Performing a Compliance Risk Assessment for Compliance Auditing & Monitoring in Healthcare Organizations

Author: Glen C. Mueller, Chief Audit & Compliance Officer, Scripps Health, San Diego, CA

Introduction

A focus group of Health Care Compliance Association (HCCA) and Association of Healthcare Internal Auditors (AHIA) members has been meeting to explore opportunities to better define and explain auditing and monitoring, clarify the roles of compliance and internal audit functions as they address issues within their healthcare organizations, and develop guidance/materials on key aspects of healthcare auditing and monitoring processes. One of the key HCCA/AHIA team initiatives is to use the *Seven Component Framework* as a guide in considering the important components of a comprehensive auditing and monitoring process. The *Seven Component Framework* for compliance auditing and monitoring is comprised of the following:

- Perform a risk assessment and determine the level of risk
- Understand laws and regulations
- Obtain and/or establish policies for specific issues and areas
- Educate on the policies and procedures and communicate awareness
- Monitor compliance with laws, regulations, and policies
- Audit the highest risk areas
- Re-educate staff on regulations and issues identified in the audit

This article examines the process of performing a compliance risk assessment and evaluating the level of risk as a means to assist compliance and internal audit functions in determining where to most effectively focus their auditing and monitoring efforts. In addition, this article discusses the benefits of organizations establishing an ongoing Enterprise Risk Management (ERM) process to facilitate better understanding and identification of risks by a cross-functional team. It is the second in a series of articles being prepared by the HCCA/AHIA auditing & monitoring focus group.

Risk Assessment and Evaluation

The responsibility for collecting, assessing, and evaluating the broad spectrum of risk assessment relevant information is generally the responsibility of multiple individuals and different functions throughout the organization. To effectively understand the aggregate relationships and implications of the information identified, most organizations would benefit from some form of an Enterprise Risk Management process to provide for a “group think” and from a full set of perspectives to assess relevant risks, understand inter-relationships of risk indicators, and determine risk mitigation and control activities.

The recently released Committee of Sponsoring Organizations (COSO) Enterprise Risk Management model elaborates on the following advantages of a more comprehensive and process view of risk management:

- Takes note of interrelationships and interdependencies among risks.
- Offers improved ability to manage risks within and across business units.
- Improves capacity to identify and seize opportunities inherent in future events.
- Considers risk in the formulation of strategy.
- Applies risk management at every level and unit of an entity.
- Facilitates communication by providing a common risk language.
- Takes a portfolio view of risks throughout the enterprise.

The new COSO ERM model specifies eight components for an ongoing process that include Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information and Communication, and Monitoring.

The American Society for Healthcare Risk Management (ASHRM) has also recently formalized an ERM Framework and restructured its 2004 edition of the *Risk Management Handbook for Healthcare Organizations* around this concept. ASHRM subscribes to the basic tenet that "risks do not exist or behave in "isolation" but can be identified, grouped, and catalogued in "risk domains". The six risk domains of the ASHRM framework are Strategic, Operational, Financial, Human Capital, Legal and Regulatory, and Technology.

Organizations should evaluate the COSO and ASHRM Enterprise Risk Management frameworks as guidelines and resources for how to establish a process that makes sense for the organization and establish an ERM program that builds on and pulls together existing processes for a more coordinated assessment of risks.

Absent a formalized ERM process, the Chief Compliance Officer and Chief Audit Executive should annually co-sponsor a risk assessment process, including others in key risk related roles, to facilitate the development of their respective annual plans from a risk-based perspective. Completing this process should result in an improved compliance risk assessment and provide for a more informed approach on how best to utilize both compliance and internal audit resources.

This article identifies and elaborates on the following phases of risk assessment and evaluation:

- Determine the Scope and Preliminary List of Compliance Risks to be Assessed
- Identify Your Organization's Key Compliance Risk Related Data
- Finalize Set of Risks to be Assessed
- Evaluate Control Activities and Level of Risk Mitigation
- Calculate Risk Concern Level and Rank Risk Areas
- Confirm Risk Evaluation Results with Senior Management and Compliance Committee
- Prepare Performance Improvement Action Plan

- Review Compliance Risk Assessment Results with Board Oversight Committee
- Incorporate Risk Assessment Results into Compliance and Internal Audit Planning

Determine the Scope and Preliminary List of Compliance Risks to be Assessed

Start a compliance risk assessment process by determining an initial list of compliance risks to be assessed, as this will facilitate identification of risk related data to be gathered and evaluated. This initial list of risks will likely be expanded after reviewing a variety of compliance risk related data such as that shown in the next section. Declaring the intended scope of risks to be considered early in the process provides notice to senior management and the board of directors as to what is not being considered.

