25 top management risks for healthcare in 2023

By Scott Gerard, CPA
George Bezzerides, CPA, CIA, CFE
Andrei de Vore, CPA, CCA

In the midst of an inflationary economy made worse by shortages of clinical, IT, and risk professionals, healthcare organizations face tough choices over where to best allocate their financial capital and human resources to mitigate undue risk exposure and enhance their return on risk. A successful decision-making process begins with knowing where risks are hiding, poised to turn a calm day into a crisis with little warning.

Crowe defines a risk area as anything that might impede a healthcare organization's ability to achieve its goals in critical areas such as patient care, regulatory compliance, operations, strategic growth, and financial performance.

To manage an environment of increasing risks and limited resources, healthcare internal audit and compliance departments must align their risk assessments and audit work plans to areas most vital to achieving the strategic goals and business objectives of their organizations. The departments must do so while staying in compliance with critical regulatory and other requirements. This risk-based approach prioritizes areas of highest risk and suggests that providers spend less effort, if any, on low-risk areas.

The better the alignment between the internal audit and compliance plans and the most critical risks to the organization, the greater the return on risk generated for an organization's internal audit and compliance investment.

Crowe identified 25 top management risks facing healthcare organizations in 2023 using input from:

- Executive management and board members at many of the largest U.S. health systems
- Risk assessments conducted by Crowe at hundreds of health systems, hospitals, and other healthcare provider clients during 2022

Every healthcare organization is different. A top risk area for one healthcare organization might not be a risk for another. Crowe did not rank the risks; however, executives and board members alike consistently identified four of the risks – workforce, inflationary economy, cybersecurity, and business continuity management – as the highest risks facing their organizations today.

The 25 top risks fall into six risk areas in alphabetical order:

- Clinical risks
- Emerging risks
- Financial and operational risks
- Legal and regulatory compliance risks
- New regulation risks
- Technology risks

For each top risk area, Crowe identified specific risks, audits that internal audit and compliance teams should consider to mitigate the specific risks, and, in most cases, tips on how technology can be used to assist in those audits.

The report concludes with a breakdown of internal audits by risk area in 2022 and the identification of gaps in internal audit work plans that might put unprepared healthcare organizations at greater risk in 2023.


CLINICAL RISKS
Behavioral health
Patient safety
Opioids
Supply chain
Telemetry monitoring
EMERGING RISKS
Coronavirus Aid, Relief & Economic Security Act
Health equity & social determinants of health
Robotic process automation
FINANCIAL & OPERATIONAL RISKS
Accounts payable processing fraud
Community benefit
Inflationary economy
Drug diversion & 340B
Physician practices
Vendors & business associates
Workforce
Workplace violence
LEGAL & REGULATORY COMPLIANCE RISKS
EMTALA
Social Security Act Section 1135
Telehealth & remote patient monitoring
NEW REGULATION RISKS
Cybersecurity
No Surprises Act
State-regulated data privacy
TECHNOLOGY RISKS
Cybersecurity insurance & ransomware preparedness
IT and operational business continuity management
Post-merger integration of IT systems and data
Are there gaps in your audit plan?

Clinical risks

Behavioral health

Interest in behavioral healthcare has grown tremendously over the past three years with the onset of the COVID-19 pandemic and its devastating impact on the mental health of adults and children alike. Providers also are expanding their behavioral health services as they expand their whole-person approach to patient care in recognition of the inextricable link between mental health and physical health. As part of that whole-person approach, providers are conducting more screenings for behavioral health issues as part of physical health assessments. Behavioral health issues are more nebulous and abstract than physical illnesses or injuries and, therefore, are harder to detect and diagnose until an acute episode flares up.

Behavioral health risks include:

- Inaccurate or unperformed suicide risk and mental health screenings on all patients served resulting in missed diagnoses and/or harm to the patient
- Staff untrained or improperly trained on de-escalation and workplace violence prevention techniques when dealing with aggressive or violent patients resulting in serious harm to staff, harm to patients, and an unsafe work environment
- Improper use of restraints and documentation of the use of restraints and seclusion in an inpatient behavioral health setting resulting in harm to patients, staff, and the organization's reputation and accreditation
- Inadequate ligature risk identification and routine assessments of ligature risks in an emergency department (ED) or inpatient behavioral health setting resulting in patient self-harm
- Limited behavioral health treatment facilities resulting in patients unnecessarily remaining in the ED for extended periods of time going untreated

Audits for consideration to mitigate behavioral health risks

- Patient suicide and mental health screening processes
- Workplace violence prevention and de-escalation education processes
- Restraints and seclusion compliance assessment
- Ligature risk assessment of the inpatient behavior health settings and ED

How audit and compliance professionals can use technology to expand behavioral health risk coverage

- Analyze electronic medical records (EMRs) for populated suicide scale flow sheets and documentation.

Patient safety

An eye-opening study published earlier this year in the New England Journal of Medicine suggests that nearly one in four patients suffers an adverse event after being admitted to the hospital.[1] Previously, in a ground-breaking study, patient safety experts from Johns Hopkins Medicine estimated that medical errors are the third leading cause of death in the U.S., following only heart disease and cancer.[2]

These stark figures exist despite many years of increased regulatory scrutiny, automation, and focus on preventable errors. Medical errors run contrary to the primary objective of hospitals and health systems to improve the patient experience, including quality, safety, and satisfaction. Despite the universality of healing as a health system goal, many hospital and health system internal auditors do not discuss clinical risks during their risk assessment discussions. Therefore, many internal audit functions do not include any clinical audits on their annual audit plans.

Errors that result in patient harm can occur in almost any area of a hospital or health system, from an emergency department visit to discharge and transition to post-acute care.

Some of the most common patient safety risks are:

- Clinicians causing adverse drug effects by administering the wrong medication to the right patient, the wrong dose of medication to the right patient, or the right medication to the wrong patient, all of which can cause patient injury or death
- Missing or incomplete medication histories and reconciliations causing a clinician to administer a drug that's contraindicated
- Clinicians performing the right surgical or other procedure on the wrong patient or the wrong procedure on the right patient, again resulting in patient injury or death
- Not identifying and mitigating the three main components of the fire triangle (fuel source, oxidizer, and ignition source) causing surgical fires in or around the patient
- Caregivers failing to perform a standardized assessment of fall risk factors, so that appropriate precautions are missed, resulting in preventable patient injury from a fall event
- Caregivers failing to implement other risk-reduction strategies such as skin monitoring, improving patient mobility, repositioning patients in bed, and optimizing nutrition, resulting in avoidable hospital-acquired pressure injuries
- Caregivers overlooking or omitting infection prevention precautions, exposing patients or caregivers to a variety of infections, including methicillin-resistant Staphylococcus aureus, catheter-associated urinary tract infections, surgical site infections, ventilator-associated pneumonia, clostridium difficile infections, or sepsis

Audits for consideration to mitigate patient safety risks

- Medication reconciliation/medication administration
- Surgical safety, including retained surgical Instruments and surgical fires
- Device sterilization, device disinfection, sterile processing department, surgical suite disinfection
- Personal protective equipment (PPE) utilization
- Falls, hospital-acquired pressure ulcers
- Healthcare-associated infection

How audit and compliance professionals can use technology to expand patient safety risk coverage

- Perform ongoing analysis of claims data to identify patient safety events for testing.
- Test full populations of established monitoring or control points in medical records to identify gaps.
- Use control assessment tools to quickly identify and summarize the presence or absence of desired clinical interventions across multiple locations.

