Risk-based Internal Audit Plans

Sharpen your risk assessment focus

By Debra Bowes, CPA, and Mark Laccetti, CPA, CGMA

Healthcare risks evolve rapidly due to technological, economic, operational and regulatory changes, public expectations and the demand for greater transparency. To keep pace, internal audit functions must take a much more risk-focused approach in developing their internal audit plans.

Risk assessments serve a vital role in helping an organization's leaders and internal auditors understand potential impediments to achieving strategic objectives. Risk assessments help identify and review the organization's risks and the effectiveness of mitigating controls, thereby ensuring that internal audit plans focus on the most crucial areas across the organization.

Plan your process

The risk assessment life cycle consists of planning, identifying, measuring and prioritizing risk. Defining objectives and scope, establishing clear roles and responsibilities, and maintaining open lines of communication will make the process successful. Consider the following factors to increase the confidence of all interested parties in your risk assessment results.

- Diversity in data, stakeholders and participants
- Technology for accumulating, analyzing and prioritizing risks
- Collaboration with stakeholders for deeper analysis

Identify, measure and prioritize risk

During the risk assessment process, consider both healthcare industry risks and organizational risks.

Healthcare industry risks – The healthcare industry is subject to a substantial amount of risk, including regulatory compliance, and financial and public expectations to lower costs and improve quality of care. Industry risk can most accurately be determined when participants in the assessment process have a general understanding of current trends in the healthcare industry and can discuss how those trends could affect your organization.

Consider creating a summary for discussion. Exhibit 1 provides examples, but is not an all-inclusive list. Topics can be assigned to participants in advance of a scheduled

Exhibit 1 – Example industry trends

Physician employment

Increasing reliance on technology

Telehealth

Changing regulations

High deductible health insurance plans

Shift from Emergency Department to urgent care setting

Payer mix shift away from commercial products

Consumerism

HIPAA enforcement

Labor shortages

Physician practice losses

Aging of population and effect on medical care needs

Mergers and acquisitions

Opioid epidemic

Cybersecurity

Transparency

meeting. Participants can prepare by performing research on their topics and leading discussions on the general trend and how their organization could be affected.

Example discussion points for industry trends

Create a list of discussion points. The following examples may help you get started.

Physician employment

- Are the organization's health systems and hospitals hiring more physicians?
- Do contracts with physicians include clear productivity goals? Does a mechanism exist to reconcile budgeted productivity with actual? Is the practice being tested?
- Do inconsistent practices among decentralized locations result in lost revenue, compliance issues and redundant expenses?
- Do standard operating procedures exist that are being followed by all physician offices?

High deductible health insurance plans

- More than half of employer-sponsored health insurance plans now have a deductible of at least $1,000.
- Increases in out-of-pocket costs for patients create the risk of higher bad debt and charity care for providers, as well as pressure on volumes as patients elect to forgo treatment and elective procedures.
- Has the organization put point-of-service collections into place? How is this being monitored for effectiveness?

Health Insurance Portability and Accountability Act (HIPAA) enforcement

- The Office of Civil Rights is responsible for enforcing compliance with HIPAA laws.
- The highest dollar amount of HIPAA violation settlements occurred in 2018.
- Average settlements are increasing, as is the level of enforcement activity.
- Patient records are an important asset that must be secured by the organization.

Mergers and acquisitions

- New employees may not be familiar with existing policies and procedures.
- Introducing a new culture to the acquired organization will be complex and challenging.
- New users and new systems interfaces create vulnerability for the IT system.

Increasing reliance on technology

- Frequent, significant system changes and upgrades can result in vulnerability in the IT environment, leading to exploitation by unauthorized parties.
- Security incidents could occur and not be sufficiently resolved.
- Lost, stolen or unsecured mobile devices can become compromised.
- Portable media, laptops or desktops with sensitive data can be lost or stolen.
- Users can introduce malware or viruses into the IT environment.

Cybersecurity

- Risk relates to an increasing reliance on technology.
- Many HIPAA breaches are related to cybersecurity attacks.
- Medical records carry a high value on the black market.
- The reputational and economic risk of a cyberattack could extract patient information, or cause systems to malfunction or potentially go offline.

In addition to emerging trends, consider risks specific to the revenue cycle in the healthcare environment: from the admissions process to charge capture to posting of payments. Because the revenue cycle for healthcare providers is a complex set of processes, a breakdown at a single point can significantly affect the organization. Issues in clinical documentation can alter reimbursement and should be examined as part of the organization's risk assessment process.

