protiviti®

Face the Future with Confidence

Adjusting Internal Audit Priorities in Healthcare Organizations

Pre-COVID-19 Survey Results and Current Audit Planning Considerations

Internal Audit, Risk, Business & Technology Consulting

Next-Generation Internal Audit in Healthcare: It’s Time to Ride the Wave of Transformation and Innovation

The COVID-19 pandemic has brought massive waves of disruption and unique challenges to the healthcare industry. These waves have driven healthcare delivery organizations to find more innovative means to treat patients safely — while staying afloat.

This white paper covers three areas of focus, two related to the analysis of the healthcare industry-specific results from the 2020 Next Generation of Internal Auditing Survey and one looking at the current state of healthcare internal audit functions:

Prioritizing Next-Generation Internal Auditing — Analysis of the survey results finds that many healthcare organizations need to step up their internal audit efforts in more than a few areas if they aim to build a next-generation internal audit function.

Pre-COVID-19 Audit Plan Priorities — Analysis of the survey results also finds that many of the top priorities from previous years are still considered top priorities in 2020. Interestingly, enterprise risk management (ERM) took its place at the top, foreshadowing unique risks that healthcare providers’ internal audit functions would have to face this year. While these top 10 priorities were assessed pre-COVID-19 and may not be the current top audit priorities for all internal audit functions, they are still priorities that should not be overlooked.

Current Audit Priorities: Detailed Risk Assessment and Audit Planning Considerations — We conclude with a look at current audit priorities and new and emerging challenges and opportunities for healthcare internal audit functions.

Since the crisis began, healthcare delivery organizations have been rapidly transforming how they deliver care and operate. Internal audit functions in many of these organizations have been repositioning their operations and adjusting their priorities to meet new challenges, while also preparing for the post-COVID-19 era. Many are aiming to accelerate their transition to become a next-generation internal audit function, which should:

- Be agile enough to defer noncritical existing efforts, redeploy resources to critical areas and move forward to support the organization's changing environment.
- Identify areas most severely affected by the pandemic, such as emergency management, cybersecurity, telehealth, funding preservation, Section 1135 Waivers and vendor risk management.
- Identify opportunities to work differently in the unfamiliar environment, and leverage lessons learned and new insights to make the internal audit team even better at what they do.
- Fully embrace innovation, transformation and new technologies so that internal audit can have a seat at the table for discussions about helping the organization navigate and emerge from the COVID-19 crisis.

"This particular paper includes content unlike any of our prior publications and takes into consideration the drastic impacts resulting from the COVID-19 pandemic. Never has it been more important to have an agile and dynamic risk assessment process to ensure audit functions deploy their resources efficiently. It is critical for today's internal audit functions to focus on the right risks at the right time to add value and remain relevant to their organizations during these trying times. This also necessitates a commitment to innovation in the areas of analytics, automation and continuous monitoring."

– Richard Williams, Global Healthcare Practice Leader, Protiviti

Prioritizing Next-Generation Internal Auditing

With greater technological capabilities and reporting resources than ever before, the method by which organizations achieve analytic insight over the next year is sure to be a silver lining within the storm cloud.

Healthcare is not the only industry experiencing challenges or in which internal audit teams are trying to adjust to rapidly changing currents. As Brian Christensen, executive vice president of global internal audit at Protiviti, notes: "Innovation and transformation require more than just a series of discrete activities. They necessitate a fundamental rethinking of the design and capabilities of internal audit. Innovation in internal audit is driven by a next-gen, trailblazer mindset, along with a willingness to make bold decisions, learn from mistakes and never stop asking, 'How can we get even better?'"

It is our view that next-generation auditing capabilities, processes and tools should be pressing priorities for the internal audit function to mature as their organizations continue to transform and stakeholder expectations for these capabilities rise. Additionally, high-functioning audit committees want internal audit functions to communicate how their transformation and innovation efforts result in more coverage of risks and more in-depth audit reviews.

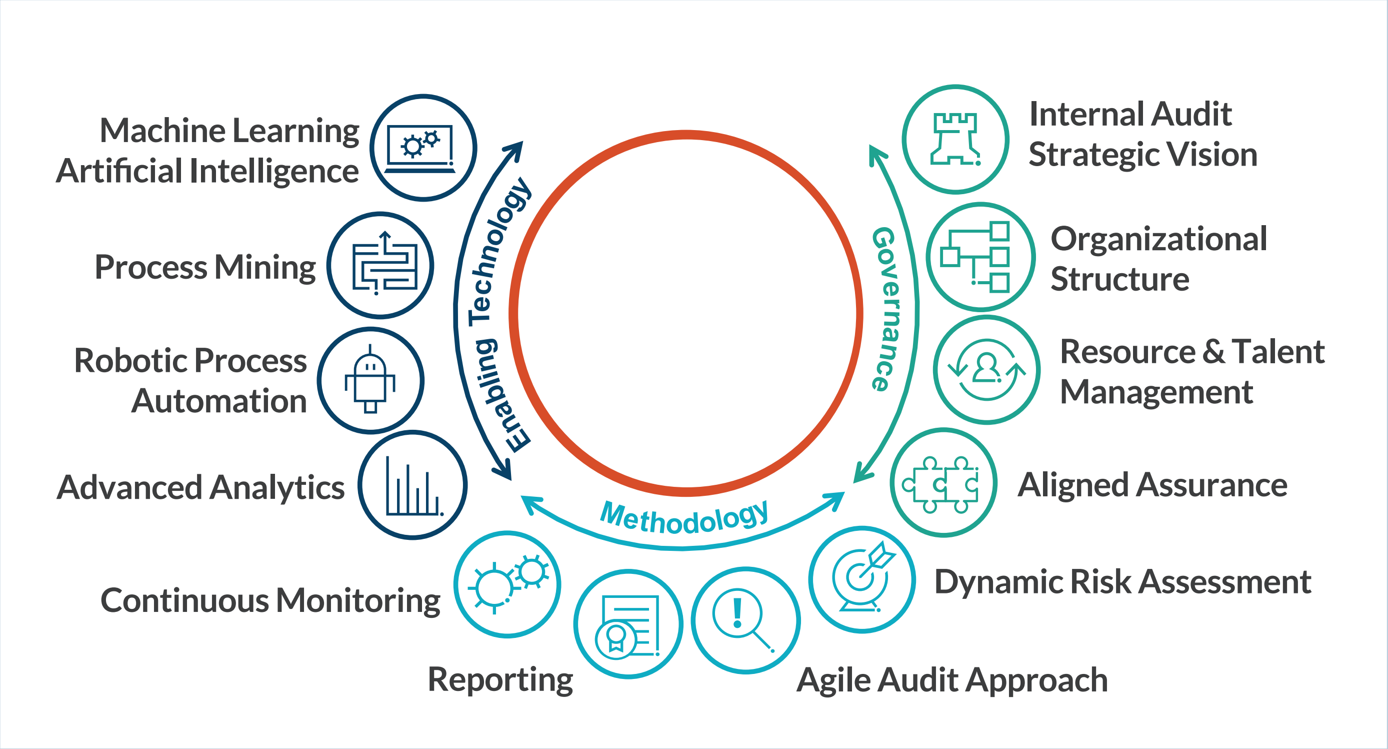
However, becoming a next-generation internal audit function requires the acquisition of different forms of knowledge and the development of new skills and capabilities. Protiviti's 2020 Next Generation of Internal Auditing Survey — to which more than 775 chief audit executives (CAEs) and other top internal audit professionals responded — finds that most audit functions need to move quickly to improve their acquisition and development of these skills. And this year's survey report, *Exploring the Next Generation of Internal Auditing,* outlines the need to advance next-generation internal auditing competencies.[1]

Next-generation internal audit capabilities, processes and tools span all three categories of Protiviti's next-generation internal audit model: governance, methodology and enabling technology (see next page).