Pharmaceuticals: Opioids

The ongoing opioid crisis continues to reshape hospitals' opioid stewardship programs. Although opioid prescribing continues a downward trend, opioid overdosing and deaths continue to increase, according to government and industry research. As a result, hospitals must redesign opioid stewardship programs into more multifaceted community collaboration efforts to fight the current opioid crisis. The crisis spans opioid use disorders (OUD), substance abuse disorders (SUD) with or without comorbid mental health illness or disorders, illegal and illicit drug use, and overdoses.

With approximately $50 billion of manufacturer, distributor, and retailer opioid settlement funds already flowing into states, hospitals will see even more focus on opioid abatement remediation strategies. Many of these strategies target prevention, treatment, and services for OUD/SUD patients.

Risks include:

- Noncompliance with regulatory, industry, and evidence-based practices for proper opioid prescribing and OUD/SUD treatment and services resulting in patient harm and patient addiction

Audits for consideration to mitigate opioid prevention, prescribing, and treatment risks

- Assessment of the hospital's opioid stewardship program

How audit and compliance professionals can use technology to expand opioid stewardship risk coverage

- Use data analytics to compare 100% of opioid prescriptions with evidence-based prescribing practices and guidelines.
- Use data analytics to evaluate OUD/SUD patients to determine the extent of early intervention protocols used.

Supply chain

A May 2022 Forbes article, "Supply-Chain Snags Create Shortages of Lifesaving Medical Supplies in U.S.," noted, "The U.S. healthcare system is facing supply shortages that dwarf the problems experienced in the early days of the COVID-19 pandemic . . ." due to "component scarcities, backlogged ports, transportation glitches, and lockdowns in China." The article went on to say that while current supply chain shortages might not be as urgent as they were during the pandemic, they include a much wider array of equipment that ranges from latex and vinyl examination gloves to dialysis-related products and pharmaceuticals.

Further, a February 2023 Becker's Hospital Review article, "Shot-Down Chinese Balloon May Affect US Medical Supply Chain," said after the downing of a "high-altitude object" and confirmation that the object was a Chinese spy balloon, "it's unclear what these actions mean for the U.S.-China medical supply chain."

And a brief in the American Journal of Managed Care cited a report from the Scrip Pharma Intelligence website that said, "FDA inspections of Chinese manufacturing plants were suspended during COVID lockdowns and the political fallout from the balloon incident may delay their resumption, even though China has ended its zero-COVID policy. The United States relies on overseas drug manufacturing, with 18 of 21 vital antibiotics and 72% of its active drug ingredients coming from abroad."

These dynamics are pulling apart the healthcare supply chain and creating specific risks for hospitals and health systems, including:

- Insufficient critical equipment and supplies resulting in potential negative impact to operations and patient care
- Inadequate emergency preparedness or supply chain instability resulting in negative patient outcomes and increased reputational risk
- Bypassing existing procurement processes and controls to obtain critical equipment or materials in short supply resulting in increased risk of overpayment or vendor fraud

Audits for consideration to mitigate supply chain risks

- Supply chain resiliency
- Supplier procurement and diversification program effectiveness
- Supply chain emergency preparedness
- Critical equipment and supplies inventory management

How audit and compliance professionals can use technology to expand supply chain risk coverage

- Analyze critical equipment and supply inventory levels to identify potential high-risk shortages and outages.
- Analyze procurement transactions to identify potential supplier diversification or geographic/geopolitical vulnerability issues.
- Analyze supplier selection data and procurement transactions for indications of potential overpayment or fraud.

Telemetry monitoring

Telemetry monitoring is the use of remote cardiac monitoring devices to detect arrhythmias in patients outside of critical care units. Telemetry monitoring gives providers real-time measurements of monitored physiologic parameters from a distance. Breakdowns in technology and clinical response time increase the risk of patient harm by disrupting or interrupting identification of critical and abnormal changes in a patient's cardiac health. Also, the use of telemetry can lead to alarm fatigue and nonaction, both of which distract from care and jeopardize patient safety.

In 2017, the American Heart Association revised its evidence-based standards to guide providers on appropriate telemetry use based on patient diagnosis. Primary interventions to decrease telemetry use include staff education, developing discontinuation criteria, integrating telemetry orders into daily communications, and hardwiring standards into the organization's ordering practices. Internal audit and compliance professionals can be a valuable resource to provide an independent assessment of the organization's risk mitigation efforts and alignment with industry standards.

Specific risks in this area include:

- Monitoring equipment not connected to patients as ordered by the provider resulting in the wrong patient being connected to a specific telemetry box or a delay in connecting a patient to telemetry
- Communication breakdown between monitor watchers and frontline staff resulting in improper escalation notification
- Lack of vendor support or lack of adequate transmission bandwidth within all areas of facilities resulting in infrastructure breakdowns, equipment malfunctions, and failures of end-of-life systems
- Lack of daily re-assessment of the need for telemetry leading to overuse

Audits for consideration to mitigate telemetry monitoring risks

- Telemetry monitoring – patient safety (clinical- and IT-focused)
- Telemetry utilization assessment

How audit and compliance professionals can use technology to expand telemetry risk coverage

- Use data analytics to analyze trends in telemetry initiation and daily usage by specialty of ordering physician and average duration of telemetry monitoring.

Emerging risks

Coronavirus Aid, Relief, and Economic Security Act

The COVID-19 pandemic brought new challenges for healthcare, but the response of the government with the passage of the *Coronavirus Aid, Relief, and Economic Security* (CARES) *Act* offered some relief. In addition to granting Provider Relief Fund (PRF) payments to healthcare entities, the law allowed employers to defer payment of their share of Social Security tax. The law also expanded COVID-19 Accelerated and Advance Payment (CAAP) funds for Medicare Part A providers and Part B suppliers, which gave certain providers and suppliers more flexibility to extend repayment time frames and receive increased payment amounts. Additionally, the *Continuing Appropriations Act, 2021 and Other Extensions Act* amended the repayment terms for providers and suppliers that requested and received CAAP funds during the COVID-19 public health emergency.

These benefits, though, are not without risk, and businesses that accepted and retained the funds must understand the consequences of noncompliance with the specific eligibility and approved uses of the funding.

Risks associated with the various aspects of the CARES Act include:

- Recipients providing or reporting inaccurate information on PRF payments resulting in payment recovery and other legal action
- Recipients not repaying deferred taxes in a timely manner resulting in penalties
- Recipients not repaying CAAP funds in a timely manner resulting in a demand letter from the Centers for Medicare & Medicaid Services (CMS) requiring payment in full plus interest on the entire amount advanced within 30 days

Audits for consideration to mitigate CARES Act risks

- Compliance with PRF guidance regarding the calculation of lost revenue and claiming of expenses
- Compliance with guidelines of advance payment repayment
- Compliance with repayment of deferred payroll taxes

How audit and compliance professionals can use technology to expand CARES Act risk coverage

- Use data analytics to gather and track expenses for PRF reporting.

