years of experience investigating complex cybercrimes, leading global forensic technology teams, and advising law enforcement and corporations on matters including hacking, data theft, and advanced analytics. David can be reached at David@semsassociates.com and 440-941-7367.

FEATURE

Elevating Behavioral Health Audits – Part 1

Gather insights into effective practices

By Erin Panek, RN, CPHQ, and Cheryl Snook, MLS (ASCP), MBA

If behavioral health (BH) audits haven't risen near the top of your audit priority list, you may need to reassess this risk area. BH needs continue to be prevalent across the United States, and healthcare systems are treating significant numbers of patients presenting with BH chief complaints/diagnoses, substance use disorders, and crisis-related concerns.

Data from the Substance Abuse and Mental Health Services Administration (SAMHSA) estimates that more than one in five U.S. adults live with a mental illness (59.3 million in 2022; 23.1% of the U.S. adult population). Individuals with mental illness or addiction are more likely than the general population to have an emergency department visit or hospitalization. As a result, auditors should consider evaluating the effectiveness of behavioral health (BH) processes, identifying compliance risks, and providing recommendations that support both patient safety and organizational objectives.

In a two-part series, we will explore several BH circumstances and their potential risks and clinical interventions. In this installment, we'll outline considerations across all types of BH engagements and specific requirements for engagements of involuntary holds. In part two, we'll review tools and opportunities for audits of suicide risk screening/interventions, use of restraints (mechanical and chemical), and other potential BH processes.

Planning activities

The success of a BH audit is often determined during the planning phase. Auditors must first gain an understanding of the BH process being performed, the risks associated with those processes, and the controls that management has implemented to mitigate those risks. Key planning activities include identifying crucial resources and subject matter experts. This enables the audit team to develop appropriate process narratives, perform effective walkthroughs, and create meaningful test plans.

Potential behavioral health (BH) processes to audit

- Involuntary holds
- Suicide risk
- Restraints
  - Mechanical
  - Chemical
- Other
  - Outpatient processes
  - Seclusion
  - Maternal BH
  - Substance use/abuse

Identifying crucial resources

Policies, procedures, and guidelines

Resources help the auditor understand the risks and unique requirements of the BH processes. Policies, procedures, and guidelines provide different perspectives on organizational expectations, requirements, and best practices. You can see an example of an emergency mental health hold policy in Exhibit 1. Reviewing these documents allows auditors to identify control expectations and develop testing criteria. Supporting forms, documentation tools, and logs should also be evaluated to understand how compliance is demonstrated in practice.

Exhibit 1 – Example policy

The following example policy was compiled from open-source reference materials, including state statute. It is provided for illustrative purposes and is not the official policy of any specific company or organization. A mental health hold for involuntary treatment policy in Colorado might include, but not be limited to, the following elements.

Emergency Mental Health Hold Policy and Procedures

Purpose

To summarize the procedure for placing an individual on an emergency mental health hold (MHH) as described more fully in the Colorado Revised Statutes, 27 65 101 et seq.

Policy for taking an individual into custody

When any person appears to have a mental illness and, as a result of such mental illness, appears to be an imminent danger to others or to self or appears to be gravely disabled, an intervening professional, upon probable cause, may take the person into custody, or cause the person to be taken into custody and placed in a designated or approved 27 65 facility for a 72-hour hold for treatment and evaluation. Once an MHH has been initiated, the person cannot voluntarily leave until the MHH has been resolved.

Procedures

1. **Placement of an MHH**
    a. **Authorized persons**
        The following persons may place an MHH:
        i. Certified peace officer
        ii. Physician or licensed psychologist with a license in the state of Colorado
        iii. APRN with psychiatric/mental health training
        iv. Licensed clinical social worker
    b. **Documentation**
        A person meeting the qualifications above must document on a *Behavioral Health Administration-approved application:*
        i. The circumstance under which the person's condition was called to the documenter's attention
        ii. That the documenter believes that the person is mentally ill and, as a result, is an imminent danger to self or others, or gravely disabled, and facts sufficient to establish this conclusion
        iii. When the person was taken into custody
    c. **Advisement of patient rights**
        Each person placed on an MHH must be advised of his/her rights, and documentation of the same must be entered into the medical record.
2. **Discharge of person placed on an MHH**
    a. **Discharge instructions**
        Each person detained for an MHH will be provided with discharge instructions.
    b. **Required elements of discharge instructions**
        At a minimum, the discharge instructions must include:
        i. A summary of why the person was detained or evaluated for an MHH
        ii. A safety plan for the person and, if applicable, the person's lay person
        iii. Notification to the person's primary care provider, if applicable
        iv. The phone number to call or text the Colorado crisis services hotline and information on the availability of peer support services
        v. A list of any screening or diagnostic tests conducted during the MHH

Employee education

Understanding employee education is another essential component of audit planning. Healthcare organizations frequently rely on training programs to operationalize BH requirements and maintain regulatory compliance. Auditors should understand how educational content is developed, who is responsible for assigning training, which employees are required to complete it, and how completion is monitored. Evaluating the alignment between educational content and organizational policies can provide valuable insight into whether staff is adequately prepared to execute required processes. Auditors should consider performing a walkthrough of education on specific BH processes.

Understanding the regulatory environment

Federal, state, and local laws

Auditors should consider federal laws/regulations and legislative initiatives. Awareness of emerging legislation and regulatory changes is especially important because they may impact organizational operations and future compliance obligations. Auditors should also keep in mind that because BH records contain particularly sensitive patient information, several laws emphasize the increased harm of BH record disclosure.

While the following list is not exhaustive, these federal laws should be considered when planning any behavioral health audit.

- The Mental Health Parity and Addiction Equity Act – Federal law that generally prevents group health plans and health insurance issuers that provide mental health or substance use disorder benefits from imposing less favorable benefit limitations on those benefits than on medical/surgical benefits.
- Health Insurance Portability and Accountability Act (HIPAA) – National standards for protecting sensitive patient health information, including mental health records.
- 42 CFR Part 2 - Regulation that provides stricter privacy protections for substance use disorder treatment records than HIPAA, particularly for programs funded or regulated by the federal government.

BH audits also require a comprehensive understanding of applicable state and local laws. State regulations, such as the statute summarized in Wyoming's Involuntary Hospitalization Process, can vary significantly and often dictate requirements surrounding patient rights/safety, involuntary holds, documentation standards, notification requirements, and release procedures. Auditors should identify the specific legal requirements applicable to each state included within the audit scope and incorporate them into audit testing.

Hospital accreditation

The Joint Commission National Patient Safety Goals (see Exhibit 2) and/or other accreditation standards specific to BH processes should also be incorporated into audit planning. These standards address key areas of patient safety care that are associated with preventable harm, medical errors, and adverse events with the objective of improving patient safety and quality outcomes.

Healthcare news sources

Auditors should also monitor industry publications, white papers, professional associations, and healthcare news sources to remain informed about developing trends and best practices in BH.

> When planning your BH audit, be sure to review the *New Perspectives* award-winning article "Behavioral Health Billing Compliance" in Volume 45, Number 2.