Becoming a next-generation internal audit function requires the acquisition of different forms of knowledge and the development of new skills and capabilities.

[1] For more information about the overall findings for all industries, read our full survey report, *Exploring the Next Generation of Internal Auditing, 2020:* www.protiviti.com/IAsurvey.

• • • Protiviti's Vision: The Next Generation of Internal Auditing



In evaluating the current state of healthcare internal audit transformation and innovation initiatives (e.g., robotic process automation [RPA] development, hack-a-thons, innovation challenges) against other industries and results from last year's survey, we find healthcare lags behind in its progress toward next-gen auditing.

Our 2020 survey results also suggest that healthcare providers' internal audit functions may have overreported their digital maturity in 2019. This year, most organizations have probably more accurately identified themselves as beginners, rather than experts, as many did last year.

Also, most healthcare provider respondents state that their internal audit function is not currently pursuing any transformation or innovation initiatives — or worse, they have no plans to do so in the future. Further, about half of healthcare provider respondents believe their internal audit functions are currently behind most competitors and will continue to be so in two years.

As audit committees receive more detailed information about internal audit transformation, their interest in transformation and innovation initiatives increases. CAEs should, therefore, bear in mind that the quality of information they share about these undertakings and how they communicate that information are more important than the quantity of the information they deliver.

Among the three next-generation internal audit categories (governance, methodology and enabling technology), healthcare internal audit functions have demonstrated the most progress in implementing and advancing competencies within the methodology category.

Methodology

The primary reasons audit groups invest in next-generation methodology competencies are to improve the stakeholder experience and achieve a real-time view of risk. Since our 2019 survey, healthcare internal audit functions have increased all four of their methodology competencies (i.e., continuous monitoring, dynamic risk assessment, high-impact reporting and agile auditing). They also indicate that they understand the need to keep improving in all areas.

Continuous monitoring, out of all 12 next-generation internal audit competencies illustrated in our next-gen model, is used by the largest percentage of healthcare internal audit functions, according to our survey results. Internal audit functions need to keep a real-time pulse on the organization's health if they want to continue to grow and be an effective partner to the business. Implementing continuous auditing and monitoring dashboards can help. Analytics and automation drive these dashboards, which can alert auditors to problem areas for further review.

A good example of continuous monitoring is a revenue analytics dashboard that can monitor day-to-day adjustments by claim adjustment reason code (CARC) and generate an alert when a specific daily adjustment exceeds an established threshold (e.g., two standard deviations from the monthly average daily adjustment). Other areas ripe for continuous monitoring include identifying excessive opioid prescribing patterns, irregular controlled substance dispensing (based on automated dispensing machine logs), duplicate payments in accounts payable and/or payroll, excessive overtime, and user access changes.

The best way to stay on top of ever-changing risks is to transition to a dynamic risk assessment process, which continuously refreshes the organization's risk profile and prioritizes where audit should be assisting the organization, rather than hold on to the old, static annual risk assessment. No doubt, this is why two in three healthcare internal audit functions report that they will use a dynamic risk assessment process for their 2020 audit plan.

Governance

Strong governance competencies can help build a solid foundation for the future of the internal audit function and help audit leaders structure their department in a flexible, multidimensional and well-equipped way to confront emerging risks.[2] Resource and talent management and aligned assurance competencies are the two areas in which healthcare internal audit functions have reported increased competencies since our 2019 survey.

This result can likely be attributed to many health-care organizations identifying the need for more resources with next-gen skills. This can be achieved by choosing to work with a strategic co-sourcing partner that has specialized expertise not found in-house (e.g., technical resources, medical record coding auditors, construction subject matter experts), leveraging rotational programs with different departments, and/or utilizing pooled/shared resources between the second and third lines of defense.

[2] The four next-generation governance competencies are aligned assurance, internal audit strategic vision, resource and talent management, and organizational structure.

Enabling Technologies

This should be a red flag for healthcare CAEs: Enabling technology competencies and tools — including machine learning (ML) and artificial intelligence (AI), RPA, or process mining tools — received the lowest competency self-assessments in our 2020 survey. Reported competency in both ML/AI and RPA also decreased from the 2019 results. Also, a strong majority of internal audit functions in healthcare delivery organizations report that they have no plans to adopt any kind of ML/AI, RPA, and/or process mining tools.

For internal audit functions working with these higher-level enabling technologies, at least three in four believe they need to improve their understanding and use of these tools. By using different enabling technologies and continuously monitoring the outputs across different areas of the organization, audit shops can assemble actionable insights around compliance, revenue cycle, finance, human resources (HR) and payroll, to name just a few, while also using the data to assess the risk to the organization dynamically.

It is vital to develop skills and capabilities in all three next-generation categories — methodology, governance and enabling technology — to create a truly next-generation internal audit function. The maturity of these areas should be aligned so that they enable and support each other.

This should be a red flag for healthcare CAEs: Enabling technology competencies and tools — including machine learning and artificial intelligence, RPA, or process mining tools — received the lowest competency self-assessments in our 2020 survey.

Pre-COVID-19 Audit Plan Priorities

Results from the 2020 Next Generation of Internal Auditing Survey also offer a broad look at pre-COVID-19 areas of focus for internal audit functions in healthcare delivery organizations, including top audit plan priorities. All of these areas present excellent opportunities to leverage next-gen auditing capabilities, especially advanced analytics, automation and continuous monitoring. Several notable priorities identified in our study are listed below. We offer a brief commentary on each one in the following pages:

- ERM
- Information Security and Cybersecurity Program Effectiveness
- Accounting, Finance and Accounts Payable
- Health Insurance Portability and Accountability Act (HIPAA) Compliance
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Controls — Finance/IT General Controls
- Fraud, Waste and Abuse Risk Management
- Mobile Applications
- Billing and Collections
- HR, Employee Screening and Payroll
- Vendor Risk Management

ERM

Pre-pandemic signs of being behind the curve in understanding and embracing true ERM fundamentals

Organizations that can proactively anticipate, adapt and respond to change will be the most successful. That is why in non-healthcare industries, many businesses use ERM methodologies to help them evaluate, prioritize and address risks that could prevent them from reaching their desired goals, missions and strategic objectives. Many organizations, to help facilitate the ERM journey, also look to internal audit's expertise to identify and evaluate risks.

The 2020 Next Generation of Internal Auditing Survey results specific to healthcare delivery organizations reflect an industry that was beginning to re-evaluate the benefits of the ERM framework to help pre-emptively address the emerging challenges associated with innovation, technology, acquisitions and regulatory scrutiny prior to the pandemic. However, current-day circumstances have changed the view of ERM to, *"Why weren't we more prepared?"* and, once the dust has settled, *"How can we set ourselves up so that we are prepared next time?"*

An effective ERM discipline provides information regarding risks, uncertainties and opportunities relevant to business and strategic objectives that could influence decision-making and enhance an organization's chances of achieving its goals. The healthcare industry, overall, has been behind the curve in understanding and embracing the fundamentals of true ERM, which is evidenced by the survey results before the pandemic. Now, it is more crucial than ever for the industry to bridge that gap. Going forward, there is an opportunity for healthcare internal audit teams to use the breadth and depth of the impact that the COVID-19 crisis has had on the industry as a lesson and opportunity to assist their organizations in effectively responding to risks and driving organizational resiliency. For example, although many organizations have multiple suppliers for personal protective equipment (PPE), the geographic concentration of those suppliers, when coupled with the unintended consequences of just-in-time inventory processes, were not clearly understood or transparently communicated. Thus, receiving a low risk score because the likelihood was assessed as low resulted in a potential high-impact risk of being short of PPE. A better understanding of concentration risk and inventory levels would have facilitated robust discussions on mitigating strategies or acceptance of the perceived low-likelihood risk.

