Feature

Build a Solid Compliance Work Plan: How Risk Assessment Helps

By Leah Guidry, JD, MA and Dwight Claustre, CHC, CHRC

Executive Summary

Our article provides the components and process for developing a healthcare compliance risk assessment. From start to finish, the article assists the compliance professional and others with developing a risk assessment process to fit an organization’s needs. Beginning with the definition of risk assessment (What), the authors walk the reader through the basis of the assessment (Why); the best timing for conducting the assessment (When); the identification of the personnel and levels that should be consulted (Who); and finally, addresses the process of conducting the assessment (How).

Introduction

Healthcare compliance risk assessments provide the basic framework for an effective compliance work plan. As such, risk assessments should be every compliance program’s first step in developing the annual work plan. Using a formal compliance risk assessment methodology assures your management that “inquiring minds” have considered the organization’s risks and prioritized them for review.

What is a compliance risk assessment?

A risk is an event that, if it were to occur, would have a material consequence on an organization’s ability to achieve objectives. A risk assessment, conducted for a healthcare compliance program, is the identification, measurement, and prioritization of compliance risks. A compliance risk assessment is not as broad as an enterprise risk assessment. The compliance risk assessment’s focus is solely on the risks affecting the organization as a result of its healthcare operations (e.g., HIPAA, the business of billing and coding processes, etc.) as opposed to those types of risks that exist by virtue of conducting any type of business operations (e.g., financial fraud, human resource regulatory requirements, etc.). Narrowing the field of risk in this manner will enable a more streamlined approach to the risk assessment process.

Why should a compliance risk assessment be done?

Conducting a compliance risk assessment enables the efficient use of compliance resources; justifies the extent of oversight exercised in particular areas; and provides a methodical, measured, and proactive approach to the work of the compliance department. Additionally, government bodies/regulators have indicated in their guidance materials that risk assessments are a part of the government’s expectation.

Without a thorough risk assessment process, the compliance department puts itself in a reactive position by having to respond to issues as they are uncovered or reported (e.g. more of a crisis operational mode). Employing a risk assessment approach, the compliance department seeks out issues and assesses their importance and then prioritizes them in relation to other identified risks.

Conducting the risk assessment process is a logical and methodological means of deploying the compliance resources that fit the needs of the organization, rather than throwing resources at the current crisis. Such a process enables the compliance department to justify the use of corporate resources to address and mitigate known risks.

However, the risk assessment is a first step to a proactive compliance plan. The implementation of the other components of the compliance program (education, monitoring, auditing, etc.) completes the proactive approach.

When should a risk assessment be performed?

If your organization has never completed a formal risk assessment, now is the time! The compliance risk assessment should be completed annually as part of the annual compliance work plan development. The Office of Inspector General’s (OIG) Work Plan is published each year in the fall and marks a good time for the compliance department to engage in the annual risk assessment process. The OIG Work Plan provides some detail on content areas the compliance department will need to address. As such, it provides a good “head start” for the identification part of the risk assessment.

To effectively use the OIG Work Plan, review the document for areas of focus that correspond with areas services your institution provides. For instance, the 2010 OIG Work Plan includes a
The actual facilitator of the compliance internal audit functions depends on how coordination between the compliance and assessed and addressed. The degree of that the concerns of the audit function are work closely with internal audit to ensure cases, the compliance department will the compliance risk assessment. In some the lead in organizing and overseeing the compliance department should take the work plan should allow for additions and adjustment of staff time to address new issues as they arise.

Who should perform the risk assessment?

The compliance department should take the lead in organizing and overseeing the compliance risk assessment. In some cases, the compliance department will work closely with internal audit to ensure that the concerns of the audit function are assessed and addressed. The degree of coordination between the compliance and internal audit functions depends on how they allocate their efforts generally.

The actual facilitator of the compliance risk assessment should be someone in the organization who has experience guiding groups to achieve common goals. If this expertise does not exist within the organization, the use of outside resources is an option to consider. If a facilitator from outside of the compliance department or organization is used for the risk assessment, they should take direction from the compliance department.

Regulatory Guidance that Speak to the Need to Conduct Risk Assessments

OIG Compliance Program Guidance for Hospitals 1998

“The OIG recommends that when a compliance program is established in a hospital, the compliance officer, with the assistance of department managers, should take a ‘snapshot’ of their operations from a compliance perspective. This assessment can be undertaken by outside consultants, law or accounting firms, or internal staff, with authoritative knowledge of health care compliance requirements.” 63 Fed. Reg. 8987, 8996 (Feb. 23, 1998).