Leveraging subject matter experts

BH audits are most effective when key stakeholders are involved early in the process. Auditors can identify and engage decision-makers, policy owners, clinical leaders, providers, social workers, nurses, care management teams, and other frontline caregivers who understand the operational realities of BH care delivery. These individuals often provide critical insight into workflow challenges, control

Individuals with mental illness or addiction are more likely than the general population to have an emergency department visit or hospitalization.

Healthcare organizations frequently rely on training programs to operationalize requirements and maintain regulatory compliance.

Exhibit 2 – Joint Commission National Patient Safety Goals

JOINT COMMISSION™

2026 Behavioral Health Care National Patient Safety Goals

(Easy-To-Read)

Identify individuals served correctly

NPSG.01.01.01	Use at least two ways to identify individuals served. For example, use the individual's name *and* date of birth. This is done to make sure that each individual served gets the correct medicine and treatment.

Use medicines safely

NPSG.03.06.01	Record and pass along correct information about an individual's medicines. Find out what medicines the individual served is taking. Compare those medicines to new medicines given to the individual served. Give the individual served written information about the medicines they need to take. Tell the individual served it is important to bring their up-to-date list of medicines every time they visit a doctor.

Prevent infection

NPSG.07.01.01	Use the hand cleaning guidelines from the Centers for Disease Control and Prevention or the World Health Organization. Set goals for improving hand cleaning.

Identify individuals served safety risks

NPSG.15.01.01	Reduce the risk for suicide.

Improve health outcomes for all

NPSG.16.01.01	Improving health outcomes for all is a quality and patient safety priority. For example, health care disparities in the patient population are identified and a written plan describes ways to improve health outcomes for all.

State regulations can vary significantly and often dictate requirements.

activities, and areas of potential risk that may not be evident through document review alone.

Process walkthroughs conducted with these stakeholders help validate process narratives and identify potential differences between documented procedures and actual practice. These discussions can also uncover informal controls, monitoring activities, and workarounds that may influence audit conclusions.

Developing an appropriate audit scope

BH audit scopes should be tailored to the organizational environment. Factors such as inpatient versus outpatient settings, BH facility types, organizational size, geographical footprint, patient populations, and available resources could potentially influence audit design.

Auditors can determine whether the engagement is intended to be an assurance audit, advisory review, or a combination, depending on organizational needs and internal audit risk assessment. The time period covered by the engagement should also be considered if there is a new or updated policy, law, or requirement.

Audit population development and sampling approaches also require consideration. The availability of reliable data, complexity of documentation requirements, extent of manual chart review, and/or potential use of artificial intelligence (AI) tools may influence testing methodology. Auditors should ensure samples are sufficient to support conclusions while remaining practical given available audit resources. Data analytics and/or AI may be useful in identifying trends, but many BH audits still require detailed review of clinical documentation and narrative notes to fully understand compliance and patient care considerations.

Also consider the population's age demographics, as BH processes often differ for pediatric versus adult patients. State and/or organizational requirements may vary for pediatric patients, including the selection of screening tools, assessment timing, and parent or guardian notification. Organizations may also differ in their definition of a pediatric patient.

Additional planning consideration

Even after careful planning to understand risks and controls, auditors may still need to update test plans during fieldwork based on patient complexity and because documentation can occur in multiple places/ways in the electronic health record.

Executing fieldwork and communicating results

During fieldwork, auditors should maintain regular communication with clients and subject matter experts. While performing chart review, questions can arise. Also, in BH environments, the identification of significant safety concerns or regulatory violations may necessitate immediate escalation rather than waiting until final reporting.

One challenge in BH audits is data/results aggregation. Unlike traditional compliance audits, findings may not always be easily quantified. Auditors may need to analyze narrative documentation, identify trends within clinical notes, evaluate medication usage patterns, or assess the timeliness of interventions. Interpretation of these data points often requires both audit expertise and clinical understanding.

When developing findings, auditors should look beyond individual exceptions and consider broader themes. Documentation deficiencies, inappropriate order management, gaps in staff education, inconsistent workflows, and unclear policies may indicate systemic issues rather than isolated events. Understanding organizational risk tolerance and involving appropriate stakeholders in action planning helps ensure recommendations are both effective and sustainable.

Auditors should be mindful of action plans that recommend hard stops in the medical record. Hard stops can include:

- Best-practice advisories – automated EHR alerts that guide clinicians toward guideline-based care
- Clinical decision support alerts – those in which the user is either prevented from taking an action altogether or allowed to proceed only with the external override of a third party

Auditors should again leverage subject matter experts to assess the operational impact of any hard stop, including

workflow integration, resource requirements, potential alert fatigue and other unintended consequences, supporting policy and education needs, monitoring expectations, practicality, and alignment with organizational risk tolerance.

Involuntary hold audit considerations

Involuntary hold processes represent a particularly high-risk BH area due to the significant patient rights, legal, regulatory, and patient safety implications involved. These holds may be referred to by different names depending on the state, including emergency holds, psychiatric holds, temporary detention orders, civil commitments, or 72-hour holds. Involuntary commitment laws exist in every state. Despite differences in terminology, the underlying objective remains the temporary detention and evaluation of individuals who may pose a risk to themselves or others or who require immediate psychiatric assessment.

Auditors should begin by understanding the complete involuntary hold process, including how patients are identified, who is legally authorized to initiate a hold, what documentation is required, and how monitoring is performed during the hold period.

Auditors should pay attention to the following (if required):

- Patient rights documentation
- Physician orders
- Required assessments
- Observation practices
- Safety interventions
- BH consultations
- Discharge procedures

It is also important to understand if any monitoring is currently being performed on patients who are placed on an involuntary hold (i.e., what is being monitored, by whom, how often, who it is being reported out to).

Consider a walkthrough on documentation of the involuntary hold, including the following questions:

- Who documents?
- Who is required to document?
- Where in the EHR is the process documented (e.g., provider notes, nursing/care management notes, flowsheets, scanned documents)?
- Are there corresponding order sets?
- Is the process different for involuntary holds placed in the community versus in the facility?

Testing should evaluate not only whether required documentation exists, but also whether actions occurred within required timeframes. Timeliness of order placement, reassessments, discontinuation of holds, and safety monitoring activities are often critical compliance elements. Because state laws vary significantly, auditors must ensure testing criteria are tailored to applicable state/local and regulatory/accreditation requirements.