Going forward, there is an opportunity for healthcare internal audit teams to use the breadth and depth of the impact that the COVID-19 crisis has had on the industry as a lesson and opportunity to assist their organizations in effectively responding to risks and driving organizational resiliency.

Information Security and Cybersecurity Program Effectiveness

Data security is a top priority and an increasing challenge — as is staying ahead of old but effective cyber threats

Security of healthcare data continues to be a top concern and priority for healthcare providers. The environments in which data is used and proliferates are expanding at a rate that very few organizations can keep their arms around. All aspects of healthcare are in dire need of data that can be analyzed for actionable directives, and access to data repositories is growing as a result. Organizations are expanding their use of data lakes and data warehouses to pull together electronic healthcare record (EHR) data with data from many other ancillary systems, so they can better understand health trends and patient health indicators.

The move to value-based care and risk-based contracts increases the need to centralize this information and bring additional personal data elements from outside into the mix to paint a more complete picture of the patient's health profile. For example, socioeconomic information can help healthcare delivery organizations better understand and predict a patient's response to different healthcare nudges or a patient's propensity to pay their portion of healthcare bills.

All of this sensitive information is often being accessed from many different locations. The expanding use of an array of vendor-hosted tools and software is one reason for this trend. As the number of touchpoints that must be protected expands, there is an even greater need for layers of security and good segmentation, as well as proper monitoring controls for detecting malicious or potentially inappropriate activity.

The use of devices connected to the hospital network also continues to expand, and the ability to know when a new device connects is becoming increasingly difficult. Also challenging amid all the digital "noise" is the ability to identify when a device is no longer on the network and to determine whether it might be a potentially lost or stolen device, which would warrant a security incident and breach risk assessment.

Healthcare also continues to experience a rising number of social engineering attacks. The widespread and persistent use of social engineering rivals any other threat seen to date. Phishing campaigns target the psyche of users, convincing them to act on directives that they may typically ignore or be unable to spot. The most important thing to note, though, is that these attack methods are not new, nor are the exploits and vulnerabilities ultimately targeted. They are not zero-day vulnerabilities for which no patch exists; instead, typically, they are exploitable vulnerabilities that have been known for 90 days or longer.

As the number of touchpoints that must be protected expands, there is an even greater need for layers of security and good segmentation, as well as proper monitoring controls for detecting malicious or potentially inappropriate activity.

Accounting, Finance and Accounts Payable

A growing need to partner with finance and accounting to advance capabilities and strengthen controls

Many healthcare finance and accounting departments find themselves in an evolving state. Whether it's due to a merger or acquisition, an enterprise resource planning (ERP) implementation, or the deployment of new processing and reporting tools, the impact on standard processes and day-to-day operations can be significant. The finance and accounting back office may find it difficult to scale and provide the same level of services (in areas such as payroll, accounts payable and financial reporting) as in years past.

The new "normal" for accounting departments working remotely with lean staffing creates greater propensity for lax controls and inefficient processes. Additionally, external cyber threats such as phishing and spoofing have been on the rise as companies have rapidly deployed remote technology. Today's healthcare auditors must consider these trends and partner with their finance and accounting teams to advance their capabilities. That includes placing greater emphasis on financial controls versus operational audits and tapping auditors' skill sets to help identify potential cyberattacks. Audits that use process mining tools and data residing in the organization's ERP system can also help identify process inefficiencies and bottlenecks quickly.

Healthcare boards and audit committees, including those of nonprofit organizations, are eager to strengthen controls to better protect critical assets from fraud and misuse. Automated controls and continuous testing of those controls are essential to creating a high-performing internal audit function.

HIPAA Compliance

A perfect storm for potential noncompliance fines and penalties — and a unique opportunity for internal audit

The rise of the digital age, the push for interoperability, and the ever-changing legal and regulatory landscape pose unique challenges, making HIPAA compliance a continued concern for providers and their internal audit functions. An unauthorized disclosure of protected health information (PHI) may present significant risks to an organization, including reputational risk and significant financial and legal exposure. The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) HIPAA enforcement activity continues to set record-breaking numbers, with HIPAA penalties surpassing $100 million. And HIPAA-related patient complaints to OCR continue to rise year over year, with no signs of slowing down.[3] In addition to HIPAA requirements, many states continue to draft new and amend existing privacy and data security laws, and organizations are struggling to keep up. Increased scrutiny and enforcement from OCR for HIPAA violations, coupled with the complexity of the regulatory landscape and the implementation of new technologies and tools, creates the perfect storm for potential fines and penalties resulting from noncompliance.

[3] "Health Information Privacy Complaints Received by Calendar Year," HHS.gov, accessed August 2020: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html.

Recent enforcement-related news includes an increase in reported violations of the HIPAA Breach Notification Rule and OCR's announcement of the new HIPAA Right of Access enforcement initiative. This new initiative was born out of an increase in patient complaints and targets organizations that fail to provide copies of medical records to patients within a reasonable time and in the requested format.

Additionally, OCR has repeatedly placed significant emphasis on the importance of conducting a comprehensive, organization-wide risk analysis. Failure to do so continues to consistently draw financial penalties for organizations. The current and rapidly changing environment has further complicated HIPAA compliance for providers and serves as a reminder of the significance of conducting accurate and thorough risk analyses. Additionally, it will be vital for healthcare delivery organizations to assess their adherence to appropriate vendor risk management processes, including the execution of Business Associate Agreements (BAAs). Further areas of increased scrutiny may include assessing compliance with permissible uses and disclosures of PHI, performing regular and proactive user access control reviews, and periodically reviewing policies and procedures to ensure that they are reflective of the current operating environment and result in appropriate training of workforce personnel on new or updated policies and procedures. The impact of COVID-19 has further highlighted the importance of adherence to HIPAA, as many organizations may have been quick to enter into third-party arrangements and implement new tools, technologies and processes during the COVID-19 pandemic. These actions make it more important than ever for organizations to revisit their HIPAA risk analysis to assess the impact of recent changes and implementations to the business and provide assurance regarding compliance with HIPAA.

Internal audit functions have the unique opportunity to assist organizations with understanding and managing privacy and security risks and should be closely involved in helping to monitor the effectiveness and adequacy of the organization's privacy and security programs. Documentation will be essential to tell the HIPAA compliance story to regulators, and internal audit should play a critical role in assessing compliance with the mandate during these challenging times.

The impact of COVID-19 has further highlighted the importance of adherence to HIPAA, as many organizations may have been quick to enter into third-party arrangements and implement new tools, technologies and processes during the COVID-19 pandemic.

COSO Internal Controls — Finance/IT General Controls

The need to assist the healthcare delivery organization in designing, implementing and evaluating internal controls

Healthcare organizations continue to experience issues with system access integrity, clinical documentation, and coding and billing, all of which may result in potential noncompliance with federal and state regulations — and costly mistakes. Effective internal control is vital to successfully weathering the ever-changing healthcare environment. And it can help mitigate many of the risks associated with the complex pressures that healthcare organizations confront today.

COSO recommends that every organization evaluate its risks and key controls to determine potential gaps that may require changes to policies and procedures, governance structure, and management oversight. The COSO Internal Control Framework was designed to help businesses establish, assess and enhance their internal controls.

In an effective internal control system, the following five components work to support the achievement of an entity's mission, strategies and related business objectives:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring activities

These components work to establish the foundation for sound internal control within the organization through directed leadership, shared values and a culture that emphasizes accountability for control. The company's various risks are identified and assessed routinely at all levels and within all functions in the organization. Control activities and other mechanisms are proactively designed to address and mitigate the significant risks. Information essential to identifying risks and meeting business objectives is communicated through established channels across the company. The entire system of internal control is monitored continuously, and problems are addressed in a timely manner.