Health equity and social determinants of health

CMS defines health equity as the attainment of the highest level of health for all people in which each person has a fair and just opportunity to reach their optimal level of health regardless of race, ethnicity, disability, sexual orientation, gender identity, socioeconomic status, geography, and preferred language. Social determinants of health (SDOH) are the economic and social conditions in which people are born, live, grow, work, and age that can affect access to care and health outcomes.

In CMS' 2022 strategic plan, the agency outlined its efforts to advance health equity by "designing, implementing, and operationalizing policies and programs that support health for all people served by [its] programs." CMS' plan intends to advance health equity by addressing health disparities that underlie the nation's healthcare system through stakeholder engagement and by building health equity into all of the agency's core functions and programs. CMS health insurance programs cover more than 150 million people across the country through Medicare, Medicaid, the Children's Health Insurance Program (CHIP), and *Affordable Care Act* marketplace plans. The programs distribute hundreds of billions of dollars throughout the U.S. healthcare system annually and provide quality oversight of most healthcare facilities, providers, and care settings across the country.

The federal government's aggressive investment of resources into achieving its health equity goals will increase focus on the measurement of such goals, including capturing related data for analysis, monitoring, and auditing. For instance, CMS adopted its first-ever set of SDOH measures to use in the inpatient prospective payment system rules for fiscal year 2023, which took effect Oct. 1, 2022. The measures include access to care, education, neighborhood and physical environment, community and social context, and economic stability. ICD-10-CM diagnosis codes specific to SDOH (Z codes) are available for providers to use in filing inpatient claims for payments.

CMS permits medical and professional coders to code SDOH diagnoses from notes from nurses and other clinicians in addition to a physician's documentation. Accurately and consistently collecting SDOH information becomes increasingly important to healthcare stakeholders as it can have a major impact on the quality of care and health outcomes, including lengthy patient stays, missed appointments, and high readmission rates. Tracking and analyzing this data can assist in enhancing patient care, improving care coordination and discharge planning, and supporting quality measures. Internal audit can provide valuable independent assessments of the organization's health equity efforts and alignment with the government's strategies.

SDOH risks include:

- Lack of strategy and programs in place to integrate health equity into the organization's core functions and existing workflows, leaving the organization unprepared to meet current and future regulatory requirements
- Lack of process, tools, and resources to capture, track, and analyze SDOH data, resulting in poor quality of care and health outcomes and ultimately creating financial risk due to increased cost of care and reduced reimbursement
- Lack of leadership engagement and provider and staff awareness regarding the organization's health equity goals, SDOH documentation, and related regulatory requirements

Audits for consideration to mitigate SDOH risks

- Health equity program assessment
- Evaluation of process for capturing, tracking, and analyzing SDOH Information
- SDOH capture rate analysis
- Review of medical record documentation and SDOH diagnosis coding
- Case management and discharge planning

How audit and compliance professionals can use technology to expand SDOH risk coverage

- Analyze claims data to determine SDOH capture rates and what SDOH elements are captured or not captured.

Increased use of robotic process automation

The field of robotic process automation (RPA) has advanced with such speed that it can be difficult to decipher what it means to an organization and the new risks introduced. RPA can offer several benefits, including enhanced efficiencies, decreased risk of human error, lower costs, and the opportunity to empower employees to engage in higher-level tasks that make the overall workplace better. As healthcare organizations design and implement more robotic processing systems (bots), internal audit and compliance leadership must consider the related risks and competencies necessary to assess RPA processes and controls.

To address the risks related to RPA, chief audit and compliance executives need to first determine if their health systems are using RPA, how many bots are deployed across the organization, and where those bots are used. The internal audit team should include these bots as part of the risk assessment process and internal audit plan. Due to limited understanding of RPA or a lack of competencies to audit bots, some audit functions audit processes up until the robotic processing occurs and then skip past the RPA to the end of the process. Internal audit leaders should make sure that if a process is deemed critical and selected for audit, the entire process is audited from end to end, including those portions that are conducted by bots.

Risks related to RPA include:

- Not appropriately testing the robotic processing system before moving into production
- Unauthorized or untested changes to the bot resulting in negative impacts to information confidentiality, integrity, and availability
- Not including RPA processes as part of the business continuity plan

Audits for consideration to mitigate RPA risks

- RPA development and testing
- RPA governance policy and processes
- Access to RPA programming and data

How audit and compliance professionals can use technology to expand RPA risk coverage

- Conduct continuous controls monitoring of processes that use RPA technology.

Financial and operational risks

Accounts payable processing fraud

Key business processes such as accounts payable (AP) are critical to every healthcare organization. While these processes are highly visible and typically well-managed, when significant changes occur within the AP process (for example, leadership or employee turnover or cutbacks) or within the overall organization (for example, changes in operating procedures due to a pandemic, implementation of a new enterprise resource planning system, or organizational consolidation or centralization post-merger), fraud risks might increase due to changes in people, processes, or technology, or suspension or elimination of key internal controls.

Specific risks include:

- Fraudulent or unauthorized payments to existing vendors or employees
- Creation of, and payment to, fictitious vendors
- Inappropriate or unauthorized updates to vendor master data, causing payments to be diverted from the correct vendor

Audits for consideration to mitigate AP processing fraud risks

- Procure-to-pay process audit
- AP and vendor master file system access and general IT controls audit
- Vendor master file change process
- Corporate purchase card audit

How audit and compliance professionals can use technology to expand AP processing fraud risk coverage

- Analyze AP transactions to identify fraudulent payments to employees.
- Analyze payments made to the same bank account for multiple vendors.
- Analyze vendor payments that lack an associated purchase order.
- Analyze vendor payments issued for amounts just under standard approval levels.
- Analyze instances in which vendors were added and removed from the vendor master file immediately before and after payments were made.
- Analyze corporate purchase card transactions for nonbusiness uses.

Community benefit

Due to increased scrutiny of not-for-profit healthcare organizations, proving that hospitals are deserving of their tax-exempt status is more important than ever. Not-for-profit hospitals are required to demonstrate community benefit in many ways, including meeting the "community benefit standard" under IRS Revenue Ruling 69-545 and meeting certain requirements under Section 501(r) of the *Affordable Care Act*. But those are simply baseline requirements for not-for-profit hospitals. The real focus is how much they are doing in addition to those baseline requirements.

Unflattering media reports and congressional inquiries of how much community benefit and charity care hospitals provide in exchange for their preferential tax treatment are putting pressure on not-for-profit hospitals to differentiate themselves from their for-profit counterparts.