Organizational risks – To evaluate organizational risks, review the results of prior risk assessments, audit reports and other relevant documentation. Additionally, conduct staff interviews, including the organization's process owners and key leaders. These activities encourage brainstorming and allow measurement of risks against the organization's objectives while prioritizing them in the context of the control environment.

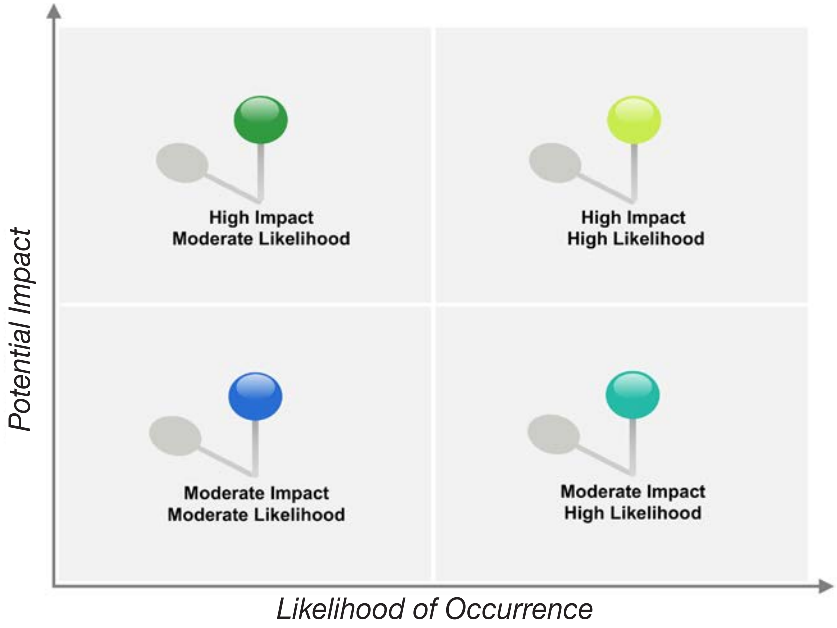
The information gathered from reviewing documentation and interviewing stakeholders will translate into a qualitative, initial risk hypothesis that serves as a basis for further discussion.

When undergoing the risk assessment process for the first time, many organizations struggle with identifying potential risks. Use the sample risk universe in Exhibit 2 to assist in the risk identification process.

Exhibit 2 – Sample organizational risk universe

Financial		
Financial preparation and reporting Budgeting and planning Liquidity Credit/interest rate	Currency Fraud Revenue recognition Payroll	Accounts payable Taxation Commodity pricing
Operational		
Staffing reliability Patient experience Scheduling	Inventory management Procurement Quality of care	Business continuity Pricing Vendor management
Strategic		
Strategic plan and execution Mergers and acquisitions	Strategic relationships and partnerships New business development	Competition Product offering
Technology		
IT project management Logical access	Data availability and integrity Information security	Network connectivity Disaster recovery
Compliance and Legal		
Contractual Regulatory Taxation	Environmental Litigation Record retention	Product liability Organizational policies
Human resources		
Talent acquisition Employee retention Succession planning	Benefits and compensation Performance management Employee development	Knowledge management Privacy
Governance		
Board oversight Organizational reporting	Strategic alignment Organizational structure	Communication Organizational change management

Exhibit 3 – Risk map



In the healthcare environment, a qualitative approach to evaluating and ranking risks maintains focus on the risk assessment's goals rather than distracting from the process with arguable quantification. Rank the organization's risks based on their potential effect on the organization, and on their likelihood (high, moderate, or low) rather than numerical values (for example, 1 for low to 10 for high).

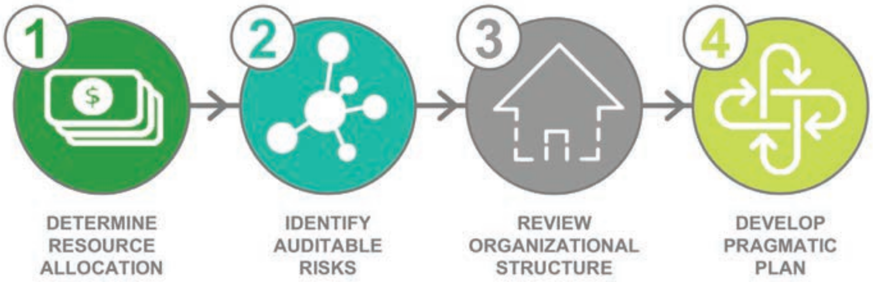
Rankings should consider the context of the organization's control environment, existing policies and potential gaps in accountability. Plot the risks on a grid as illustrated in the risk map in Exhibit 3 and with qualitative and quantitative metrics (e.g., loss of reputation and number of days of downtime).