OIG Supplement Compliance Program Guidance for Hospitals 2005

“Has the hospital developed a risk assessment tool, which is re-evaluated on a regular basis, to assess and identify weaknesses and risks in operations? Does the risk assessment tool include an evaluation of Federal healthcare program requirements, as well as other publications, such as the OIG’s CPGs, work plans, special advisory bulletins, and special fraud alerts?” 70 Fed. Reg. 4858, 4875 (Jan. 31, 2005).

US Federal Sentencing Guidelines, Chapter 8—Sentencing of Organizations

The U.S. Sentencing Commission published amendments to the U. S. Sentencing Guidelines on November 1, 2010 that include an amendment related to effective compliance and ethics programs. Included in this section (§8B2.1) is a provision that requires the organization to “periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement... to reduce the risk of criminal conduct identified through this process.” A link to Chapter 8 of the guidelines is found at: http://www.ussc.gov/Guidelines/2010_guidelines/Manual_PDF/Chapter_8.pdf

To some degree, the personnel chosen for participation will be dependent on your organizational structure. At a minimum, managers from the following areas and selected members of their staff should participate:

- Compliance Team
- Legal
- Patient Financial Services (billing)
- Administration
- Health Information Management
- Pharmacy and other ancillaries
- Laboratory
- Risk Management
- Charge Description Master Team
- Admitting/Registration
- Human Resources
- Quality
- Nursing
- Medical Staff

Involving individuals from these areas enables the compliance department to gain valuable insight into the issues they face and the degree to which established controls will mitigate risks as they arise. The purpose of the risk assessment is to identify particular risks and assess which risks have effective mitigating controls in place. From this, you should be able to determine how much oversight the compliance department should allocate to addressing risk.

Staff level personnel know how the processes actually work, as opposed to how the policy and procedure state they are supposed to work. This is why it is important to involve the front line staff in your risk assessment activities. The most appropriate use of these individuals is to help understand the current processes, challenge assumptions, and test the strength of internal controls.

What is compliance risk?

The question most frequently asked by those participating in a risk assessment is, “What is a compliance risk?” All too often, people will begin listing personal issues or concerns that are not necessarily compliance risks, but rather issues that they believe are important to address. To maintain clarity and efficiency, it is imperative that the risk assessment is guided by a common definition, including examples, of compliance risk. Making the distinction between compliance risks
and general business/enterprise risks, will provide assistance in developing and maintaining the necessary compliance risk assessment focus.

Generally speaking, compliance means adhering to a standard, policy, or law. Regulatory compliance deals with ensuring that the personnel of an organization are educated with respect to applicable laws and regulations, and that good faith efforts are made to comply with them consistently. Compliance risk, then, is the likelihood an applicable law or regulation may be violated.

Healthcare compliance risks are those issues, events, and situations that present themselves by virtue of being a healthcare provider. These include such laws and regulations as HIPAA/HITECH, EMTALA, billing and coding, Stark and Anti-Kickback, etc.

Once the definition is grasped, you should encourage the individual(s) to draw on their knowledge and experience to determine what the compliance risks are for the organization. To get the discussion started, the project leader/facilitator should be prepared with examples of several typical kinds of risks. It can be useful to ask personnel to come prepared with their own top three to five compliance concerns, and to be prepared to discuss these in the session.

If you employ facilitated group sessions, it is advantageous to include a mix of personnel from different departments in the organization. The variety permits a discussion of issues from various perspectives that can illuminate issues and controls, as discussed below.

Regardless of the approach used, you will want to ask a number of questions. The following three open-ended questions should be included:

- What can go wrong?
- Where is our organization most vulnerable?
- What are the issues that concern you the most?

**How to do a risk assessment**

In many cases, healthcare work is a top-down process. The physician determines the patient’s diagnosis and sets the course for treatment. Then, all other disciplines (nursing, lab, pharmacy, etc.) apply their discipline and training to treat the patient, but always in accordance with what the physician has determined to be the right approach.

**Examples of Compliance Settlements with the Federal Government**

Government enforcement of healthcare fraud, waste, and abuse, drives many compliance program activities and helps to determine the risks that need to be addressed. Tracking and analysis of enforcement actions help compliance professionals determine what risks to assess for their institution. As such, risks are not assessed in a vacuum or solely based on internal data, but are assessed in accordance with the broader panoply of government actions.

The following are examples of settlements during just the past two years. If the organizations had conducted a thorough compliance risk assessment, they may have uncovered these issues and avoided the cost of the settlement. Also, they may have avoided the costs of defending their cases along with the resulting corporate integrity agreement requirements (e.g., Independent Review Organization, legal counsel guidance, etc.).