Test plan considerations should include:

- State required forms (involuntary hold forms and/or patient rights forms)
  - Determine need/requirement of forms (state/organization specific)
  - Determine what is legally required to be filled out on the form
- Determine process differences
  - Community versus facility holds
  - State differences on who can place someone on hold, who can sign documents
  - State differences on who needs to be notified and how
  - Pediatric versus adult patient population
- Orders, order timing, and order discontinuation
  - EHR order requirement for involuntary hold
  - Additional precautions if necessary/required (e.g., suicide, elopement)
  - Mealtime safety precautions
  - 1:1 observation/sitter versus video monitoring
  - BH consult/assessment
- Documentation and timing of interventions
  - Justification of involuntary hold
  - 1:1 observation and timed assessments
  - Room safety check
  - Discharge processes

Conclusion

Behavioral health audits require a thoughtful and multidisciplinary approach that combines regulatory knowledge, clinical understanding, operational awareness, and strong audit methodology. Successful engagements begin with comprehensive planning, involve appropriate stakeholders, and focus on identifying meaningful risks and opportunities for improvement. As BH services continue to expand and evolve, auditors play an important role in evaluating compliance, strengthening patient safety, and supporting high-quality care delivery across health-care organizations. **NP**

Resources

Mental Illness - National Institute of Mental Health (NIMH)

Acute Care Use for Ambulatory Care–Sensitive Conditions in High-Cost Users of Medical Care with Mental Illness and Addictions--PMC

Suicide - National Institute of Mental Health (NIMH)

NCDAS: Substance Abuse and Addiction Statistics [2023]

Cheryl Snook, MLS (ASCP), MBA, is an Internal Audit Manager at Intermountain Health. Her auditing focus is clinical processes and operations for both acute and ambulatory care areas.

Erin Panek, RN, CPHQ, is an Internal Audit Director for Intermountain Health. Her auditing focus is clinical processes and operations for both acute and ambulatory care areas.

Accounting for *more* than numbers.

You're in the right hands with Weaver.

Afton G.
Valued team member since 2021.

weaver
Assurance • Tax • Advisory

Learn more at **weaver.com**

The Seven Signs of Ethical Collapse – Part 3

Pull back the curtains that cover bad behavior

By Marianne M. Jennings, JD

Twenty years ago, I published my book The Seven Signs of Ethical Collapse: How to spot moral meltdowns in companies... before it's too late. *While the companies whose names are splashed across the headlines for falling into ethical collapse have changed, the patterns that lead to collapse have not. Auditors should understand these patterns and evaluate if their organization is at risk.*

This is the third of a four-part series where I review the seven signs with examples of organizational collapses that occurred since my book's publication. In this installment, I focus on three signs that are often more evident to auditors than governance.

The Seven Signs

In this four-part series, I review the seven signs of ethical collapse that auditors, leaders, governance, investors, and other stakeholders can observe and must confront:

1. Pressure to maintain the numbers (Part 1, in *New Perspectives* Volume 45, Number 1)
2. Fear and silence (Part 2, in *New Perspectives*, Volume 45, Number 2)
3. Young 'uns and a bigger-than-life Chief Executive Officer (Part 2)
4. Weak board (Part 2)
5. Conflicts (Part 3)
6. Innovation like no other (Part 3)
7. Goodness in some areas atoning for evil in others (Part 3)

Summary (Part 4, upcoming in *New Perspectives*, Volume 45, Number 4)

Sign #5: Conflicts

A conflict of interest (conflict) at work happens when personal interests, relationships, or outside activities interfere—or even just appear to interfere—with an employee's ability to make objective, unbiased decisions for their employer. Conflicts are the most difficult type of ethical lapse for those involved to admit and the easiest for those not involved to spot. But conflicts are a sign of impending ethical collapse because the conflicting relationships often end up costing the organization financially and reputationally.

WeWork

The full story on WeWork appears in the discussion of Sign #6: Innovation like no other. But the company's conflicts alone indicated it was headed for Chapter 11 bankruptcy.

Adam Neumann was the founder and CEO of WeWork. Mr. Neumann owned four of the buildings leased to WeWork. He borrowed $740 million using his shares of WeWork as collateral for a personal loan. His wife, Rebekah, was a co-founder and executive. Mr. Neumann's brother-in-law

Conflicts are the most difficult type of ethical lapse for those involved to admit and the easiest for those not involved to spot.

was running WeWork. Mrs. Neumann's brother-in-law was the chief product officer. Mr. Neumann was the landlord on many of the properties that WeWork was leasing. WeWork's vice chairman of the board had his parents serve as the real estate brokers on a WeWork building in Miami. Arash Gohari, the co-head of WeWork, also owned a building leased to WeWork. UA Contractors did renovation work for WeWork but also renovations in two of the Neumann's homes. Employees were not sure if UA Contractors was working for WeWork or the Neumanns.[1]

FTX

FTX had the same board members at FTX as it had at Alameda, which was its hedge fund/trading firm. There was little chance that either board would flag the issue of investor money deposited in the FTX crypto firm flowing to Alameda for its investment portfolio.

Columbia University

In 2026, Columbia University Medical School and its affiliation with New York Presbyterian Hospital (NYP) finally released a report outlining the findings of a third-party review[2] of its handling of the 25 years of sexual abuses of female patients by one of their top ob-gyn physicians. Robert Hadden's medical license was stripped, and he is serving a 20-year prison term for the crimes he committed during his long medical practice and affiliation with the Columbia Medical School.

In 2012, a patient reported to the New York Police Department (NYPD) Hadden's sexual assault during her postpartum office visit. NYPD officers went immediately to Hadden's office and arrested him. Hadden was released that evening without any charges being filed. The medical and administrative leadership at Columbia and NYP concluded that it was a first-time report and permitted Hadden to return to work provided he adhered to the chaperone policy during examinations.

Profiled organizations

In this four-part series, we consider the ethical and financial collapse of:

- Atlanta Public School system (APS)
- Boeing
- BP p.l.c. (formerly British Petroleum)
- Columbia University Medical School and New York Presbyterian Hospital
- FTX
- Madoff Investment Securities, LLC
- Nikola
- Theranos
- Wells Fargo
- WeWork
- additional healthcare-specific incidents are also noted

During the following five weeks that "Hadden continued to see (and abuse) patients,"[3] he repeatedly avoided allowing Columbia to interview him about the incident that led to his arrest. Then Hadden took paid and unpaid medical disability leave for nearly two years before his employment was terminated.

Civil lawsuits and state and federal charges followed as many women came forward with allegations of sexual abuse by Hadden over a 25-year period. Columbia and NYP hired a third party to investigate how Hadden was able to continue the abuse over decades. That report revealed the following:

1. There was a lack of enforcement of the chaperone policy and a failure to designate employees as chaperones to be present during patient exams.

[1]Eliot Brown, "WeWork Draws Worries of Conflicts," *Wall Street Journal*, September 7, 2019, p. B1.

[2]Joan Loughnane, Michael Levy & Kathleen Carlson, "Report of Investigation into the Circumstances That Allowed Robert Hadden to Abuse Patients," March 10, 2026, https://www.cuimc.columbia.edu/file/57777/download?token=tUnNbKrl

[3]*Id*, at p. 67.