Risks associated with incomplete and inaccurate community benefit reporting include:

- Public scrutiny
- Inquiries from state charity officials and other local officials
- Challenges to property tax exemption, sales tax exemption, and possibly income tax exemption

Audits for consideration to mitigate community benefit reporting risks

- Community benefit calculation accuracy
- Community benefit reporting with a focus on unreported or underreported community benefit activities
- Community benefit policy and procedures review
- Review of environmental, social, and governance reporting that might incorporate community benefit

Inflationary economy

"Everything Everywhere All at Once" won the 2022 Oscar for best picture. The movie wasn't about myriad challenges facing hospitals and health systems, but it could have been. Challenges such as labor shortages, wage pressures, declining operating margins, new COVID-19 surges, runaway expenses, rising interest rates, bank failures, investment losses, and more continually buffeted hospitals and health systems from all sides in 2022 and during the first quarter of 2023.

As patient volume slowly returns to pre-COVID rates and state and federal COVID relief funds end, rising inflation presents an additional hurdle to providers' financial health. Entering 2023, hospital and health system management and governance need a full range of resources to counter the ongoing barrage of operating and financial headwinds.

An inflationary economy presents healthcare organizations with specific financial risks, including:

- Deteriorating liquidity metrics leading to credit downgrades
- Uncertain investment returns contributing to deteriorating liquidity
- Slow and unpredictable patient volume recovery
- Intractable labor issues and wage pressures
- Rising supply, pharmaceutical, and equipment costs

To combat the inflationary economy and strengthen operations, healthcare leaders are using some of the following resources and tactics with a focus on performance and margin enhancement:

- Increasing clinical operation efficiencies
  - Clinical excellence and value-based payments
  - Clinical efficiencies and outcomes
- Improving revenue cycle management performance
  - Billing and collections
  - Charge capture and clinical documentation improvement
- Increased digital transformation and creating value
  - Labor efficiencies
  - Increased risk coverage at lower cost
  - Identifying cost saving opportunities

Audits for consideration to mitigate inflationary economy risks

- Denials management
- Revenue charge capture
- Procurement (with focus on spend)
- Timekeeping and payroll (with focus on overtime and premium pay)

How audit and compliance professionals can use technology to expand inflationary economy risk coverage

- Use data from organizations' enterprise resource planning, EMRs, payroll, and other systems to design and roll out automated digital transformation to provide continuous auditing of accounts payable, payroll, general ledger, and supply chain risk areas, which can help reduce risk and identify revenue enhancement and cost saving opportunities.

Pharmaceuticals: Drug diversion and 340B

Drug Enforcement Agency (DEA) regulations can be complex and difficult to understand, and citations involving these regulations can lead to multimillion-dollar settlements for organizations. A DEA audit or inspection also can lead to criminal prosecution and administrative action against a DEA registrant if the agency finds violations of the *Controlled Substances Act*.

The dispute between safety net hospitals and drug manufacturers over new price limitations by manufacturers on hospitals' use of the federal 340B Drug Pricing Program is heading into a new phase of legal battles that ensures this fight will remain a dominant issue in the 340B arena for months to come. Furthermore, hospitals' lack of compliance with 340B Program regulations might result in repayment to drug manufacturers or removal from the program. Also, rapidly rising costs along the pharmaceutical supply chain combined with the complexities of accurately capturing medication charges can contribute to a reduction in revenue and additional compliance risks.

Specific risks for hospitals and health systems include:

- Removal from the 340B Program due to lack of compliance
- DEA monetary penalties and/or criminal prosecution
- Loss of pharmacy revenue
- Patient harm/addiction

Audits for consideration to mitigate drug diversion and 340B Program risks

- 340B Program compliance assessment
- Drug diversion monitoring controls assessment
- Medication billing assessment

How audit and compliance professionals can use technology to expand drug diversion and 340B Program risk coverage

- Test 100% of critical data elements related to 340B Program compliance.
- Test 100% of critical data elements related to drug diversion monitoring controls.
- Test 100% of medication charges to confirm drugs administered and wasted are accurately billed.

Physician practices

Physician practices provide continuing care in the community and are the primary entry and exit points for many health systems. Although acute care facilities are highly regulated and frequently audited, ambulatory care settings, where processes are often manual, face less regulatory oversight of the operations and processes. In acquired physician practices, medical groups, and ambulatory clinics, lack of staff training, staff turnover, temporary staff, staff shortages, and time pressures can easily derail high-touch processes and can introduce additional unknown risks to a hospital or health system acquirer. Hospitals and health systems must establish "closed loop" processes and workflows to prevent patient harm, avoid liability, and improve quality.

Risks related to physician practices include:

- Missed referrals (for example, to cardiology), resulting in avoidable patient injury or death
- Lost screening results leading to a failure to diagnose or a misdiagnosis of a disease like cancer in time to initiate optimal treatment
- Missing or poorly performed medication reconciliation leading to clinicians concurrently prescribing contraindicated medications
- Unidentified temperature variations within a refrigerator resulting in the need to revaccinate patients and increased risk of reputational damage and legal liability
- Failure by hospitals or health systems to notify primary care physicians of patient admissions, discharges, or transfers resulting in gaps in care

Audits for consideration to mitigate physician practice risks

- New acquisition or pre-acquisition clinical practice assessment
- Diagnostic test and referral management
- Medication management (physical controls and reconciliation)
- Device disinfection (sterilization and/or high-level disinfection)

How audit and compliance professionals can use technology to expand physician practice risk coverage

- Identify diagnostic tests or specialist referrals ordered but not completed.
- Analyze medication reconciliation frequency and completion.

Vendors and business associates

Hospitals and health systems increasingly rely on third-party vendors in a variety of clinical, financial, and operational areas to augment staffing levels and achieve cost savings and increased efficiency. As technology has become increasingly critical to healthcare operations, vendors often require access to key information technology systems and networks. Sophisticated cybercriminal attacks are becoming more frequent, with many ransomware and cyberattacks targeting vendors and vendor systems as an entry point into a provider organization's IT systems.

Strong contracting and oversight processes for these significant vendor relationships are critical for provider organizations to achieve their business goals and objectives. When an essential vendor fails to perform as expected, operational, financial, compliance, and reputational risks can ripple across the entire enterprise.

Common risks associated with vendor relationships include:

- Inadequate vendor screening and selection procedures
- Overcharging or billing for services not provided
- Failure to meet service, performance, or financial terms in accordance with contract requirements
- Failure to comply with facility policies and standards, resulting in compliance and reputational risks
- Weak privacy and IT security controls for vendors that have access to hospitals' IT systems and data

Audits to consider for mitigating vendor and business associate risks

- Vendor selection and contracting
- Vendor onboarding, management, and monitoring
- Vendor HIPAA privacy and IT risk assessment
- Business continuity planning with focus on critical vendor services

How audit and compliance professionals can use technology to expand vendor and business associate risk coverage

- Analyze the vendor master file to identify duplicate and incorrect entries.
- Analyze accounts payable transactions to identify duplicate and inaccurate payments to vendors as well as vendor payments that could represent conflicts of interest, particularly for physicians (for example, lack of compliance with the *Sunshine Act*).
- Analyze vendors' access to systems to identify excess or inappropriate access.

Workforce

Hospital CEOs' top concern in 2022 was workforce challenges, according to the 2022 survey of hospital CEO challenges conducted by the American College of Healthcare Executives (ACHE).[3] It was the second consecutive year that workforce challenges ranked No. 1 on ACHE's annual list of hospital CEO worries.