**Stark and Kick-back Settlements**

$30 Million Detroit Medical Center—Detroit, MI December 2010

As part of their due diligence to purchase the Detroit Medical Center, Vanguard Health System uncovered office lease agreements and independent contractor relationships that were either inconsistent with fair market value or not put in writing, violations of the False Claims Act, the Anti-Kickback Statute and the Stark Statute, according to the Department of Justice.

$14 Million Omnicare, Mariner, GA November 2009

The government alleged that Omnicare and other co-conspirators paid kickbacks to keep future business flowing to the Omnicare pharmacy.

$3.3 Million Christiana Care Health System, DE March 2010

The government alleges the hospital overpaid a group of neurologists for the reading and interpretations of encephalograms as a reward for hospital referrals.

$1.5 Million Rush University Medical Center, IL March 2010

The government alleges that Rush billed Medicare for services provided by physicians at the time when there were non-compliant lease arrangements in place.

**Medical Necessity Settlements**

$886,000 Yale-New Haven Hospital, CT July 2009

The government alleges, instead of performing Gamma Knife procedures on an outpatient basis, the hospital admitted the patients for overnight stays and billed Medicare for inpatient admissions that were not medically necessary.

$846,000 Wheaton Community Hospital, MN January 2010

The government contended that, from 1998 to 2004, Wheaton Community Hospital admitted some patients and kept others admitted to acute care when doing so was not medically necessary. The defendants then billed Medicare for the cost of these hospital admissions.

**Billing Settlements**

$2 Million West Valley Imaging, NV March 2009

The government alleged that the defendants submitted false or fraudulent claims to Medicare by improperly providing diagnostic tests to Medicare beneficiaries. The required treating physicians’ orders were absent, billing for certain tests under CPT codes were not supported by the medical records, and certain other Medicare billing and coverage requirements were not satisfied.

**Research Settlements**

$2.6 Million Weill Medical College March 2009

Weill Medical College of Cornell University settled fraud allegations that it defrauded the government in connection with federal research funds awarded under grants made by the National Institutes of Health, and the Department of Defense.
The compliance risk assessment, on the other hand, is a process that gathers data from the bottom-up. The personnel closest to the transaction details can provide you with the best perspective and help to quantify and qualify the risks.

The process of gathering risk data can be done in a variety of ways, but each approach entails eliciting information from people in the organization. Horizontal and vertical data gathering should be used. In other words, senior management and front line staff (vertical) should be included in the data gathering process as well as personnel from various (horizontal) departments (e.g., care delivery, medical staff, ancillary and support departments).

The means of data gathering will depend on the resources available. Survey tools, facilitated group sessions, and individual interviews (or a combination of all of the above) can be useful for the data gathering stage.

Risk identification
The first step in the assessment process is to identify the risk. You can accomplish this by listing the risks that the group or interviewee came prepared to discuss. When the participant(s) seem to have difficulty identifying issues, the facilitator/interviewer should ask about:
- Issues gleaned from the OIG Work Plan.
- Government enforcement trends.
- The facility’s own history of government enforcement.
- The knowledge of the care delivered within the facility.

When a complete list of identified risks is compiled, the list can be used in the next step of the process, which is measurement.

Risk measurement
The purpose of the measurement step is to determine:
- The impact and extent of each risk.
- The degree of vulnerability that the organization faces with respect to each risk.
- The strength of the controls currently in place to mitigate each risk.

For each identified risk, you will need to work with the group or interviewee to measure the degree of concern or risk impact. You will also need to determine the issue’s potential level of impact in three specific areas:
- Legal impact
- Financial impact
- Impact on the organization’s reputation

Next, you should determine your organization’s vulnerability with respect to each risk, including the likelihood that the risk would occur and how detectible the risk would be if it did occur. If a risk is likely but easy to detect, it might map lower on a resulting heat map. But if the risk is likely, but hard to detect, it will be one that needs greater attention on the resulting work plan.

Risk control
Lastly, you will need to determine controls that are in place to mitigate each risk. Understanding controls that exist and the effectiveness of those controls to mitigate a risk is one of the most important elements of the analysis. A risk may be high and the organization may be vulnerable to the risk, but if effective controls are in place, the likelihood of occurrence is minimized. Conversely, the failure of controls can enhance the probability of occurrence.

The benefit of using group sessions is that they are an effective means of identifying controls that exist along a continuum. Persons at the beginning of a process might unwittingly believe that controls are in place at the end of the process to address errors or problems. By including personnel from along the entire continuum of a process, you can highlight erroneous assumptions, thus providing clarity to the group as to whether or not the identified risk is actually mitigated.