2. Employees did not report what they were witnessing as chaperones because they were not trained on how to be a chaperone or how to report concerns about a physician. Employees feared retaliation if they raised questions about a doctor's behavior in Columbia's and NYP's hierarchical professional environment. Even when employees were asked about an incident reported about Dr. Hadden they responded that they witnessed nothing inappropriate (a function of their fears of retaliation).
3. There was no complaint reporting policy for patients or employees.
4. There was no process for handling patient or employee reports or complaints if a patient or employee came forward with concerns.
5. There was a distinction in classification of patient and employee reports. There were reports (e.g., about long wait times) that were treated differently from complaints, with complaints requiring some type of action. But discretion in classification controlled the scope of response. There were also alternative terms used such as "grievances" with a resulting lack of clarity in responses.
6. When there were complaints about Hadden, no record was placed in his file. When the NYPD was doing its investigation, administrators told the officers that it was the first complaint against Hadden. There was no system in place for tracking complaints, investigations, and outcomes. Complaints were often dismissed based on undocumented conversations.
7. Deference to physicians was the cultural norm.
8. Administrators believed Hadden's denials over employee complaints because of their friendships with Hadden or, with their limited information, his stellar reputation.[4]

Precision Lens

After nearly a decade-long lawsuit, a Minnesota federal jury found that Precision Lens had submitted 64,575 false claims to Medicare, which resulted in more than $43 million in overpayments from the program. The settlement of $490 million included treble damages and penalties and recognized that Precision Lens regularly offered kickbacks in the form of luxury travel, sports tickets, and so on, to incentivize the use of its products in cataract surgeries.

In addition to the risk of kickbacks, other conflicts may particularly affect physicians and other healthcare professionals. Healthcare providers may hold shares in other sectors, such as pharmaceutical companies or research centers, receive gifts or payments from them, and accept travel expenses to attend meetings. Clinicians may be involved in developing new treatment methods and medical devices or may participate in educational activities and various research studies. These collaborations and activities can lead to conflicts of interest.

Even when healthcare leaders think they work without bias, relations may indirectly influence organizational structures and independence, clinical evidence and treatment decisions, research integrity, and public opinion. Stark and Anti-Kickback laws were enacted to discourage financial incentives from corrupting medical judgment.

Audit tools for Sign #5

Assess your organization's conflict of interest policy to assure it:

- Clearly defines, in writing, what constitutes a conflict of interest
- Identifies classes of individuals in your organization covered by the policy
- Facilitates disclosure of information that may help identify conflicts of interest
- Sets out procedures to follow in managing conflicts of interest

Columbia hired a third party to investigate how a doctor was able to continue the abuse over decades.

[4] *Id.*, pp. 1-10.

Stark and Anti-Kickback laws were enacted to discourage financial incentives from corrupting medical judgment.

Review the periodic conflict disclosure process, the process for evaluating disclosed potential conflicts of interest, and measures to mitigate or eliminate conflicts. Review records of all disclosures, evaluations, mitigating measures, and decisions related to actual or possible conflicts of interest.

Use the Columbia-NYP report findings to evaluate your organization's processes for rules violations investigations, systems for reporting and tracking reports, resolution explanations and documentation, and potential conflicts in the investigation and reporting processes.

Sign #6: Innovation like no other

The previously covered Theranos, Nikola, and FTX examples all illustrate how companies with new products and ideas capture investor and media attention but avoid high-level scrutiny. The charm of new ideas and products creates a shield from inquiry.

WeWork (aka WeCompany)

WeWork's idea of temporary offices located across the country sounded brilliant, and its CEO, Adam Neumann, was a charmer. But no one was paying attention to the company's governance, controls, and processes until it tried to go public.

Its filings with the SEC indicated the company was employing members of the CEO's family, there were too many private jet excursions, and spending was excessive, especially on emergency shipments of furnishings for the offices. As a result, an attempted 2019 initial public offering was suspended, an intervening rescue package forced out Neumann (who still managed to collect an exit package of roughly $1.7 billion), and WeWork ended up in Chapter 11 bankruptcy in 2023.[5]

Although the business media referred to it all as a "stunning downfall," it was anything but because all seven signs were present. WeWork did return with a new IPO as WeCompany and then paid Adam Neumann over $5 million for the WeWork name. Since 2024, it has new owners, has downsized, and faces challenges, but at least the Neumann spending is gone.

Telemedicine fraud

The rapid expansion of telemedicine in the United States, particularly during and after the COVID-19 pandemic, transformed how healthcare services were delivered. While virtual care improved access for millions of patients, it also created opportunities for large-scale fraud.

In 2023, federal authorities uncovered widespread abuse of telehealth platforms, marking one of the largest healthcare fraud enforcement actions in history. The U.S. Department of Justice (DOJ) announced criminal charges against dozens of individuals, including doctors, telemedicine executives, laboratory owners, and marketing intermediaries, for orchestrating schemes that generated over $2.5 billion in fraudulent claims. Investigators found that sham telemedicine consultations were routinely used to authorize medically unnecessary genetic tests, durable medical equipment, pain creams, and prescription medications.

The scandal exposed major weaknesses in telehealth oversight, billing controls, and provider accountability. Relaxed regulations, combined with limited real-time verification of patient interactions, allowed fraudulent actors to exploit digital healthcare systems at scale. Beyond financial losses to Medicare and taxpayers, the schemes posed serious patient safety risks by promoting unnecessary or inappropriate medical interventions.

NextGen Healthcare

The $31 million False Claims Act settlement against NextGen Healthcare, an electronic health record vendor, demonstrates an emerging field of healthcare technology fraud cases.

Two nurses blew the whistle by informing the DOJ that "NextGen Healthcare sold software that was designed to [help providers meet meaningful use requirements] for a Medicaid stimulus program. However, [this software] relied on an auxiliary product designed only to perform the

[5] Peter Eavis, "WeWork's Woes Not Shared by Rival," New York Times, October 2, 2019, "p. B3

certification test scripts of the program and lacked 'critical functionality.'" According to the DOJ, NextGen also violated the Anti-Kickback Statute by providing "remuneration" to clients—with tickets to sporting events and credits worth up to $10,000—to incentivize purchases and referrals for NextGen's software.

Audit tools for Sign #6

When others may be blinded by the razzle dazzle of innovation, internal auditors can continue to serve as the eyes and ears of the organization by adhering to the IIA Global Internal Audit Standards. Carefully abide by Domain II: Ethics and Professionalism Standard 2.1 Individual Objectivity, and Standard 2.2 Safeguarding Objectivity, by making judgments based strictly on balanced, verifiable evidence.

Healthcare organizations should welcome information from internal sources. Remember that a whistleblower wrote a letter to the Centers for Medicare & Medicaid Services (CMS) exposing problems at Theranos. CMS undertook a surprise inspection, which uncovered numerous violations. Another whistleblower notified a journalist who published an article revealing that Theranos was not using its own machines for blood tests and that its "Edison" device provided unreliable results. While Theranos denied all the allegations as false, law enforcement and the SEC then began investigating Theranos.

Verify the effectiveness of your organization's compliance reporting process. As Vic Hartman pointed out in a previous Healthcare Fraud column ("Internal Auditors' Role in Navigating the False Claims Act," *New Perspectives* Volume 44, Number 4), whistleblowers typically report misconduct through internal mechanisms. Therefore, auditors should:

- Test reporting mechanisms
- Evaluate responsiveness to complaints
- Analyze complaint patterns for organizational blind spots
- Assess cultural factors that inhibit a speak-up environment

Sign #7: Goodness in some areas atoning for evil in others

This sign is one of the easiest to spot and perhaps the most telling. An emphasis on all the good the organization is doing for others may mask areas of potential concern. First, there may not be as much attention to running the business itself as there should be. Second, philanthropy may be undertaken because of an accurate belief that goodness in popular causes deflects scrutiny and atones for fraud and other bad behavior.