"Hospitals need to take both long- and short-term measures to address critical workforce issues so they can continue to provide safe, high-quality care now and in the future," said Deborah Bowen, ACHE president and CEO, in a statement accompanying the ranking.

The workforce challenges that healthcare organizations face include recruiting, hiring, and retaining qualified employees as demand for healthcare services increases due to the aging U.S. population and the competition for healthcare workers intensifies. Workers leaving the healthcare sector due to pandemic-related burnout and accelerated retirements have only exacerbated the challenge over the past three years.

One way healthcare organizations have responded is through increased reliance on travel nurses. Some formed their own travel nurse programs in an attempt to limit related costs. Others offered increased benefits or incentives to retain workers. Some of those that couldn't respond with creative solutions reduced or eliminated services or service lines at select sites of care.

The situation has created a number of specific risks that hospitals and health systems historically have not had to deal with before at such scale.

Those risks include:

- Decreased quality and safety of patient care and clinical outcomes, leading to higher readmission rates, higher hospital-acquired infection rates, and higher mortality rates
- Lower quality scores leading to lower reimbursement rates
- Higher labor costs attributable to higher salary and benefit expenses and travel nurse program expenses resulting in impaired financial performance
- Increased difficulty in filling openings in the executive ranks, especially in organizations where the approach to succession planning (that is, identifying and mentoring successors) has not been formalized or well-established

Audits for consideration to mitigate workforce risks

- Travel nurse management and contract compliance
- Critical department staffing levels
- Recruiting and retention processes
- Succession planning
- Premium employee pay levels

How audit and compliance professionals can use technology to expand workforce risk coverage

- Analyze travel nurse timekeeping and billing data to assess propriety of agency billings.
- Use data analytics to identify patient readmissions and assess for staffing-related root cause(s).
- Analyze employee retention expenses and turnover data to assess effectiveness of retention programs.

Workplace violence

Seventy-three percent of healthcare workers in critical care settings around the world said they experienced workplace violence over the past year, according to the Violence Study of Healthcare Workers and Systems survey conducted by researchers with Global Remote Research Scholars Program.[4] The researchers conducted the survey in 2022 and released the results in January 2023.

The Joint Commission's new workplace violence prevention accreditation standards for hospitals took effect in January 2022.[5] The standards require hospitals to manage worker safety and security risks, collect information to monitor security incidents, participate in workplace violence prevention education and training, and develop and enforce workplace violence prevention programs.

More recently, ECRI named "physical and verbal violence against healthcare staff" as one of its top 10 patient safety concerns for 2023.[6]

Specific workplace violence risks include:

- Failure to comply with standards of The Joint Commission and other regulatory agencies related to prevention of workplace violence
- Failure to monitor security personnel and outsourced security vendors
- Adverse financial impact and lower quality resulting from employee turnover
- Harm to patients and healthcare provider team members

Audits for consideration to mitigate healthcare workplace violence risks

- Regulatory readiness, including compliance with Joint Commission standards
- Prevention of patient/visitor/family violence to staff audit
- Security event response assessment

How audit and compliance professionals can use technology to expand healthcare workplace violence risk coverage

- Evaluate reporting of violence resulting in staff harm.
- Analyze response time to events based on policy or service agreements with security vendors.
- Evaluate most frequent types of violent events and sources of violence threats.

Legal and regulatory compliance risks

Emergency Medical Treatment and Labor Act

Congress enacted the *Emergency Medical Treatment and Labor Act* (EMTALA) in 1986 to ensure patient access to emergency medical care and prevent the transfer of patients for financial reasons without consideration of their medical condition or stability for the transfer. Emergency care includes medical screening, examination, stabilizing treatment, and transfer, irrespective of any state laws or mandates that apply to specific procedures.

EMTALA-related risks include:

- Employees who are unaware of EMTALA and its requirements due to significant staff turnover
- Uncertainty regarding whether state law or EMTALA applies
- Penalties for noncompliance with EMTALA regulations

Audits for consideration to mitigate EMTALA risks

- Compliance with EMTALA guidelines within the emergency department
- Compliance with EMTALA guidelines for patients presenting outside the emergency department
- EMTALA transfer and receiving processes (anti-dumping)

Social Security Act Section 1135

Healthcare organizations must reassess compliance in areas where the federal government gave them legal waivers and regulatory flexibilities under Section 1135 of the *Social Security Act*. The expiration of these waivers and flexibilities ranges from immediate termination to up to five months after the COVID-19 public health emergency (PHE) ends. Healthcare providers must prioritize compliance with these expirations to avoid penalties. Understanding which waivers and flexibilities the organization used will be a starting point for the reassessment of compliance post-PHE. Given the high employee turnover that healthcare organizations experienced during the pandemic, the reassessment must include an analysis of current practices, updates to policies and procedures as needed, education and training of professionals on post-PHE policies, and audits to validate compliance and assess any gaps.

Risks associated with *Social Security Act* Section 1135 include:

- Continuing to operate under waivers after the expiration date, resulting in an increased risk of failing to meet compliance, billing, and reimbursement requirements
- Civil monetary penalties and possible exclusion from the Medicare and Medicaid programs

Audits for consideration to mitigate *Social Security Act* Section 1135 risks

- Post-PHE waiver compliance
- Physician contract and payment compliance
- Coding and billing audits
- HIPAA compliance
- EMTALA compliance

How audit and compliance professionals can use technology to expand *Social Security Act* Section 1135 risk coverage

- Analyze and test COVID-19-related diagnosis codes to validate appropriate coding post-PHE.
- Use data analytics to test billing practices post-PHE.
- Analyze calculation of incentive compensation payments.

Telehealth and remote patient monitoring

Telehealth is patient use of digital information and communication technologies to access healthcare services electronically instead of in person. Remote patient monitoring technologies allow a provider to monitor a patient's health electronically instead of in person. These might include:

- Web-based or mobile apps for uploading patient data such as food logs and blood sugar levels for patients with diabetes
- Devices that measure and wirelessly send data such as blood pressure and oxygen levels
- Wearable devices that automatically record and send data such as heart rate, tremors, physical activity, and sleep
- Home devices for seniors or people with dementia to prevent falls
- Devices that send notifications to remind patients to exercise or take medications

The significant increase in care delivery via telehealth touches a range of federal laws, which include anti-kickback statutes, the *False Claims Act*, and HIPAA. Although federal telehealth waivers and flexibilities are slowing, with most ending with the end of the COVID-19 PHE, Department of Justice (DOJ) and Department of Health and Human Services (HHS) guidance and enforcement activities associated with telehealth services are increasing.

HHS' Office of Inspector General (OIG) published a report in September 2022 that summarized findings of the agency's study of how providers bill Medicare for telehealth services provided to beneficiaries. OIG said it identified "concerning billing" that indicated fraud, waste, or abuse in how providers charge Medicare. As a result, OIG said the CMS should strengthen its monitoring and conduct targeted oversight of telehealth services. Internal audit and compliance can be a valuable resource in providing an independent assessment of a provider organization's compliance with telehealth regulatory billing requirements as well as the security of its telehealth platform.