Risk prioritization
When compliance risks have been identified and measured, they need to be prioritized. In most cases this process flows naturally from the measurement discussion. However, if the size of the organization has required numerous group sessions or the risk assessment has been conducted with surveys or individual interviews, the facilitator must aggregate the data and develop a final prioritized list. The items on the final list should be categorized into low risk items, midlevel risk items, and high risk items.
High risk items will be those that people raise repeatedly, are hard to detect, have a high likelihood of occurrence, or will have a significant impact if they were to occur. Moderate risk items might be those that are frequently mentioned, but have high or moderate detectability scores. Lower risk categories are unlikely or those that could be likely, but would have a low impact upon occurrence.

Clearly, the high risk items will take precedence in the development of the annual compliance (or audit) work plan. Depending on your time availability during the year, you may want to add some of the medium-level risks to the plan. When developing the work plan, be judicious in apportioning resource availability to risk issues to be addressed. You will likely not be able to address everything you would like to. Additionally, reserve some staff time to address urgent issues as they arise during the year.

**Testing the Controls**

Before the process is completed, the identified controls that allegedly mitigate or detect the designated compliance risks should be tested. Testing these controls is a crucial step in making sure that the prioritization of the categorized risk list is accurate as possible.

Testing the controls is essentially a process in which the group’s discussion of the strength of the control is validated or invalidated through observation. Testing can be carried out by having non-interested parties (i.e., people from other departments, outside advisors, etc.) confirm by observation that the control is in place and works properly. Depending on the extent of risk and the importance of the control, it may be necessary to perform structured testing to confirm the control catches various scenarios.

If the control can be validated as effective, then no changes to the risk prioritization are necessary. However, if the control is either not in place as expected, or is not as effective as believed, the risk will need to be re-prioritized and a stronger control implemented.

**Summary**

The importance of conducting a formal compliance risk assessment and to continually review and update the compliance work plan is critical to a thoughtful compliance program. Compliance work plans can be created in a vacuum using external resources and compliance department experience. Yet, such a detached endeavor does not provide the value achieved through the active engagement of the organization. Scoping out the project, getting the right people to the table, and following a methodical approach are all keys to a successful product. NP

---

**Authors**

Leah Guidry, JD, MA, is a Managing Director in Huron Consulting Group’s Healthcare Compliance & Investigations Practice. She has more than 20 years of experience working with healthcare systems, hospitals, academic medical centers, physician groups, and pharmaceutical and device manufacturers. Leah works out of Huron’s Washington, DC office. You may reach her by email at lguidry@huronconsultinggroup.com or by telephone at 202-250-4679.

Dwight Claustre, CHC, CHRC, is an independent contractor in Phoenix, AZ with 31 years of experience working with hospitals and healthcare systems in the areas of compliance, operations, and risk management. Dwight previously served as the system compliance director for Catholic Healthcare West, a 40-hospital system based in San Francisco, California. You can reach Dwight by email at dwightclaustre@yahoo.com or by telephone at 623-866-9106.

---

**An Inside Perspective on Managing Risk — continued from page 41**

Directors are key internal stakeholders who expect much from their internal auditors—not the least of which is quality. Internal auditors have the opportunity to demonstrate their quality by implementing a Quality Assurance and Improvement Program, which lays out a step-by-step plan for excellence. In addition to conducting ongoing and periodic internal assessments, the internal audit activity must undergo an external quality assessment (QA) every five years, in order to be in conformance with the Standards. In addition to indicating a willingness on the part of the internal auditors to undergo the same scrutiny, they devote to all other aspects of the organization, the external QA thwarts the risk of complacency and ensures continual improvement of the internal audit activity.

In short, it’s safe to say that no function brings greater value to an organization’s risk management process than does its internal audit activity. For more information, please visit www.TheIIA.org. NP

Richard Chambers, CIA, CGAP, CCSA, President & CEO, leads The IIA Global Headquarters’ leadership team in developing the global business infrastructure and framework that supports The IIA’s 96 institutes all around the world and advances the organization’s strategic priorities. He initiates partnerships with other global groups and works to ensure internal audit competencies are globally consistent and the International Standards for the Professional Practice of Internal Auditing are globally recognized and embraced. Under his direction, The Institute has enhanced and launched new services to address urgent needs facing CAEs and has substantially increased the caliber of timely internal audit thought leadership. For more information you may reach The IIA at www.theiia.org or by telephone at 407-937-1200.