Examples of fifteen categories/types of compliance risks that might be included in a compliance risk assessment are as follows:

1. Not complying with requirements of a Corporate Integrity Agreement or Settlement.
2. Using an excluded physician, employee, or vendor.
3. Submitting a claim to a government payor for a service not medically necessary.
4. Submitting a claim to a government payor for a service not performed.
5. Submitting an inaccurate or inadequately documented claim to a government payor.
6. Making improper payments to physicians.
7. Failing to timely and accurately meet external reporting requirements.
8. Not complying with HIPAA Privacy regulations.
9. Not complying with HIPAA Security regulations.
10. Not evaluating or considering relevancy of OIG Annual Work Plan components.
11. Improper handling and disposal of hazardous waste.
12. Not complying with Human Subjects Protection requirements for clinical trials.
13. Inadequate reporting and monitoring of conflicts of interest.
14. Not completing prior years plan for compliance auditing and monitoring.
15. Individuals voicing compliance concerns directly to OIG or media, instead of compliance.

Identify Your Organization's Key Compliance Risk Related Data

One of the important tasks in performing a compliance risk assessment is to identify relevant sources of information to be considered in determining your organization's business units, departments, processes, and information systems that represent the highest compliance risk to your organization. Risk related data sources and measures can be thought of in terms of the following nine broad categories of information.

- Revenue Cycle Information (with focus on government payors)
- Surveys / Independent Feedback on Operations
- Events Metrics
- Financial Metrics
- Insurance and Lawsuit Claims
- External Reviews
- Strategic Plans
- Technology Risks
- Corporate-wide Performance Dashboards

Traditionally compliance functions have focused on only a subset of the Revenue Cycle metrics and information. Our focus group believes it is essential to evaluate a fuller set of enterprise-wide risk data, as outlined below, since many can have a direct impact on the assessment of relative compliance risks. For example, when you combine the metrics of department turnover with Medicare/Medicaid percentage of total revenue by department, those departments with the profile of *high turnover / high percentage of Medicare/Medicaid revenue* have a higher compliance risk due to greater likelihood of temporary and new staff not being as familiar with policies and procedures, possible disgruntled "whistleblower" staff, and increased opportunity for errors. We suggest over forty types and sources of information, to be considered in a compliance risk assessment, which should be supplemented with additional information specific to your organization.

Revenue Cycle Information (with focus on government payors)

- OIG Annual Work Plan related initiatives
- Degree of compliance with corporate integrity agreement requirements
- Billing claims denials by department
- Medicare/Medicaid percentage of total revenue by department
- Coding accuracy statistics and trends
- Trends in government payor mix by department and specialty
- Utilization reports by DRG and CPT codes
- Physician billing - Medicare Development Letters
- Results of reviews by Fiscal Intermediary or other reviewers
- Government payor credit balances / trends
- Internal audits and compliance reports and status of corrective actions

Surveys / Independent Feedback on Operations

- Patient satisfaction surveys/polls
- Employee satisfaction surveys/polls
- Physician satisfaction surveys/polls
- Periodic survey/interviews of senior management as to greatest risks

Events Metrics

- Occurrence reporting (patient care and employee safety statistics)
- Compliance Hot-line calls
- Compliance issues reported directly to compliance and internal audit
- Adverse Drug Events statistics
- Patient complaints logs
- Staff turnover by department
- Sick time/absenteeism by department
- Percentage of traveler and registry nurses vs. full time employees
- Number of clinical trials/protocols

Financial Metrics

- YTD budget variances by business unit and department
- Sarbanes Oxley Section 404 Internal Controls Review – Action Plan
- Overtime by department
- Liquid assets (cash, inventory) by department
- Amount of Federal grants & contracts included in A-133 Audit
- Amount of contract staff versus employed staff

Insurance and Lawsuit Claims

- Worker compensation claims by department
- Crime-theft policy claims
- Property damage claims
- Medical malpractice claims
- Lawsuits by department

External Reviews

- Consultants reports
- Feasibility studies
- Surveys by state regulatory agencies
- JCAHO reviews
- Independent auditor's (CPA Firm) annual management letter

Strategic & Capital Plans

- Review risks from new acquisitions
- Determine special risk considerations from large system implementations
- Consider risks of new business arrangements such as outsourcing
- Evaluate construction projects for financial and community reputation risks
- Consider risks associated with not meeting certain strategic objectives

Technology Information

- Business continuity and disaster recovery vulnerability
- Bio-medical equipment
- Extent of E-commerce and need for protection of customers confidential data
- HIPAA Privacy and Security regulations vulnerability
- Implementation of new software/hardware risks

Corporate-wide Performance Dashboards

- Assess implications and associated risks with "warning" signs
- Identify new risks and emerging risks
- Compare yourself to "like" organizations

Finalize Set of Risks to be Assessed

Solicit the input of others in your organization using the preliminary list of compliance risks and risk related information gathered. First, review OIG work plans from past three years and have both compliance and internal audit staff do the same. Then, solicit input and review risk-related data and information gathered

Second, interview senior management and managers in key compliance related roles, using a questionnaire based on information gathered previously. Complete interviews with senior management and key managers obtaining their input on critical compliance risks; obtain their confidence level in risk mitigation control activities; and identify other factors/considerations.