Internal audit can assist in designing, implementing and evaluating internal control for healthcare delivery organizations. Specifically, all control components and principles can be subjected to tests to determine whether they are present and/or functioning. The overall assessment reveals the severity of the deficiencies when aggregated across the components. Focusing on strengthening and/or automating key controls in an organization's existing control structure is vital in the current landscape. Further, internal audit may want to consider adopting the COSO Internal Control Framework, as it facilitates an increased understanding of the existing internal controls and indicates where improvements should be made, resulting in reduced risk for all stakeholders.

COSO recommends that every organization evaluate its risks and key controls to determine potential gaps that may require changes to policies and procedures, governance structure, and management oversight.

Fraud, Waste and Abuse Risk Management

Deterring fraud with a high-functioning, well-established and integrated next-generation internal audit function

Fraud, waste and abuse are always on the minds of payers, regulators and enforcement agencies. The inappropriate use of healthcare resources, whether through the provision of medically unnecessary services, drug diversion or kickbacks, results in millions of overpayments each year for healthcare services — and drives up healthcare costs.

As a result, agencies such as the Centers for Medicare and Medicaid Services (CMS), the Department of Justice (DOJ) and the HHS Office of Inspector General (OIG) have continued to expand enforcement efforts. Over the years, for every dollar spent by the government to fight healthcare-related fraud and abuse, anywhere from four to eight dollars have been recovered.

Even with processes to prevent and detect potentially fraudulent activities, healthcare delivery organizations could face an investigation that may cost them not only financially, but also reputationally. Understanding the organization's vulnerabilities and establishing an appropriate framework to identify and respond to them are essential in today's environment, as regulators are increasingly demanding more active investigation and management of a wide range of compliance risks.

Fraud prevention is the baseline of fraud risk management and has traditionally consisted of implementing simple controls along with designing an ethical and moral tone for the organization. Developing a strong compliance program is crucial to preventing healthcare fraud and abuse activities. Per the OIG, a compliance program should "establish a culture … that promotes prevention, detection and resolution of instances of conduct that do not conform to Federal and State law, and Federal, State and private payer healthcare program requirements, as well as … ethical and business policies. In practice, the compliance program should effectively articulate and demonstrate the organization's commitment to the compliance process."[4]

The DOJ further emphasizes the importance of a compliance program in preventing fraud and abuse in its "Evaluation of Corporate Compliance Programs" guidance, revised in June 2020.[5]

One of the most common anti-fraud controls is a high-functioning, well-established and integrated next-generation internal audit function. As opposed to compliance auditors performing probe audits to assess potential risks, internal auditors in healthcare organizations today have the tools to obtain a view of an entire population of claims, transactions or arrangements and identify outliers. They can obtain and compare information between multiple systems to validate the appropriate movement of information, pharmaceuticals or patients. Organizations can identify risk areas more quickly by using advanced analytics and automated processes and better utilizing limited resources to surface and mitigate risks. This allows more time and effort for focused, in-depth investigations, while managing risks.

[4] "Compliance Program Guidance for Hospitals," HHS OIG, *Federal Register*, Vol. 63, No. 35, February 23, 1998: oig.hhs.gov/authorities/docs/cpghosp.pdf.

[5] "Evaluation of Corporate Compliance Programs," DOJ, June 2020 update: www.justice.gov/criminal-fraud/page/file/937501/download.

Mobile Applications

Navigating untested waters in the quest to deliver more personalized and convenient patient care

As part of the overarching move to become more consumer-centric, healthcare organizations continue to connect healthcare services and provide touchpoints for patients and clinicians through mobile devices. This focus includes deploying mobile applications from software companies like large EHR providers, but the industry is also seeing a reemergence in developing custom, homegrown applications. One reason for this trend is that many healthcare providers find that out-of-the-box mobile applications do not meet their needs or provide their consumers the interface, interaction or experience intended.

Whether it is by using off-the-shelf or custom-developed applications or something in between, healthcare providers are moving certain aspects of care to meet the patient where they want to interact. But this creates challenges for providers, such as:

- The need for custom code and application development — skills the organization may not have in-house.
- The use of agile and lean methodologies for project delivery, which can be difficult to adopt initially, from a company culture perspective.
- The fact that many applications deal with sensitive electronic PHI to help make the interaction with the application more personalized and user-friendly.
- The fact that mobile applications often need to be developed and implemented quickly — and most healthcare organizations are not conditioned to move fast when rolling out new offerings.

Many healthcare providers are just starting to navigate the waters of mobile applications, and it is a journey they must make. Internal audit can help by assessing whether these digital initiatives and the associated governance programs are being given their proper due diligence.

Healthcare organizations should also consider assessing whether a defined development, security and operations program (DevSecOps) that establishes the foundation for accelerated change and uses project delivery constructs like agile and lean can help them meet the multitude of demands of these new system development efforts.

Mobile applications often need to be developed and implemented quickly — and most healthcare organizations are not conditioned to move fast when rolling out new offerings.

Billing and Collections

The opportunity to become a pivotal partner in billing and collections efforts today, and for the future

An important attribute of financial reporting is ensuring that revenue integrity is maintained through various control activities, including solid reconciliation efforts that accurately identify payments received and variances from payers. For provider organizations' financial health, the ability to identify initial payer denials or adjustments accurately and employ robust reconciliation efforts is crucial.

Internal audit should use next-generation audit capabilities, advanced analytics, and continuous monitoring and auditing for timely identification to assist management in being aware of issues and effectively managing and monitoring the billing and collection processes. Internal audit should be engaged as a partner in healthcare organizations' billing and collections efforts now and into the future to assist in the development and strengthening of the overall control environment.

HR, Employee Screening and Payroll

Audits a critical tool for identifying gaps in HR practices and minimizing associated legal or regulatory violations

With high turnover, staffing shortages and complex regulations, HR continues to be a top area of concern for healthcare organizations. HR professionals' responsibilities are wide-ranging, and the resources available to handle a growing workforce are often limited. HR audits can reduce the risk of legal and regulatory liability from ineffective or inadequate HR processes. They can also identify whether specific HR practices are appropriately designed to address compliance, legal and reputational risk.

It is essential for employee screening to be an area of focus for healthcare organizations from both regulatory compliance and patient safety perspectives. An effective audit will incorporate a review of target areas such as timely background checks, government sanction list monitoring, due diligence of third-party vendors, and appropriate licensure and credentialing of healthcare professionals. Data analytics and automation may also be useful for identifying trends and process gaps related to the screening process.

Additionally, as payroll accounts for one of the most significant costs for healthcare providers, it is imperative to conduct a thorough review of payroll practices. Within the healthcare setting, there are various payment structures that must be accounted for, making payroll audits relatively complex. These audits may reveal noncompliance with Department of Labor (DOL) regulations and/or state regulations, potential employee fraud, inequitable pay, errors in manual and/or automated calculations, or outdated/lack of approved payroll policies and procedures. Also, as organizations implement advanced payroll software, the updated processes should be audited early on to ensure the system is working effectively and to minimize potential risks.

The results from HR audits will help identify gaps in practices and can be used to develop and implement strategies to reduce the potential for legal or regulatory violations and achieve best-in-class performance.

Vendor Risk Management

Adding value by assessing the vendor risk management life cycle based on inherent risks

Healthcare organizations partner with third-party vendors either to outsource services, drive service excellence, control costs and risks, or gain some other type of advantage. These relationships can create value as well as risk for healthcare providers, including financial, reputational, compliance and even patient safety risk. Many healthcare providers struggle with vendor risk management, and the inability to adequately assess and understand the risks that vendors pose is becoming incredibly costly for many of these organizations.