The risk map offers a starting point to prioritize risks jointly with leadership, and facilitates substantive discussion of risks, their likelihood and impact. If desired, you can facilitate one or two discussions to vet the highest priority risks and their relative placement on the risk map. The risk assessment should include risks identified by process owners, administration, executive leadership and the board audit committee.

Create the plan

A prioritized list of risks enables you to work with management to develop your audit plan. The process outlined in Exhibit 4 requires you to determine available resources, match resources with the identified risks, sort the selected audits by organizational units, and consolidate the audits into an achievable plan. The plan should outline the needed audit activities to address risks and should describe the link between proposed audits and high priority risks to ensure that the proposed activities are clear, understood and relevant.

Exhibit 4 – Plan creation process


1
2
3
4
DETERMINE RESOURCE ALLOCATION
IDENTIFY AUDITABLE RISKS
REVIEW ORGANIZATIONAL STRUCTURE
DEVELOP PRAGMATIC PLAN

A qualitative approach for risks maintains focus rather than distracting with arguable quantification.

Because risk assessments only provide details of risks at a specific point in time, you should work continuously with organizational leadership to regularly update the audit plan to reflect changes in the business and emerging risks.

Determine resource allocation – Collaborate with leadership to determine the funding level and resources dedicated to the internal audit function so the audit plan is tailored to maximize the amount of work performed toward the identified risks. The plan should be scaled and customized appropriately to achieve risk coverage within the available resources. Also, consider the need to recruit talent with healthcare-specific experience, particularly in the areas of revenue cycle and clinical documentation.

Identify auditable risks – Place each risk on a risk map as illustrated in Exhibit 3. Determine whether a risk is auditable, or is an overarching area to monitor and consider in evaluating and auditing other risks.

Review organizational structure – Consider major initiatives or changes of your organization. An audited risk area where significant changes are underway might benefit from deferral to a future period. For example, if a new human resources system is being implemented, auditing that area in a future year or structuring a project with an approach other than a traditional audit may be more effective and appropriate.

Develop a pragmatic plan – Based on the above factors, develop a multi-year audit program and strategy with annual audit plans based on prioritized needs. Include enough scheduling and resource flexibility to accommodate special analyses or ad hoc audit requests to address emerging risks and needs throughout the year, while optimizing time and resource demands on staff.

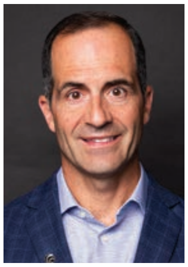
Gain approval – Submit the annual plan to senior leadership and the audit committee for review and approval.

Monitor and update – Ongoing monitoring of risks should occur to keep up with changes. You will be able to continually evaluate your work in the context of new risks and adjust audit activities to keep the focus on critical areas. This approach ensures the best use of resources and enables the audit plan to remain flexible and evolve along with the organization's needs.

Conclusion

Your professional standards and your stakeholders' expectations require you to develop a risk-based plan to ensure that your priorities are consistent with your organization's objectives. Build a robust plan by considering diverse information and collaborating with your stakeholders for deeper analysis. Sharpen your risk assessment focus to add more value and improve your organization's operations. **NP**

Debra Bowes, CPA, is a Partner in Baker Tilly's Healthcare Practice. She has experience with numerous types of financial and compliance audits, including single audits under uniform guidance. Debra can be reached at Deb.Bowes@bakertilly.com and (570) 651-1741.



Mark Laccetti, CPA, CGMA, is a Partner in Baker Tilly's Risk, Internal Audit and Cybersecurity Practice. He has experience in performing business process risk assessments and conducting operational, financial, and compliance audits. Mark can be reached at Mark.Laccetti@bakertilly.com and (215) 557-2217.

I think all good reporting is the same thing—the best attainable version of the truth.
- Carl Bernstein