Evaluate Control Activities and Level of Risk Mitigation

Once the set of compliance risks to be assessed has been determined, the next step is for a knowledgeable group of individuals (ERM committee or risk oversight group) to evaluate relevant risk related information, control activities, and results of interviews to determine the extent the organization is mitigating each risk.

Calculate Risk Concern Level and Rank Risk Areas

There is not one generally accepted approach to calculate Risk Concern Level. However, many approaches consider some type of mathematical weighting process for likelihood, impact, and risk factor (percent unmitigated). Both objective and subjective measures come into play so the two most important parts of the evaluation are consistency in application of the process and the multi-disciplinary "group think". With the benefit of the risk related information gathered, a risk oversight group can usually reach consensus as to the areas with the highest risk concern levels that should be given priority for monitoring, auditing, and the implementation of additional control activities. Key terminology used in this assessment process is as follows:

Likelihood:	Inherent probability of a risk occurring, without considering existing controls.
Impact:	The potential significance of a risk, without considering existing controls.
Risk Factor:	The estimated percentage of unmitigated risk.

The risk oversight group for each organization should assign risk scales or categories, such as high/medium/low, 1-5, or 1-10 for likelihood and impact along with criteria for the scale ratings. This allows the risks to be categorized and prioritized to permit both better focus and more cost-beneficial mitigation. The Risk Factor is 100% minus the confidence level that control activities or other factors will effectively mitigate a risk occurrence or impact. Examples of how confidence level of percentage mitigated might be assigned are 95% for a computer calculation, 75% where process controls are strong and consistently applied, and 25% where controls are minimal or are not effective.

The calculation for each risk's concern level can be expressed as:

(Likelihood) X (Impact) X (Risk Factor) = Risk Concern Level

For example, a compliance risk with high likelihood, high impact, and 75% confidence level in the mitigating controls (using scale of 1-10 for likelihood and impact) would be assigned a Risk Concern Level as follows: 9 X 10 X (100-75) % = 22.5 Risk Concern Level

There is a great deal of subjectivity in assigning values to the three factors used in the Risk Concern Level determination, which makes it critical to have enough experienced individuals directly involved in this process. An outside resource, such as consultant that performs risk assessments at different organizations or a peer compliance professional, can provide additional value and perspective.

Confirm Risk Evaluation Results with Senior Management and Compliance Committee

Present and discuss results of risk evaluation with the Corporate Compliance Committee and other group of senior executives, not part of the risk oversight group, to confirm the "corporate risk appetite"; test the reasonableness of designated risk likelihood, risk impact, and risk mitigation factor for each of the risks selected for evaluation; and ratify the areas deemed to have highest Risk Concern Levels. It is important to note that this assessment does not focus on re-evaluating each risk since the individuals involved confirmed the assessment approach. However, the highest risks should be agreed upon as such relative to the other risks identified.

Prepare Performance Improvement Action Plan

Conducting an enterprise risk assessment or compliance risk assessment will result in the identification of opportunities for improvements in terms of revising or implementing policies, adding control activities, or the need for additional education and awareness of issues. These opportunities should be formalized into a Performance Improvement Action Plan with assigned responsibility and timelines. This action plan could be treated as an audit report for follow-up purposes or included as an appendix to the annual compliance plan and reviewed periodically by the compliance committee.

Review Compliance Risk Assessment Results with Board Oversight Committee

It is important for Board committee(s) overseeing the internal audit and compliance functions to be educated on the customized compliance risk assessment process that is followed by the organization and to understand how this assessment impacts the focus of audit and compliance efforts.

Incorporate Risk Assessment Results into Compliance and Internal Audit Planning

The results of the compliance risk assessment process will provide valuable input in preparing for and prioritizing compliance monitoring and auditing activities. Where possible, the risk assessment process should coincide with the planning cycles for your organization's corporate compliance plan and annual internal audit plan.

About the HCCA / AHIA Auditing and Monitoring Focus Group

The HCCA/AHIA auditing and monitoring focus group will be developing a series of additional articles regarding the seven components to expand on the roles of compliance and internal audit functions, provide detailed "how to steps", and discuss the essential coordination links between compliance, internal audit, legal, and management that are necessary for each component.

Members of the HCCA / AHIA focus group are:

- Randall K. Brown, Baylor Health Care System Dallas, TX, RandalBr@BaylorHealth.edu
- Britt H. Crewse, Duke University Health System Durham, NC, crews012@mc.duke.edu
- Al W. Josephs, Hillcrest Health System, Waco, TX, al.josephs@hillcrest.net
- Glen C. Mueller, Scripps Health , San Diego, CA, Mueller.glen@scrippshealth.org
- Debi J. Weatherford Revenue Cycle Solutions, Marietta, GA, debi.weatherford@revenuecycle.net

The next two priorities for the focus group will be to publish articles and guidance materials in December 2004 and January 2005 on (1) key compliance monitoring activities with references to applicable laws and regulations and (2) providing compliance auditing methodologies, tools and techniques.