In general, healthcare organizations recognize the importance of vendor risk management; however, few organizations can say they are doing it effectively. Many think that current manual vendor risk management processes cannot keep pace with increasing cyber threats and vulnerabilities, which are compounded by the undertaking of a wide variety of new digital initiatives.

Given increasing regulatory scrutiny, it is essential that vendors, defined as business associates (BAs) under HIPAA, and the associated rules are identified. Complicating this are questionnaires aimed at determining whether a vendor is a BA and, if so, whether the vendor has acceptable controls in place, which are often inaccurate or incomplete. The processes in place to get comprehensive answers from vendors and verify the accuracy of the information they provide are often insufficient. Once identified as a BA, regulatorily required language and a business associate agreement (BAA) should be included in the contract.

Many healthcare organizations worry that their senior executives or regional leadership can bypass the third-party assessment process to secure a lucrative business relationship, creating an enormous loophole for even the most effective vendor risk management programs. Finally, many healthcare organizations do not believe their vendor risk assessments, as they exist today, are valuable for providing actionable insights to the C-suite and board of directors.

Internal audit can add value to the vendor management function by assessing the organization's processes to classify and perform due diligence on vendors based on inherent risks. Internal audit can also assess how contractual documents are being created, retained and reviewed as a function of that identified risk. Additionally, internal audit can evaluate the vendor risk management life cycle to determine how effectively the organization uses ongoing assessments and performance monitoring mechanisms (e.g., scorecards, questionnaires, on-site assessments) to manage the overall portfolio of vendor risk.

Internal audit can add value to the vendor management function by assessing the organization's processes to classify and perform due diligence on vendors based on inherent risks.

Current Audit Priorities: Detailed Risk Assessment and Audit Planning Considerations

The top 10 audit plan priorities identified above represent both risk areas as well as opportunities for internal audit and their organizations to achieve value and improve performance. However, the reality for many organizations is that COVID-19 has changed audit work plans and, in many organizations, elevated existing risks and/or added new risk areas that could not have been anticipated in the 2020 survey. These risks are discussed below, and their impact includes the need to pivot internal audit staff to prioritize urgent business needs or reduce staffing due to financial performance. If this sounds all too familiar, it will be important to help your organization understand the reprioritization of internal audit activities and the associated impact on the coverage of top 2020 risks for this year and the next. If reprioritization and/or budgets will not allow the internal audit coverage of key risk areas at an organization, these risk areas should still be defined, reported and accepted throughout the organization's oversight structure.

The impact of the COVID-19 crisis on individuals, businesses, communities and governments around the globe continues to expand. Over the last several months, resource and operational burdens on healthcare organizations have expanded exponentially. Waves of demand, changing regulatory requirements and stimulus legislation (e.g., the Coronavirus Aid, Relief and Economic Security [CARES] Act) have created a new environment in healthcare. So, in addition to outlining this year's pre-COVID-19 healthcare internal audit plan priorities, we are presenting the current (i.e., post-COVID-19) audit priorities that we've identified through our various interactions with CAEs.

Listed below are several notable priorities that have emerged or augmented standard practices as a result of the pandemic. A brief commentary on each, and discussion of the challenges and opportunities for internal audit, are provided on the pages that follow.

- Funding Preservation
- Telehealth
- Revenue Integrity
- Cybersecurity
- Regulatory Compliance (e.g., Section 1135 Waivers)
- Emergency Management
- Supply Chain
- Patient Safety

Funding Preservation

Helping healthcare organizations to access and preserve funding relief and substantiate appropriate use of funds

Healthcare providers have endured significant challenges throughout the COVID-19 pandemic. They have seen a significant disruption in revenue due to the cancellation and/or deferrals of elective procedures. Additionally, providers have incurred incremental costs associated with the procurement of PPE, "deep cleaning" and other time-intensive protection activities, such as reconfiguring facilities and establishing emergency command centers and remote workforce teams.

Funding relief has been made available to providers through a variety of programs. This includes the CARES Act, the Paycheck Protection Program and Healthcare Enhancement Act, CMS advance payments, Federal Emergency Management Agency (FEMA) programs, and others. Healthcare organizations must be aware of what funding programs exist and from which programs they received money. They must also be aware of what they must do to retain and preserve those funds.

Healthcare internal auditors can serve a vital role in helping their organizations access and preserve funding in several ways, including by:

- Telling the story (understanding how the organization has articulated and documented the impact of COVID-19 and encouraging that it be clearly linked to the use of funding relief).
- Facilitating awareness of and access to funding sources (determining that all available funding programs have been considered and that the associated terms and conditions can be met).
- Enhancing governance oversight (ensuring effective representation of the board, management and advisers to oversee the inherent complexities of the funding programs).
- Ensuring fund management (reviewing internal controls that support the monitoring, accounting and documentation of funds received).
- Overseeing compliance (assurance activities that confirm terms and conditions have been met).

The CARES Act, the Paycheck Protection Program and the Healthcare Enhancement Act have allocated $175 billion in funding to the Provider Relief Fund (PRF). As of early September 2020, an estimated $50 billion of the PRF was still available for distribution. Recipients of these funds have had to submit attestations representing their agreement to terms and conditions and provide periodic reporting. We have seen savvy and agile internal audit programs assist in establishing funding trackers, documenting key controls to meet terms and conditions, and reviewing attestations and reports before submission.

There have been significant developments regarding the use of provider relief funds during September and October of 2020. On September 19, 2020, HHS issued the "Post-Payment Notice of Reporting Requirements," which effectively further restricted how providers could account for lost revenue by considering year-over-year change in net patient care operating income.[6] This guidance was significant because previous guidance from HHS suggested lost revenue could be accounted for in the year-over-year change in actual revenue from patient care-related sources.

Following the September notice, HHS announced on October 1, 2020, a phase 3 general distribution of $20 billion.[7] Eligible providers are required to submit an application. While HHS has made payments on a rolling basis under the previous general distributions, Phase 3 final payment amounts for applicants who have already received payments equaling 2% of annual patient care revenue will be determined once all applications have been received and reviewed. This will be computed after the November 6, 2020 application deadline and HHS review of applications.

The final significant development during October was when HHS issued *General and Targeted Distributions Post Payment Notice of Reporting Requirements.*[8] HHS commented that it received feedback from many voicing concerns regarding this approach to permissible uses of provider relief funds, including the September 19 announcement. In response to concerns raised, HHS amended the reporting instructions to increase flexibility around how providers can apply PRF money toward lost revenues attributable to coronavirus. After reimbursing healthcare-related expenses attributable to coronavirus that were unreimbursed by other sources, providers may use remaining PRF funds to cover any lost revenue, measured as a negative change in year-over-year actual revenue from patient care-related sources.

Internal audit professionals possess the knowledge and experience to assist an organization both with successful identification, organization and retention of required documents to support the use of funds as well as with the identification and return of funds not used or appropriately supported. The government funding sources have clearly stated their intentions to perform audits to ensure the allowable use of PRF dollars. This includes the announcement by the HHS OIG in August 2020 that its work plan now includes an audit of "CARES Act Provider Relief Funds — General and Targeted Distributions to Hospitals."

Telehealth

A crucial role for internal audit to play in setting up efficient, effective, compliant and profitable telehealth services

Telehealth has irreversibly changed how healthcare is delivered. Healthcare organizations now have an opportunity to develop or significantly expand their telehealth services to provide patient care and improve patient safety and satisfaction. However, telehealth also presents several challenges that provider organizations must manage. Internal audit has a role to play in helping to develop and review clinical workflow, documentation and coding completeness and accuracy for these services and the controls around implementing effective and secure technology.