The shroud of social responsibility is quite protective, at least until the eventual crash. Healthcare itself is a public good and often allows even greater liberties in operations and finances because of the goodness in serving others and saving lives.

Organizations chase social responsibility issues with the hope of receiving good ratings and becoming a darling with assumed goodness that re-directs discerning eyes away from their actual business performance. "But," say outsiders, "you committed fraud." And the response is along the lines of, "But we did recycle." The equation of atonement is not quite equal.

BP

BP was celebrated as an oil company that embraced environmental issues and was working to wean itself and customers away from fossil fuels. BP was named #1 on *Fortune* and AccountAbility's annual rankings of the world's most responsible companies in 2007.[6] Then came the 2009 explosion on BP's Deepwater Horizon offshore well, and nothing would ever be the same. The social responsibility evaluators were shocked, shocked! that their star oil company would cause a bigger spill than the Alaska Exxon Valdez oil spill.

Those of us who had studied BP knew that Deepwater Horizon was an inevitable collapse because of the cost

While virtual care improved access for millions of patients, it also created opportunities for large-scale fraud.

[6]Natalya Sverjensky, "Beyond Petroleum: Why the CSR Community Collaborated in Creating the BP Oil Disaster," *Ethical Corporation*, Aug, 2, 2010.

An emphasis on all the good the organization is doing for others may mask areas of potential concern.

pressures BP was facing and the inability of engineers and contractors working in the field to raise their concerns about safety, risk, and needed repairs.

In fact, BP had a similar explosion (not as significant as the Deepwater Horizon explosion) at its Atlantis offshore rig a year before. Little was noted because of BP's devotion to environmental causes: no changes resulted to prevent explosions. "[M]anagers put off repairing the pump in the context of a tight cost budget.... Leadership did not clearly question the safety impact of the delay in the repairs.... A BP safety officer told company investigators, 'You only ever got questioned on why you couldn't spend less.'"[7]

The pressures BP was facing were that its earnings and exploration were down and the pressure to increase earnings was affecting the timing of repairs and honest evaluations of safety impacts. Issues were overlooked because of BP's vaunted social responsibility status.

FTX

Samuel Bankman-Fried often touted the buzzwords "effective altruism" and claimed he wanted to give FTX profits away to change the world for the better. FTX was an environmental, social responsibility, and government (ESG) darling. ESG ratings are, at best, inconsistent, and at worst inaccurate and politically charged.[8]

Audit tools for Sign #7

Provide information on the quality of ESG rankings and ratings, including data and commentary in your organization's tax reports and other community-facing reports. Keep the board informed of ESG goals and any associated risks. Provide the board with background information on companies listed high in ESG rankings. Track expenditures for ESG projects and memberships to support board oversight. Share issues on problems with ESG-darling organizations and the effects of customer and investor backlash.

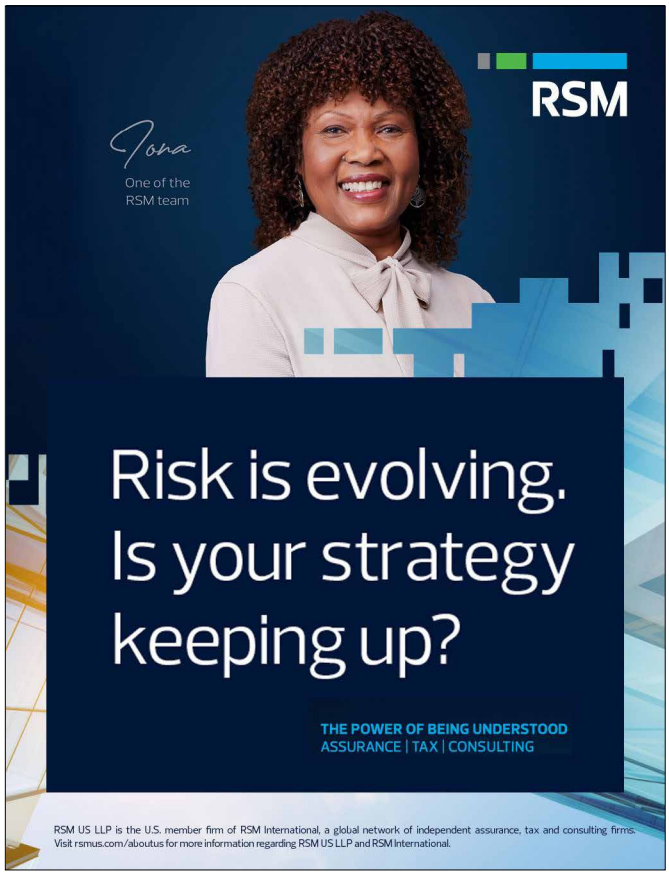
Shine the light

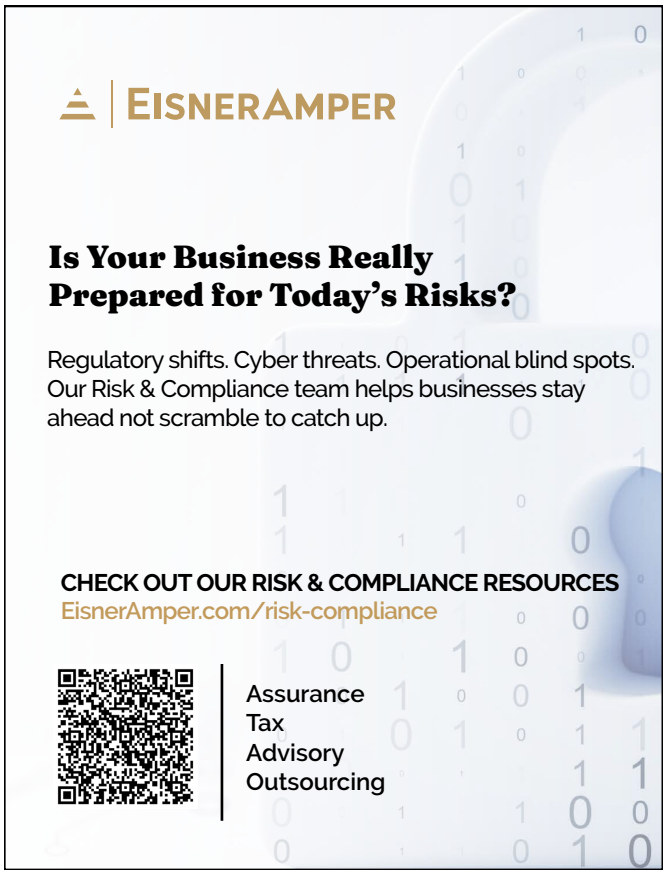
This subset of the seven signs highlights how auditors can intervene before overlooked concerns become systemic failures. Internal auditors are uniquely equipped to identify certain ethical warning signs early and challenge organizations to act on what they uncover. **NP**