In addition to the compliance-related risks surrounding telehealth, it is important for healthcare provider organizations to understand and assess potential impact related to how current and future industry disruptors are using telehealth to better position themselves over traditional means of delivering health services.

Specific risks in this area include:

- Improper credentialing for telehealth providers
- Poor service quality due to technology malfunctions or unavailability
- Cyberattacks on telemedicine technology resulting in system failure or disruption
- Breached patient confidentiality and privacy
- Improper coding and patient billing for telemedicine encounters
- Loss of patient volume to industry disruptors

Audits for consideration to mitigate telehealth and remote patient monitoring risks

- Compliance with documentation and billing requirements for telehealth services
- IT assessment of telehealth platform and devices
- Cybersecurity assessment of network and unified communication supporting telehealth

How audit and compliance professionals can use technology to expand telehealth and remote patient monitoring risk coverage

- Use data analytics to identify providers with the highest volume of telehealth services and analyze trends to identify potential indicators of billing fraud, waste, or abuse.

New regulation risks

Cybersecurity

As evidenced by the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA), which directly affects the healthcare and public health sectors, federal legislators and regulators as well as healthcare leaders are continually addressing cybersecurity and privacy challenges. Because of the collective high interest by these stakeholders, it's likely that the cybersecurity requirements for HIPAA-covered entities will be strengthened in the next few years. The primary change likely will come in the form of updated attestation methods from a check-the-box model currently in place to a provide-proof-and-be-graded model much like the model introduced by the Department of Defense, the Cybersecurity Maturity Model Certification (CMMC).

Risks faced by healthcare organizations in this space include:

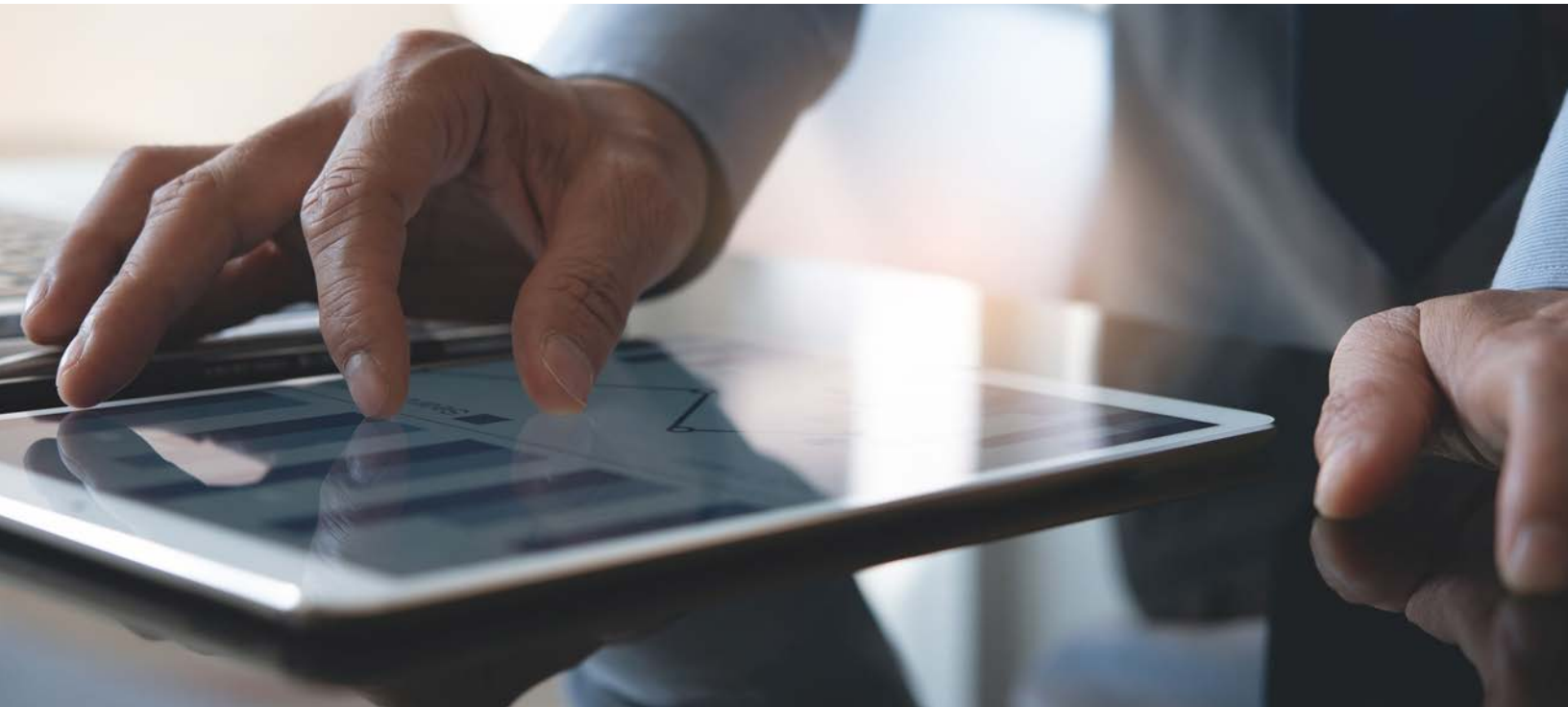
- Inability to react quickly to the accelerating change in government cybersecurity policies and regulations

Audits for consideration to mitigate cybersecurity policy and regulatory compliance risks

- HIPAA security and privacy assessments
- National Institute of Standards and Technology (NIST) cybersecurity assessment
- CMMC precertification readiness assessment

How audit and compliance professionals can use technology to expand cybersecurity risk coverage

- Use a cyber tool stress test (for example, Department of Defense-class IT tool testing) to identify gaps in the use of cyber and IT risk management tools.



No Surprises Act

A year into the enactment of the federal *No Surprises Act* (NSA), which generally prohibits the practice of balance billing patients, CMS extended the period of enforcement discretion for billing challenges in which good faith estimates (GFEs) don't include expected charges from co-providers or co-facilities. Also, due to concerns about the burden of implementing advanced explanations of benefits (EOBs) for patients with commercial insurance, facilities and providers must share a GFE with the payor, and the payor must include the GFE in an advanced EOB sent to the patient. CMS temporarily deferred enforcement of this portion of the NSA as well. CMS has begun to audit providers and payors for noncompliance with all other requirements that went into effect on Jan. 1, 2022.

Risks associated with the NSA include:

- Civil monetary penalties for each violation in which a patient receives a surprise medical bill
- Negative reputational risks resulting in lost revenue for facilities and providers

Audits for consideration to mitigate NSA risks

- NSA process effectiveness
- NSA compliance

How audit and compliance professionals can use technology to expand NSA risk coverage

- Use data analytics to analyze whether actual billed charges are within $400 of the GFE.
- Analyze compliance with GFE timing requirements.
- Use data analytics to identify potential balance billing exceptions.

State-regulated data privacy

Five states – California, Colorado, Connecticut, Utah, and Virginia – passed new privacy laws that go into effect in 2023 to increase protection of consumers' personal data. In addition, eight other states are either holding hearings on privacy bills or planning to introduce privacy bills this year. The objective of the new state laws is to regulate the collection, use, and sharing of personal information. Though healthcare organizations as covered entities or business associates already are required to comply with HIPAA, the new state privacy law requirements might apply as well. In states that have passed new privacy laws, the statutes typically give enforcement authority to a state agency like the state attorney general.

Risks associated with new state privacy laws include:

- Financial penalties and negative reputational risk stemming from how healthcare organizations use consumers' personal data
- Failure by healthcare organizations to fully de-identify consumers' personal information

Audits for consideration to mitigate the risks associated with new state privacy laws

- Data governance assessment
- Data privacy compliance

Technology risks

Cybersecurity insurance and ransomware preparedness

In 2021, businesses in many industries, including healthcare, found it increasingly difficult to obtain cybersecurity insurance, according to a number of reports, including one from the U.S. Government Accountability Office.[7] Such reports also said brokers and carriers were actuarily analyzing individual policy applications and raising premiums for coverage as much as 20% per quarter.

The acceleration in the difficulty of obtaining cybersecurity insurance has slowed. However, as a result, it is still more costly for hospitals and health systems to obtain a cyber policy in 2023 than it was in previous years.[8] This is due to the steep rise in cybersecurity criminal activity and the targeting of hospitals and other providers, frequently via ransomware. Healthcare organizations with demonstrably stronger cyber controls than their peers are having an easier time obtaining cyber insurance and seeing their premiums rise less dramatically. See additional information under the section on risks related to IT and operational business continuity management.

Specific risks in this area are:

- Inability to obtain cyber insurance
- Financial impact of rising cyber insurance costs
- Financial impact of a mass IT outage without cyber insurance or with only limited coverage

Audits for consideration to mitigate cybersecurity insurance risks

- HIPAA assessment (frequently required to apply for cyber insurance coverage)
- NIST control assessment
- Ransomware and phishing awareness

How audit and compliance professionals can use technology to expand cybersecurity and ransomware risk coverage

- Use a cyber tool stress test (for example, Department of Defense-class IT tool testing) to identify gaps in the environment's ability to manage known and unknown threats.

IT and operational business continuity management

Although cyberattacks and ransomware events aren't the only ways to hamper or shut down clinical operations (consider employee strikes and natural disasters), recent attacks have served to highlight the importance of an organization's ability to become operational after a full or partial IT shutdown. Being ready to respond to such an emergency and continue to care for patients and communities is one of the most significant risks facing healthcare providers.

Ransomware risk will continue to increase as healthcare organizations become more dependent on IT to run and support most of its operational, clinical, and financial processes and as IT complexity accelerates each year.

Being prepared for extended downtime and understanding the organization's plan to recover from a ransomware attack are becoming foundational to business operations.

Specific risks include:

- Inability to react to a limited or full IT system outage
- Inability to react to a local or regional natural or manufactured disaster
- Inability to return to normal clinical and business operations after a ransomware attack
- Degraded business operations, reputation, and cash flow due to a ransomware or disaster event
- Legal action from affected parties

Audits for consideration to mitigate IT and operational business continuity risks

- Business continuity plan assessment
- IT backup and recovery audit
- Tabletop IT and business continuity audit
- Ransomware and phishing awareness to expand risk coverage

Post-merger integration of IT systems and data

Mergers and acquisitions continue to be a strategic reality for healthcare provider organizations. The process of integrating the merged or acquired organization carries several inherent risks, perhaps none as large as those presented by the integration of disparate IT environments.

Common IT system integration risks that require leadership attention include:

- Mistakes in consolidating patient demographic and clinical information leading directly to exposing data to inappropriate access, lost data, and patient safety events
- Failing to consider all aspects of decades-old legacy IT environments when integrating disparate applications and systems
- Failing to use detailed planning and thorough efforts and care to reduce cyber risk in the integration of two or more cybersecurity environments resulting in introduction of new cybersecurity risks.
- Inability to implement an intra-organization integration plan in a timely manner resulting in falling short of objectives of the merger
- Unavailable IT and cybersecurity expertise and resources needed for infrastructure integration resulting in a lack of support to maintain an excessive number of applications and systems post-integration

Audits for consideration to mitigate risks associated with post-merger integration of IT systems and data

- Data integration project management audit
- Data integration testing audit
- Cybersecurity program assessment
- IT integration project audit

How audit and compliance professionals can use technology to expand post-merger integration of IT systems and data risk coverage

- Conduct cyber tool stress testing (for example, Department of Defense-class IT tool testing) to identify gaps in the environment's ability to manage known and unknown threats in both environments and identify variances between acquirer and acquired organizations.

How audit plans compare

To help healthcare internal audit and compliance leadership prepare for risk assessment meetings and discuss with governance how their annual work plans compare to others across the industry, Crowe analyzed audit projects conducted during 2022 by the hundreds of professionals in the Crowe Audivate® user community.

Audit coverage by risk area 2022

Compliance – 32.4% of total audits. Audits conducted within this risk category related to:

- 340B Drug Pricing Program compliance
- Clinical documentation improvement
- Clinical research
- Coding and billing compliance
- Compliance program effectiveness
- *No Surprises Act*
- Physician compensation
- Physician contracting
- Two-midnight rule

Quality, patient safety, and clinical operations – 15.1% of total audits. This category included audits related to:

- Behavioral health
- Hospital-acquired conditions
- Infection prevention
- Patient experience
- Patient handoff
- Patient safety (including surgery safety and PPE)
- Sterile processing
- Telemedicine

Finance and accounting – 12.1% of total audits. This risk category contained audits related primarily to:

- 501(r) compliance
- Accounts payable
- Accounts receivable and accounts receivable valuation
- Charge capture
- Federal grants and funding, with the CARES Act assessments representing the largest percentage
- Financial close and financial reporting processes

Revenue cycle – 11.2% of total audits. This category contained audits related to:

- Charge description master
- Advance Beneficiary Notice of Noncoverage (ABN)
- Billing and claims submission
- Charity care
- Denials management
- Price transparency

Information technology – 7.2% of total audits. These audits included:

- Minimal audits for IT disaster recovery
- Biomedical device security
- Cybersecurity assessment
- Data backup and recovery
- End point encryption
- Incident response
- IT governance and telemedicine technology (privacy and security)
- IT vendor oversight
- System and security post-merger integration
- System pre- and post-implementation
- User access

Supply chain and materials management – 6.4% of total audits. Audits in this risk category related to purchasing agreements, vendor selection, medical device credits, and access to PPE supplies.

Human resources – 3.7% of total audits. These audits were related mostly to payroll and timekeeping, with a limited number of audits associated with recruiting and retention.

Pharmacy – 3.6% of total audits. This risk category contained audits related primarily to controlled substances drug diversion, with a limited number of opioid stewardship audits.

Business continuity, ransomware readiness, and disaster preparedness – 2.3% of total audits.

Health system joint ventures – 1.2% of total audits.

Physician practices – 1.2% of total audits. This category included audits related to physician office coding and billing, charge capture, and limited coverage of risks related to physician credentialing and physician office clinical risk management.

“Other” audit topics accounted for the 3.7% of the remaining responses with no area representing more than 1%.