[6] *Post-Payment Notice of Reporting Requirements*, Department of Health and Human Services, September 19, 2020: www.hhs.gov/sites/default/files/post-payment-notice-of-reporting-requirements.pdf.

[7] *Trump Administration Announces $20 Billion in New Phase 3 Provider Relief Funding*, Department of Health and Human Services, October 1, 2020: www.hhs.gov/about/news/2020/10/1/trump-administration-announces-20-billion-in-new-phase-3-provider-relief-funding.html.

[8] *Post-Payment Notice of Reporting Requirements*, Department of Health and Human Services, October 22, 2020: www.hhs.gov/sites/default/files/post-payment-notice-of-reporting-requirements-october-2020.pdf.

Given the increased need for and reliance on telehealth services during the pandemic and beyond, it will be increasingly important for internal audit to ensure that risks are mitigated and scalability of these services is considered. It is important to establish a programmatic approach that includes compliant and efficient workflows, website updates, planned expansion of services, scheduling and visit management processes, and billing and coding procedures. Internal auditors can also help ensure HIPAA compliance and third-party risk management of new and existing vendors as telehealth and virtual care platforms are implemented and become vitally important to healthcare delivery systems.

Setting up and managing a telehealth service requires a comprehensive approach to program design and execution as well as to monitoring cost, quality and service performance. A multidimensional approach by internal audit, with a focus on six key areas — revenue cycle, clinical integration, regulatory compliance, workstream management, technology, and privacy and security — will allow organizations to mitigate risk and ensure optimal delivery of telehealth services.

Medicare and commercial payers are significantly expanding the array of services provided via telehealth that they will reimburse, and they are increasing payment rates. So, coding, billing and revenue integrity department leaders must work collaboratively to develop and maintain a matrix of reimbursable services and coding requirements (e.g., modifiers, place of service) by payer, and to communicate regularly any changes to the coding and billing teams.

Revenue Integrity

An ideal time to consider employing advanced methodologies and tools in revenue integrity efforts

The time to take a more agile, data-driven and proactive approach to managing an organization's billing and collections functions has never been more evident. Leveraging continued technological innovations, including the use of AI and advanced analytics, is a great opportunity to assist management with identifying and helping to resolve continued margin pressures. Fortunately, healthcare organizations can leverage their next-generation internal audit functions to identify potential control gaps as well as opportunities for greater efficiencies and effectiveness.

Although revenue integrity processes remain a constant concern within the industry year over year, it is especially difficult to separate it from the current global state of affairs and how it impacts a provider's long-term financial health. Revenue integrity departments must have a good handle on specific activities. From correctly identifying COVID-19 patients for proper coding and billing to knowing which payers have waived patient financial responsibilities to being able to accurately identify over- and underpayments, previously streamlined functions have become more complex. Many organizations have increased bill holds for a secondary review of billing before notifying and pursuing collections from patients, with the understanding that any billing inaccuracies will not only negatively impact the overall patient experience during a time of heightened sensitivities but also lead to inefficiencies and costly rework.

Although revenue integrity processes remain a constant concern within the industry year over year, it is especially difficult to separate it from the current global state of affairs and how it impacts a provider's long-term financial health.

Operational processes to review claims and append specific modifiers pertinent to cost-sharing (CS) and telemedicine (95, GT) must be assessed and monitored frequently to ensure those processes are functioning as intended and claims are submitted accurately.

Many organizations have improved their monitoring and reporting processes to better understand billing inaccuracies that may negatively impact the overall patient experience. One example is a process that validates patient room and board (R&B) accommodation levels, particularly ensuring intubated COVID-19 patients have the correct intensive care accommodation assigned. The use of next-generation auditing techniques and continuous monitoring and analytics tools can play a key role in the identification of variances, as provider organizations return to a semblance of normalcy.

Ensuring controls like these are in place will prove pivotal going forward. Due to the increase in uninsured patients, many healthcare organizations are submitting applications for federal and state grants and funding. Many of these funds require organizations to submit daily COVID-19 statistics such as the volume of admissions, ventilators in use and mortalities. The mechanisms and approach to obtain and submit this information will be under scrutiny and reviewed by federal and state entities in future audits. It is essential that revenue integrity and internal audit functions are aware of the documentation required to pass these audits. This will reduce the risk of an organization forfeiting any federal or state aid received to offset the economic impacts of the pandemic.

Additionally, with more employees working remotely, organizations must also consider what tools to use to measure and monitor employee productivity. Departments need to establish baseline metrics for performance and consistently track, trend and monitor them to ensure that employees who have transitioned to a work-from-home environment remain productive. This is an ideal time for healthcare providers to evaluate controls in place from a revenue integrity perspective and improve or reinforce them in conjunction with their internal audit function. Internal audit should strongly consider employing previously mentioned advanced tools and next-gen methodologies to help bring organizations back to normal and lead them into a more prosperous future as they emerge from the crisis and begin to transition to a post-COVID-19 environment.

Cybersecurity

Minimizing security risk to support workers, ensure consistent system functionality and reduce disruptions

COVID-19 has placed significant pressure on the healthcare industry to adapt in multiple ways to a constantly changing landscape that includes emerging cybersecurity threats along with the need to manage a remote workforce and the associated security for remote connections.

Cyberattacks have skyrocketed during the COVID-19 pandemic outbreak, as nefarious parties attempt to capitalize on the crisis by preying on fears and curiosity, even targeting those trying to help. Providing tighter information security is essential to defending healthcare organizations adequately while a second type of pandemic is underway — one aimed at compromising their sensitive data and most prized networks and applications.

On April 8, 2020, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) issued a joint alert[9] reflecting a surge of "COVID-19 related themes by malicious cyber

[9] "COVID-19 Exploited by Malicious Cyber Actors," Alert (AA20-099A), April 8, 2020, joint alert from DHS, CISA and NCSC: https://us-cert.cisa.gov/ncas/alerts/aa20-099a.

actors.” This surge comes while healthcare providers are changing multiple aspects of their environments to enable a new normal. These changes include:

- Deploying new telehealth platforms and external-facing websites.
- Adding new virtual private network (VPN) connections so that administrative personnel can work from home.
- Placing workforce members on temporary furloughs.
- Making changes to EHR to enable better identification, diagnosis, orders and tracking of COVID-19 patients.

The balancing act of needing to move quickly to address the community’s biggest health needs while protecting the privacy and security of sensitive information is very difficult, and it is one that attackers know is likely to lead to vulnerabilities on which they can capitalize. While this increase comes as no great surprise to the information security community (attackers love a crisis), the solution is also no major surprise. It all boils down to good information security hygiene practices, which contribute to a strong information security program. These are prime areas for internal audit to assess:

- Vulnerability management (addressing known vulnerabilities with good patching processes).
- Identity access management (IAM) and multi-factor authentication (MFA) (utilizing multifactor authentication mechanisms to grant access to known and authorized users for external-facing systems and portals).
- Education and security awareness for the workforce (e.g., providing regular reminders, tips and tricks on what to be on the lookout for).

Another technical consideration might be to add identifiers to data loss prevention (DLP) tools to identify messages coming from outside the organization with “COVID-19” in the subject line and immediately tag them as external to the organization, which provides users with another indicator of a potential threat.

While the world is focused on healthcare workers valiantly fighting for their patients’ health, reducing information security risks throughout the entire system will help ensure these workers have the resources needed to save more lives. Minimizing security risk will add stability to support healthcare staff, wherever they are working, and it will help ensure consistent system functionality and reduce disruptions. It should be a key focus for internal auditors to assess how well their organization is addressing these areas of concern.