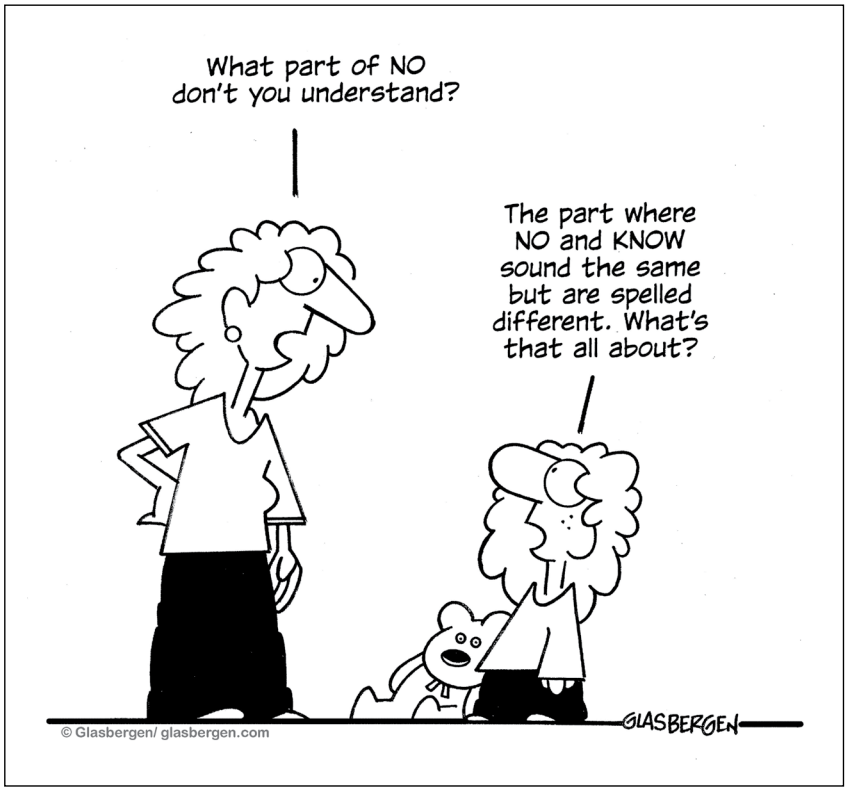
Marianne M. Jennings, JD, is a Professor Emeritus of Legal and Ethical Studies in Business at the W.P. Carey School of Business, Arizona State University, where she taught for 35 years. Her book The Seven Signs of Ethical Collapse *(St. Martin's Press, 2006) has received several book awards, including recognition of the* Library Journal. *Her next book,* Hornswoggled: How Management Books, Gurus, Theories, and Fads Harm Organizations, *is forthcoming in 2026. You can reach Marianne at Marianne.Jennings@asu.edu.*

[7]Guy Chazen, Benoit Faucon, & Ben Casselman, "Safety and Cost Drives Clashed as CEO Hayward Remade BP," *Wall Street Journal* June 30, 2010, p. A1.
[8]Joe Rennison, David Yaffe-Bellany, and Matthew Goldstein, "The Altruistic Beginnings of the FTX Debacle," *New York Times*, February 23, 2023, p. B1.

"It's dreadful what little things lead people to misunderstand each other."
- Lucy Maud Montgomery


RSM
Tona
One of the
RSM team
Risk is evolving.
Is your strategy
keeping up?
THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING
RSM US LLP is the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms.
Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.


EISNERAMPER
Is Your Business Really
Prepared for Today's Risks?
Regulatory shifts. Cyber threats. Operational blind spots.
Our Risk & Compliance team helps businesses stay
ahead not scramble to catch up.
CHECK OUT OUR RISK & COMPLIANCE RESOURCES
EisnerAmper.com/risk-compliance
Assurance
Tax
Advisory
Outsourcing


What part of NO
don't you understand?
The part where
NO and KNOW
sound the same
but are spelled
different. What's
that all about?
GLASBERGEN
© Glasbergen/ glasbergen.com

FEATURE

Auditing Capital Projects

Take a strategic approach to mitigating risks and improving project outcomes

By Kenneth J. Brzozowski, CCA, CCP, and Mary Jane R. Schroeder, CIA, CRMA, CICA, CHIAP®

Capital projects are among the largest and highest-risk investments an organization will undertake. Their complexity, long duration, and reliance on multiple internal and external stakeholders create exposure to cost overruns, schedule delays, control breakdowns, compliance issues, and fraud. Effective capital project auditing should therefore be proactive, risk-based, and integrated throughout the project lifecycle, not limited to closeout cost recovery.

For capital projects, earlier audit engagement brings greater value. Auditors can help management recognize risk indicators, strengthen governance, clarify contract requirements, and confirm that key financial, quality, and safety controls are operating before weaknesses become embedded in project execution.

Setting the stage

Capital projects in the healthcare industry are experiencing significant growth, driven by increasing demand for expanded access, specialized care, and modernized facilities. According to ConstructConnect, more than $28.4 billion in healthcare project starts were forecasted domestically for 2026, increasing to a forecast of $34.3 billion for 2029, with new construction leading activity and refurbishment projects also gaining momentum. Key healthcare capital trends include:

- Decentralization: Healthcare systems are expanding access by bringing comprehensive care to communities beyond the central hospital system. For example, a system in the Southeast built a new full-service acute care facility that includes a 24/7 emergency department, operating rooms, inpatient units, and a medical office building offering outpatient and specialty services.
- Specialized facilities: For example, Connecticut's first proton therapy center delivers highly specialized cancer treatment; it required exceptional construction precision. To ensure safe and accurate delivery of therapy, the building included multi-foot-thick radiation-shielded cyclotron vaults and vibration-sensitive equipment.
- Adaptive reuse: Healthcare systems are showcasing adaptive reuse when expanding and modernizing facilities by repurposing underused sites such as abandoned car dealerships, supermarkets, and retail stores. Many of these sites have become ambulatory and surgical care centers.

These trends demonstrate the scale and complexity of healthcare capital investment. This growth also increases exposure to budget overruns, schedule delays, logistics uncertainty, control weaknesses, ineffective project delivery or contracting, and potential fraud.

Per BSA Design Hospital Construction Cost Data for 2026, hospital construction costs vary significantly by facility type, with large acute care facilities commanding the highest pricing due to their complexity and specialized infrastructure requirements. Outpatient and smaller facilities remain more cost-efficient but still face elevated pricing levels.

Construction costs also differ considerably by region, with the Northeast and West Coast recording the highest premiums as labor constraints, regulatory requirements, and permitting complexity drive costs higher. This level of activity underscores the need for strong governance, disciplined controls, and robust audit practices to help ensure these investments are effectively managed.

Poor oversight of construction projects leads to severe operational and financial consequences. While organizations often experience strained internal resources, delayed facility openings, and unrecoverable cost overruns, the lack of

Auditing capital projects requires a shift from a cost recovery mindset to a cost prevention approach.

strict controls also opens the door to criminal exploitation. Breakdowns in governance have resulted in major legal and financial penalties, including a federal audit that uncovered a $4.8 million fraud scheme on a medical facility construction project involving misrepresentation of subcontractor eligibility, improper passthrough contracting, and undisclosed kickbacks.