Use of data analytics to expand risk coverage

As data becomes increasingly accessible throughout the healthcare industry, it is more important than ever for internal auditors and compliance professionals to show the return on investment they bring to their organizations. Making the case to management about the importance of investing in technologies such as data analytics is a vital component of demonstrating such value.

Of the audits conducted in 2022 by members of the Audivate community, 29% of the audit projects used data analytics to enhance risk coverage, and 71% of the audits did not use data. Of those that did use data, about half used spreadsheet software to perform the analytics and half used other tools and technologies.

For those that are not currently using data analytics to make their audits more efficient, technology can help to greatly expand risk coverage.

In addition, whether due to retirements, pandemic-related burnout, employees exiting the healthcare industry, or tighter financial budgets, hospitals are challenged to hire and retain experienced accounting professionals. Although risks within financial processes have existed for decades, lack of experienced staff has increased this risk area and can negatively affect key financial controls resulting in:

- Audit adjustments
- Out-of-period corrections
- Restated financial statements
- Losses through inappropriate vendor or employee behavior
- Lost savings in the supply chain
- Conflicts of interest related to physician-led purchasing decisions

With the existence of monitoring technology that enables continuous controls, internal audit and compliance professionals can now expand financial risk coverage and deliver enhanced value to their organization by:

- Focusing more time on conducting root cause analyses
- Testing 100% of transactional financial processes
- Identifying cost savings
- Allowing the technology tools to identify outlier transactions that could indicate:
  - Ineffective controls
  - Inaccurate payroll calculations
  - Timekeeping deviations
  - Compliance issues
  - Potential fraud

Is there a gap in your work plan?

In 2008, Berwick and Associates[9] described what is now a widely accepted triple aim in improving the U.S. healthcare system through the simultaneous pursuit of three goals: improving the experience of care, improving the health of populations, and reducing per capita costs of healthcare. This was expanded in 2014 to a quadruple aim with the addition of clinician well-being and in 2022 to a quintuple aim with the addition of health equity.

However, despite this clear strategic direction, the analysis of healthcare audit projects conducted during 2022 suggests that healthcare work plans have not shifted to recognize this industry change. According to discussions with compliance and internal audit executives, one reason why audit plans contain gaps is because audit and compliance teams are not including some key risk areas during their risk assessment discussions. Therefore, those key risk areas are not identified as top risks and consequently not included in organizations' annual audit and compliance work plans. Given the quintuple framework, these are several of the risk areas that appear to be underrepresented on work plans:

- Patient safety-related audits of acute care clinical areas, physician practice patient care assessments, and behavioral health initiatives are frequently absent from health system work plans. Despite being tied to two-thirds of the original triple aim, clinical audits accounted for only 10% of audit projects in the Crowe analysis.
- Discussions about health equity and social determinants of health are more prevalent than actual audits of these areas. Many health systems are in only the initial stages of implementing their health equity strategy. However, it is not too early to audit the direction and achievement of measurable milestones.
- Provider burnout threatens the sustainability of all other aims, as does verbal and physical violence against healthcare workers. However, current audit and compliance work plans are far more likely to focus on the cost of hiring travelers than on workforce strategies to recruit, retain, and protect existing staff.
- While cybersecurity is as prevalent in audit plans as it is in news headlines – many information security professionals warn "it's a matter of if, not when" – few health systems are auditing their organization's business continuity management program. Audits within this risk area would provide management and governance with assurance that the organization can keep serving patients during a natural or manufactured disaster or in the event of a two-hour, two-day, or even two-month system outage.

Next steps for achieving return on risk

Today more than ever, healthcare organizations' resources are limited even as the number and significance of potential risks grow. Taking these steps can help organizations make sure internal audit and compliance functions are aligned with the most significant risks they face, are achieving greater risk coverage, and are using data analytics to enhance efficiencies and achieve a better return on risk:

- Review the top risks as part of preparing for annual risk assessment interviews and the work plan development process.
- For those that are not currently using data analytics, ensure teams are using data and technology for each project in the annual work plan to enhance the risk assessment process, increase efficiencies, and expand risk coverage. Consider how technology and analytics can be used, including the implementation of monitoring technology that enables continuous controls.
- Once the annual work plan is developed, compare it to the top risks and the most common audit projects conducted by those within the Crowe Audivate user community. Determine whether variances are justified for the organization or if there is a gap in the work plan.
- Continually align and reallocate limited resources to the healthcare organization's top management risks as well as the industry's top and emerging risks to deliver the greatest return on risk.

Crowe provides both proprietary technology and deep industry experience to more than 1,000 healthcare organizations to address these top risks and many others.

Please contact us today to set up an appointment to discuss how our team can use our technology, deep expertise, and experienced resources to support your organization's work plan.

Learn more

Scott Gerard
Partner, Healthcare Consulting
+1 818 325 8457
scott.gerard@crowehrc.com

George Bezzerides
Senior Manager, Healthcare Consulting
+1 916 266 9592
george.bezzerides@crowehrc.com

[1] David Bates, David Levine, Hojjat Salmasian, et al., "The Safety of Inpatient Health Care," New England Journal of Medicine, Jan. 12, 2023, https://www.nejm.org/doi/full/10.1056/NEJMsa2206117

[2] Martin Makary and Michael Daniel, "Medical Error – the Third Leading Cause of Death in the US," BMJ, May 3, 2016, https://www.bmj.com/content/353/bmj.i2139

[3] "Survey: Workforce Challenges Cited by CEOs as Top Issue Confronting Hospitals in 2022," American College of Healthcare Executives news release, Feb. 13, 2023, https://www.ache.org/about-ache/news-and-awards/news-releases/survey-workforce-challenges-cited-by-ceos-as-top-issue-confronting-hospitals-in-2022

[4] "Most Critical Care Workers Experience On-the-Job Violence," Society of Critical Care Medicine news release, Jan. 21, 2023, https://sccm.org/sccm/media/PDFs/Global-Survey-Impact-Violence-Against-Healthcare-Workers-CC-News-Release-Final.pdf

[5] "Workplace Violence Prevention Standards," R3 Report, The Joint Commission, June 18, 2021, https://www.jointcommission.org/standards/r3-report/r3-report-issue-30-workplace-violence-prevention-standards

[6] "Top 10 Patient Safety Concerns 2023," ECRI, https://www.ecri.org/top-10-patient-safety-concerns-2023-special-report

[7] "Rising Cyberthreats Increase Cyber Insurance Premiums While Reducing Availability," U.S. Government Accountability Office, July 19, 2022, https://www.gao.gov/blog/rising-cyberthreats-increase-cyber-insurance-premiums-while-reducing-availability

[8] Tina Reed, "As Cyber Attacks on Healthcare Soar, so Does the Cost of Cyber Insurance," Axios, March 6, 2023. https://www.axios.com/2023/03/06/cyber-attacks-cost-of-cyber-insurance

[9] Donald Berwick, Thomas Nolan, and John Whittington, "The Triple Aim: Care, Health, and Cost," Health Affairs, May-June 2008, https://pubmed.ncbi.nlm.nih.gov/18474969/

crowe.com

CHC2402-001B