While the world is focused on healthcare workers valiantly fighting for their patients’ health, reducing information security risks throughout the entire system will help ensure these workers have the resources needed to save more lives.

Regulatory Compliance (e.g., Section 1135 Waivers)

Helping the organization transition back to a strong culture of compliance post-pandemic

Federal and state government responses to the pandemic provided numerous opportunities for organizations to better serve patients affected by COVID-19. On March 13, 2020, the declaration of a national emergency enabled the HHS secretary to temporarily suspend, modify or make flexible (authorized under Section 1135 of the Social Security Act) certain federal requirements related to the Medicare Conditions of Participation, Medicaid plans (including the Children's Health Insurance Program) and HIPAA.

While the Section 1135 Waivers ("waivers") relaxed several specific federal requirements, it is important to note that the state laws still apply, unless modified by other means. The waivers address and relax only specified regulatory requirements. For example, multiple waivers are in effect related to telehealth, but specific coding requirements remain. There is a waiver of the fair market value requirement for physician arrangements, but all other Stark Law requirements still need to be met. Navigating the requirements and concessions without running into Stark, False Claims Act, Anti-Kickback or other regulatory consequences takes a team of skilled professionals. It is essential to engage the legal, compliance and internal audit teams in interpreting the waivers during the pandemic, identify how they relate to the organization, and determine what controls can be put in place to mitigate the risks.

Further, an organization's actions post-pandemic are just as important. COVID-19 has changed the regulatory landscape and created new compliance risks. We believe the waivers that organizations utilize during the pandemic period will be scrutinized by regulatory bodies, especially as they pertain to additional reimbursement received. The regulatory agencies will be looking to ensure that new and old regulations are followed as designed as soon as the official state of national emergency ends.

With the relaxation of regulatory compliance afforded by the waivers, it seemed relatively easy to shift from a strong culture of compliance to a state of less stringent regulatory requirements. Once the waivers end, will the transition back to that strong culture of compliance be as easy? As we shift to the new normal, the transition may be slow in some instances and abrupt in others. While there is some consideration for a gradual shift in areas where waivers were applied, in many, there will be a hard shift when the national emergency ends or when the organization can no longer justify the use of the waivers.

Changing behavior is difficult, especially as organizations begin to see normal operations slowly return. This is an opportunity for internal audit to partner with compliance to review and ensure that everyone returns to following the rules. Sustaining a culture of compliance is challenging enough already. Adding a layer of complexity, where workforces tend to be more remote, will present even more issues.

In addition to the waivers, healthcare organizations and internal audit should reassess, identify and prioritize COVID-19 compliance risks by dynamically conducting or updating their risk assessment. For example, if a healthcare organization accepts CARES Act funding, it is required to comply with the associated terms and conditions or risk False Claims Act exposure. Further, internal audit can support its organization by ensuring that the organization is educating staff on new policies and requirements, while also re-educating them on requirements that will come back.

Emergency Management

Helping the organization determine what the pathway to recovery will be

COVID-19 affects every aspect of emergency management, especially the ongoing recovery process, as we transition to the "new normal." And while emergency management is not a new concept for healthcare delivery organizations, COVID-19 has transformed how organizations and internal audit must prepare for and respond to emergency situations.

The structure of an emergency management plan starts with a facility-specific hazard vulnerability analysis (HVA), which identifies the top emergency-related risks, and ends with an actionable recovery plan based on lessons learned throughout the duration of the emergency. With the current COVID-19 pandemic, accreditation bodies such as The Joint Commission are requesting document reviews prior to on-site visits and are assessing how an organization adapted its infection control and emergency management processes in response to the pandemic. They will focus their reviews on current practices to ensure the organization continues to provide safe care and work in a safe environment. Internal audit needs to focus on the integration of current emergency plans with COVID-19-centric requirements.

Organizations, with the support of their internal audit teams, will want to incorporate lessons learned during the pandemic into their business impact analyses and continuity plans in order to enhance their emergency plans further. There are five critical themes of emergency management that internal audit should review:

1. **Emergency Preparedness Plan Based on an HVA —** Regulatory requirements require that each facility review its HVA annually for technological hazards, natural hazards, human hazards and hazardous materials. The organization should also include infectious diseases and active shooter situations in the top 10 risks, which can be reviewed by internal audit.
2. **Demobilization and Resiliency Planning —** Internal audit can validate that a demobilization plan is in place that enables the efficient and effective return of resources and equipment to their original state. Resiliency planning takes into account pre-event, response and recovery considerations for various departments and patients.
3. **After Action Reporting and Lessons Learned —** After action reports must be submitted to CMS and incorporated into an organization's emergency preparedness plan. Lessons learned, positive and negative, can provide significant value as teaching opportunities. Internal audit can assist organizations to ensure that lessons learned are used to configure a more robust and tailored emergency preparedness plan that allows for avoidance of negative impact.
4. **Business Impact Analysis Feeds Into Business Continuity Plans —** The business impact analysis is foundational to the business continuity plan. Internal audit can assist management by reviewing the analysis and plan to verify that it identifies and prioritizes critical processes that should be maintained after an incident.
5. **Business Continuity/Recovery Plans —** These plans allow organizations to start their recovery early, even while the emergency is in progress, and to secure the smoothest possible transition. They also help mitigate risk, enhance resilience and assist organizations in achieving new-normal standard operations.

As healthcare delivery organizations transition to a new normal, internal audit can validate that regulatory requirements are met to facilitate the pathway to recovery. Proper and thoughtful emergency management execution is vital to a healthcare organization's success during unprecedented emergencies such as COVID-19.

Supply Chain

Creating a supply chain resiliency plan that supports a risk mitigation approach

The healthcare supply chain involves numerous steps to get different product types to flow from manufacturers to patients. Success requires the participation of various stakeholders who work in concert to meet patient care needs. Ensuring adequate access to supplies, pharmaceuticals and equipment is essential to maintaining worker and patient health and safety. Manufacturing disruption and production issues during public health emergencies and other disasters can play a significant role in supply chain operations through the activation of programs designed to protect the availability of essential supplies and services. Vendors for commonly needed products during these events, including vaccines and PPE, are often limited. As COVID-19 has demonstrated, demand for these products can far exceed production capacity.

Organizations should consider a supply chain resiliency plan that focuses on staff, providers and patients, takes into account the role of manufacturers and distributors, and identifies any key vulnerabilities in the supply chain process. There are three main components of a supply chain resiliency plan that internal audit can assist with and/or monitor. These include:

1. **Pre-Events:**
   - Identify hazards, vulnerabilities and threats, specifically focusing on events that could significantly disrupt supply delivery or compromise current supplies.
   - Establish an alternate distributors list for critical supplies as well as understand the location, transport time and potential interruptions in delivery between distributors and providers.
   - Identify alternative methods and routes for deliveries based on predicted hazards. Determine the organization's role for planning, information sharing, indexing, and managing resource requests and brokering with distributors during an incident.
2. **Response:**
   - Forecast the organization's supply needs. Critical to this is knowing what supplies are needed and having the supplies on-site, a place to store them, and a plan for their replenishment.
   - Mitigate or adjust to staff shortages, as staff absenteeism may occur during these events, especially for downstream components (e.g., distributors, last mile and healthcare facilities). It can be a challenge to maintain healthcare operations during disruptive events.
3. **Recovery:**
   - Resume normal operations and communicate the resumption of normal allocation, delivery and/or activities with distributors and organization partners.
   - Communicate to patients and providers about resumption of normal activities and processes.
   - Include consideration of a 90-day stockpile reserve.
   - Re-evaluate contracts with group purchasing organizations (GPOs) to include an exception to independently utilize other distributors during an emergency for supplies that are not available.

A supply chain resiliency plan can support a risk mitigation strategy in accelerating a return to normal for the recovery processes.