Conspiracy to commit healthcare fraud carries a maximum potential penalty of 10 years in prison and a $250,000 fine. Conspiracy to violate the federal Anti-Kickback Statute carries a maximum potential penalty of five years in prison and a $250,000 fine.

In addition to these oversight risks, healthcare capital projects are being delivered in an increasingly uncertain market environment. Current and ongoing challenges include labor availability for project managers, engineers, and skilled trades; supply chain constraints; cost and price escalations; evolving project delivery methods; increased competition for goods and services; and insurance availability. Together, these factors reinforce the importance of timely independent review, transparent reporting, and proactive risk management throughout the project lifecycle.

Frame of mind

Auditing capital projects requires a shift from a cost recovery mindset to a cost prevention approach. This proactive stance requires audit involvement early enough to assess whether project governance, procurement strategy, contract terms, reporting structures, risk management practices, and cost controls are adequate before major commitments have been made or spending has occurred. See Exhibit 1 for an outline of the audit project lifecycle.

Project versus audit lifecycles

Auditors must understand how a construction project's development timeline dictates the timing and focus of the audit team's activities. While no two construction projects are identical, standard audit activities should align with common project execution milestones.

The project lifecycle and the audit lifecycle must be evaluated together. The timing of an audit intervention directly determines an organization's control options: early audits prevent risks, mid-project audits mitigate active issues, and late audits focus entirely on cost recovery and lessons learned.

Exhibit 2 maps the sequential project phases to their typical completion percentages, specific audit timing definitions, and core project characteristics.

Exhibit 1

FRAME OF MIND: AUDIT PROJECT LIFECYCLE

Design & Contracting	Construction	Commissioning / Close-Out
Initiation & Planning	Build Phase	Closeout
► Pre-Contract Audit ► Design Contract Audit ► Readiness Review ► Governance / Risk Review	► Initial Audit ► Interim Audit ► Performance Audit ► Quality Management	► Closeout Audit

Exhibit 2 – Project lifecycle, audit considerations, and timing

Project phase & completion %	Audit timing	Key project characteristics	Audit considerations
1. Conceptual & feasibility (0% complete)	**Pre-planning review**	Defining overall project need, securing early funding strategies, establishing preliminary budgets, and performing initial risk assessments	Reviewing governance frameworks, testing the feasibility of cost estimates, and evaluating initial scope definitions
2. Design & procurement *(before contract award)*	**Pre-contract award audit**	Developing engineering blueprints, refining budgets and project value, issuing solicitations, evaluating bids, and finalizing commercial terms	Assessing procurement compliance, verifying contract obligations and audit rights, reviewing cost-of-work and general conditions, and testing cost accounting system readiness
3. Early construction *(10% to 20% complete)*	**Initial audit**	Administering initial building steps, establishing project and cost reporting, and onboarding core contractor teams	Testing contract compliance and baseline governance, reviewing procurement and bid-award activities, and evaluating initial project management controls
4. Mid-construction *(40% to 80% complete)*	**Interim audit**	Managing ongoing physical building phases, administering active project schedules, and processing rolling payment applications	Conducting interim billing audits and labor rate testing, evaluating active change management and schedule shifts, testing use of allowances, contingencies and insurance, and following up on prior audit observations
5. Commissioning & closeout *(95% to final payment)*	**Closeout audit**	Testing systems and facility turnover, managing final project payments, and addressing outstanding legal claims or credits	Reconciling final contract value, allowances and contingencies, verifying lien waivers and closeout deliverables, and assessing claims, shared savings and lessons learned

Reading the signs

Capital projects have unique facts and circumstances, but common risk areas occur across industries and delivery methods. Risks can arise from ambiguous contract terms, insufficient change management workflows, or improper cost reconciliations. Additionally, external factors such as political volatility, shifting tax policies, labor markets, tariffs, pandemics, and supply chain disruptions can significantly impact project outcomes. Exhibit 3 outlines common risk areas, subtopics, and findings.

Exhibit 3

Common risk area	Common subtopics	Common findings
Project delivery (see Exhibit 4 for descriptions of common project delivery methods)	• Time & materials • Guaranteed maximum price • Indefinite delivery / indefinite quantities or unit price	• Owner or contractor lacks experience with the selected delivery method • Weak contractor coordination • Incomplete scope definition • Governance structure does not exist or align with delivery risk
Construction contract	• Baseline budgeting • Contingency/allowances • Insurance (may include contractor-controlled insurance program or owner-controlled insurance program) • Shared savings clauses • Final contract value reconciliation	• Ambiguous “cost of work” definition • Unclear tiered mark-ups • Lack of approved detailed hourly wage/rate schedules • Insufficient change management workflow • Insufficient audit rights or record retention requirements
Cost management	• Scope amendments • Contingency drawdowns • Insurance mark-ups on changes • Fee adjustments • Schedule impacts	• Insufficient transfers in/out reporting • Incorrect insurance premiums/enrollment • Improper cost reconciliations • Incorrect use of contingency and allowances • Unsupported cash flow variances
Change management	• Project schedule • Risk register • Cost forecasting • Executive reporting • Issue escalation	• Excessive changes indicative of poor initial planning • Lack of supporting documentation for scope changes • Undefined contract obligations or missing deliverables • Incomplete pricing support or unvalidated subcontractor quotes • Delayed approval or retroactive change documentation
Project controls and reporting	• Project schedule • Risk register • Cost forecasting • Executive reporting • Issue escalation	• Baseline schedule not approved or not actively maintained • Risk register is inaccurate or not shared with key stakeholders • Inconsistent reporting between source systems and executive reports • Limited documentation of mitigation actions and owners

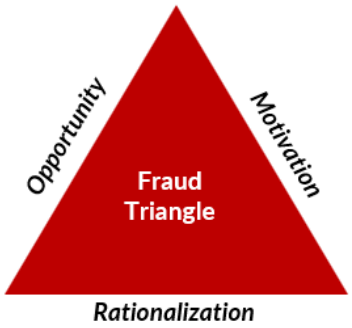
Exhibit 4 – Six main project delivery methods

Project Delivery Method	Description
Design-Bid-Build (D-B-B)	Also called "traditional project delivery," it involves a design team and a general contractor working directly for the owner under separate contracts.
Design-Build (D-B)	The owner provides a contract to a single firm that handles both the design and construction aspects of a project.
Construction Manager at Risk (CMAR)	The construction manager acts as a representative for the owner during the design and construction phases, and the CM takes on project risk, usually with a contract that has a guaranteed maximum price.
Construction Management Multi-Prime	The owner acts as the general contractor and establishes contracts with the design team as well as the major subcontractors on the project.
Public-Private Partnership (PPP or P3)	A private company and government entity collaborate on a project, typically funded by the government entity and managed by the private company.
Integrated Project Delivery (IPD)	Everyone involved in the project is on a single contract that is predetermined before the design phase begins, spreading risk and responsibility equally among all stakeholders.

Fraud Risks

Fraud remains a significant concern in construction projects because of the number of contracting parties, the volume of transactions, reliance on subcontractors, and the specialized nature of project records. Common fraud schemes in public and infrastructure-related construction environments include bid rigging and collusion, bribery, conflicts of interest, small and local business fraud, kickbacks, materials overcharging, product substitution, and time overcharging.

The fraud triangle is a useful lens for understanding fraud exposure: opportunity, motivation, and rationalization. Capital projects can create opportunity when controls are immature, project teams are under schedule pressures, invoices are complex, cost data is not transparent, and/or management overrides established review processes.



Auditors should remain alert to fraud indicators such as inconsistent project controls reporting, unsupported payment documentation, limited transparency into subcontractor costs, recurring override of established controls, management resistance to audit inquiries, stale or incomplete risk registers, and unresolved discrepancies between cost systems, payment applications, schedules, and executive reports.

Bridging the gap

To bridge the gap between risk identification and mitigation, organizations should cultivate a culture supporting best-in-class auditing for capital project management. This requires full-scale integration of audit and assurance practices throughout the project lifecycle, from initiation through closeout.

Key strategies include:

- Conducting readiness reviews to assess organizational preparedness for decision management for critical spending and expenditures
- Performing governance reviews to confirm whether established controls are adequate and operating as intended
- Developing and maintaining a comprehensive risk register to document and address emerging risks and mitigation strategies
- Evaluating governance documents, policies, procedures, project management plans, and contract templates before they are relied upon in execution
- Using interim audits to identify control gaps early enough to take corrective action during the design and construction duration

Governance reviews

A governance review evaluates two critical dimensions of a project: design adequacy and operational compliance.

- Design adequacy assesses whether governing documents (such as charters, policies, and contract templates) include the necessary authority, roles, approval thresholds, risk management expectations, and audit rights. A framework is inadequate when a material control or decision-right is missing or ambiguous.
- Operational compliance assesses whether the project team is executing the work in accordance with those established requirements.

To evaluate both design adequacy and operational compliance, auditors should review core project documents, which may include:

- Organization or project charter
- Board approvals and delegated authority records
- Financial approval authorizations
- Corporate policies & procedures
- Project management plans and playbooks
- Contract templates and executed agreements
- Risk register, issue logs, and project controls reports

Turning the tide

As with any audit engagement, it is critical that auditors understand their audience, establish credibility, and clearly communicate the engagement objectives and scope of the review. While construction audits are a foundational component of healthcare system capital programs, construction project teams can still view audit involvement as an administrative disruption to their tight schedules.

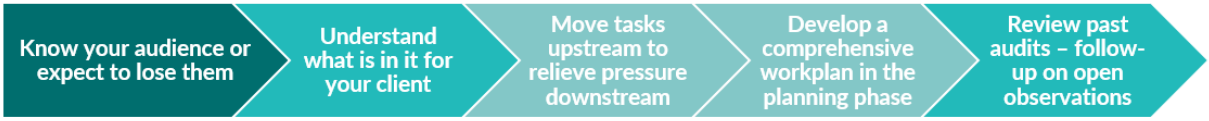
Audit teams can ease this friction by engaging early, clarifying their methodology, and demonstrating how the review actively protects project outcomes and delivery timelines. To maintain trust and maximize project value, healthcare audit functions should focus on an integrated advisory model built around three core pillars:

1. Proactive strategic engagement
    a. Engage early to influence controls and risk allocation parameters before major project spending occurs.
    b. Share the audit methodology with project stakeholders before fieldwork begins to establish clear expectations and buy-in.
    c. Broaden the audit scope beyond simple payment applications to evaluate project managers, architects, construction managers, and key consultants.
2. Technical program immersion
    a. Immerse the audit team deeply into the capital program to thoroughly master the selected project delivery method.
    b. Act as a subject-matter expert and recognize when to engage specialized technical expertise.
    c. Convert abstract open issues into highly structured, documented risks with clear mitigation owners and status tracking.

While no two construction projects are identical, standard audit activities should align with common project execution milestones.

Exhibit 5

TURNING THE TIDE: AUDITING BEST PRACTICES



3. Collaborative transparency
    a. Maintain objective independence while remaining non-adversarial and highly integrated into project workflows.
    b. Build constructive working relationships across facility leadership and external stakeholders using a trust-but-verify mindset.
    c. Extend local recommendations across the organization's entire capital project portfolio to maximize institutional value.

Upon project completion, organizations should convene formal lessons-learned sessions with key stakeholders. These insights should be permanently documented, assigned to operational owners, and embedded directly into future procurement templates, contract governance documents, and project controls procedures.

Indicators of success

The ultimate value of a construction audit function is measured by how effectively it executes the five-step roadmap outlined in Exhibit 5. When an audit team successfully shifts its focus upstream to prevent downstream risk, the metrics for success transform from simple cost-recovery numbers to the following long-term operational improvements:

- Shifting risks upstream: By developing comprehensive workplans during the early planning and design phases, audit findings serve as an early warning system. This prevents systemic scheduling or control errors before they repeat across the portfolio.
- Proactive self-correction: A mature audit presence prompts project owners and contractors to understand what is in it for them. This realization drives teams to actively identify and remediate internal control gaps before a formal audit phase even begins.
- Trusted advisor state: The highest indicator of success occurs when management actively seeks audit input during the initial conceptual stages of a project. Moving outside the rigid boundaries of traditional engagements establishes the audit function as a trusted advisor on capital risk.

Conclusion

Auditing capital projects cannot be reduced to a simple retrospective exercise in identifying baseline control gaps or chasing cost recovery. Instead, a mature audit function serves as a forward-looking mechanism that improves owner and contractor performance, strengthens governance, and systematically prevents project failures. By prioritizing early engagement, mapping risk indicators, and fostering a culture of collaborative transparency, internal auditors do more than protect a budget. They provide health system leaders and stakeholders with the objective assurance that critical investments are being managed efficiently, effectively, and ethically—ultimately ensuring that capital resources successfully transition into vital community healthcare infrastructure. **NP**

Kenneth Brzozowski, CCA, CCP, is the Director of Audit and Advisory Services for Talson Solutions, LLC. He has managed domestic and international construction audits, risk assessments, procedure reviews, and readiness reviews. He sits on the advisory board of the National Association of Construction Auditors (NACA). He can be reached at kbrzozowski@talsonsolutions.com

Mary Jane R. Schroeder, CIA, CRMA, CICA, CHIAP®, is Vice President of Internal Audit for Penn State Health and the former Associate Vice President of Internal Audit for Main Line Health. She is a former board member and chair of the Association of Healthcare Internal Auditors (AHIA). She can be reached at mschroeder3@pennstatehealth.psu.edu

CERTIFICATION

CHIAP
Certified Healthcare Internal Audit Professional®

The CHIAP Certification is the only professional certification unique to healthcare internal auditors. Take the next step in your career by adding this valuable certification to your resume!

Start Your Exam Preparation Today...

Review the complete Body of Knowledge (BOK) outline in the CHIAP Candidate Handbook.

- Test your knowledge with over 50 Sample Exam Questions.
- Watch the 8-part BOK Webinar Series.
- Search for additional resources in the AHIA Virtual Learning Audit Resource Center.
- Visit the AHIA website for more information on Exam Preparation Resources.
- FAQs