Patient Safety

Supporting a culture of safety during a pandemic

Keeping patients and employees safe during this time of increased risk of disease transmission while operating at full capacity-plus takes a coordinated approach. A culture of safety, where staff and clinicians can speak up, is a must. And while creating a strong culture typically takes years, changes made while responding to a crisis can dramatically accelerate the process. There are many ways leaders can facilitate a culture of safety, such as daily huddles, frequent and easy-to-understand communication, leadership visibility, and setting clear expectations.

For the internal audit department, it is important to verify that there is a well-established mechanism for reporting patient safety events, near misses and unexpected incidents, and that staff are routinely utilizing it. A review of trended patient safety data which looks at volume, location and type of events is an effective mechanism to evaluate the prevalence of reporting. A strong culture of safety is dependent upon high levels of reporting so that problems can be identified.

High-reliability organizations, which are relentless in prioritizing safety, close the loop — from identification to execution of improvements to monitoring that solutions stick and achieve desired outcomes. Internal audit can support a culture of safety through the monitoring of patient safety data and ensure that issues identified are addressed at both the broad organizational level and the individual department level.

Additional Considerations

Beyond the detailed risk assessment and audit planning considerations outlined above, internal audit functions should also be aware of and monitor key risks associated with the following considerations:

- Accreditation/regulatory readiness (e.g., conditions of participation [CoP])
- Compliance program effectiveness
- Employee safety
- ERP implementations
- Information blocking
- Opioid and drug diversion
- Pricing transparency
- Remote workforce monitoring

In Closing

In a rapidly changing world, healthcare internal audit functions address emerging challenges every day. The COVID-19 pandemic and its impacts on the healthcare landscape are massive waves of disruption that require an adjustment of internal audit's priorities.

Historically, innovation and transformation initiatives within healthcare's internal audit functions have lagged behind other industries in key technology and governance areas. However, healthcare delivery organizations are now demanding more from internal audit — and that need and expectation have only intensified in the current environment.

Too many internal audit functions and leaders are stuck in traditional roles and relationships, which can create resistance to innovation and transformation. If an internal audit function wants to remain relevant in a post-COVID-19 world, it must evolve and innovate quickly.

Healthcare internal audit must develop innovative approaches as processes change, new technologies are adopted and regulatory demands fluctuate. The function should not be content with doing the same things in the same ways. Auditors must learn how to identify and mitigate emerging risks, encourage best practices, and deliver creative solutions that audit committees need, when they need it.

It takes commitment and courage to pursue innovation. That commitment must originate with internal audit leadership, who must then have the courage to initiate uncomfortable but necessary changes that will help accelerate the transformation of their organization into a next-generation internal audit function — one equipped with the skills, tools and capabilities to support healthcare delivery organizations in the current crisis, and beyond.

The time for healthcare internal audit functions to ride the wave of transformation and innovation is now.

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of Fortune 1000 and 35% of Fortune Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

OUR HEALTHCARE INTERNAL AUDIT SOLUTIONS

Healthcare organizations today are faced with a myriad of challenges and many are underutilizing one of their greatest assets: internal audit. Leading internal audit functions have moved well beyond checking the box on policy compliance and serve as a strategic partner to help ensure their organizations become more innovative and explore new technologies, identify and mitigate emerging risks, develop creative solutions to complex business challenges, and encourage best practices to enhance business functions. Protiviti's industry-leading healthcare internal audit solutions are flexible with proven methodologies, provide access to a vast array of skills, are value-added and collaborative, incorporate tools/techniques such as robotic process automation and advanced analytics, and allow us to be a strategic partner in helping your organization confidently face the future.

CONTACTS

Richard Williams
Global Healthcare Industry Leader
+1.214.395.1662
richard.williams@protiviti.com

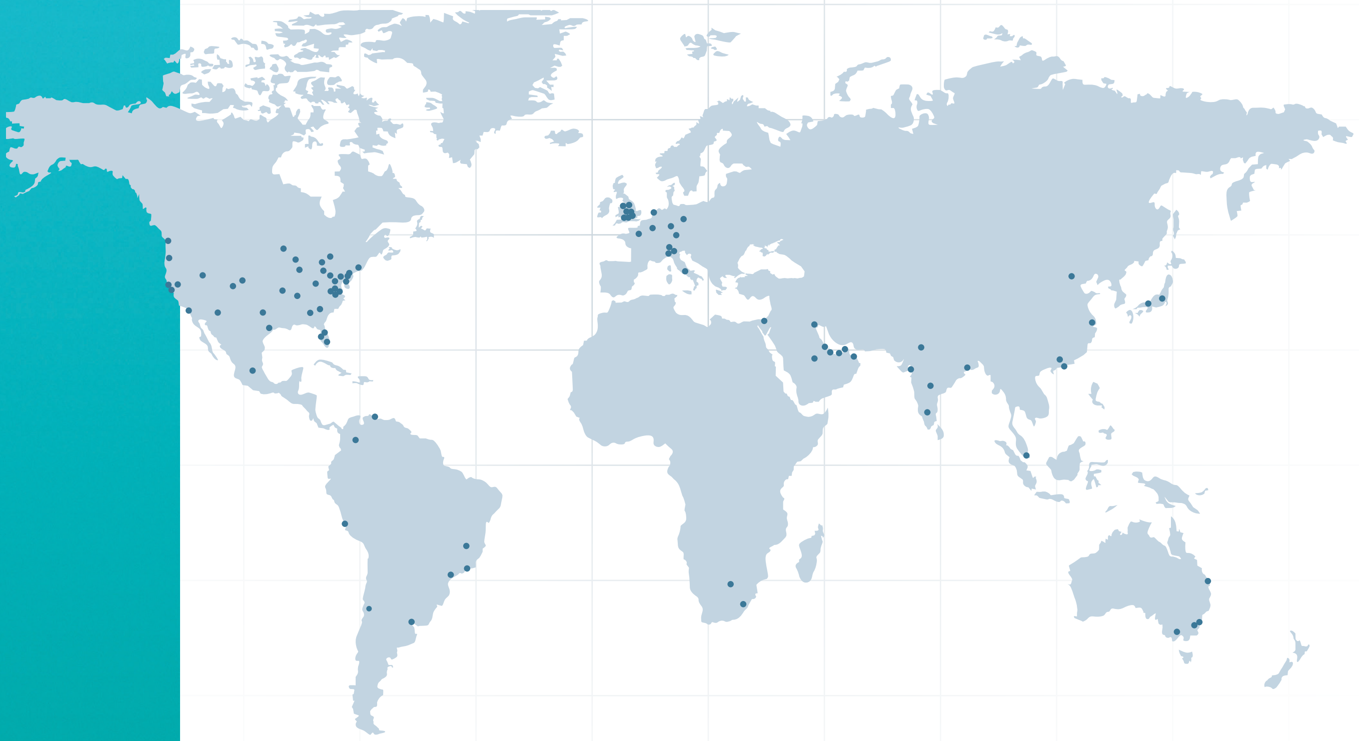
Jarod Baccus
Internal Audit Solutions Lead
+1.281.513.9559
jarod.baccus@protiviti.com

David Kupinski
Central Region Healthcare Lead
+1.317.937.7593
david.kupinski@protiviti.com

Bryon Neaman
Northeast Region Healthcare Lead
+1.410.375.7946
bryon.neaman@protiviti.com

Vickie Patterson
Southeast Region Healthcare Lead
+1.813.348.3407
vickie.patterson@protiviti.com

Alex Robison
West Region Healthcare Lead
+1.602.273.8022
alex.robison@protiviti.com



THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte
Rio de Janeiro
Sao Paulo

CANADA
Kitchener-Waterloo
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM