HCCA Compliance Institute – Las Vegas, NV

Session S206

Monday April 24, 2006, 1:30-2:30pm

Conducting a Compliance Risk Assessment

Randall K. Brown, CIA
Baylor Heath Care System
RandalBr@BaylorHealth.edu

Glen C. Mueller, CPA, CIA, CISA
Scripps Health
mueller.glen@scrippshealth.org

Risk Assessment and Evaluation

Most healthcare organizations would *benefit from a more comprehensive* compliance risk assessment process using more of an Enterprise Risk Management perspective and process.

Our approach to compliance risk assessment *provides for a greater set of perspectives to assess relevant compliance risks*, understand inter-relationships of risk indicators, and "*group think*" of subject matter experts to identify/ determine risk mitigation and control activities.

Why Conduct a Comprehensive Compliance Risk Assessment?

- Because you are a responsible healthcare audit/ compliance professional that recognizes the importance of identifying those risks that are most relevant to your organization.
- It leverages the combined knowledge and perspectives of Compliance, Internal Audit, and others, resulting in a more informed approach on how to best utilize their respective resources.
- It allows you to focus your monitoring and auditing activities on the highest priority areas.
- Demonstrates a proactive approach to minimize the likelihood that you will receive an unexpected visit from the OIG or other regulatory agency.

What is Different about a Comprehensive Compliance Risk Assessment?

It is an expanded way of thinking about your risks by combining the frameworks of:

- the COSO ERM Model

- the risk framework of the American Society for Healthcare Risk Management.

.

COSO - Key Elements that Characterize ERM

- **Takes note of interrelationships and interdependencies among risks.**
- **Offers improved ability to manage risks within and across business units.**
- **Improves the organization's 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.**

COSO - Eight Components
(comprising an ERM Program)

- **Internal Environment**
- **Objective Setting**
- **Event Identification**
- **Risk Assessment**
- **Risk Response**
- **Control Activities**
- **Information and Communication**
- **Monitoring**

COSO – ERM is built on the *COSO Internal Control–Integrated Framework*

The *ERM Framework* includes <u>three additional components</u>:

objective setting,

event identification, and

risk response,

and the five components taken from the COSO internal control model are broader in their descriptions and in terms of the practical guidance.

Risk Management Handbook for Healthcare Organizations

The 2004 Fourth Edition of the

Risk Management Handbook for Healthcare Organizations *

The Handbook Task Force and senior leadership for the American Society for Healthcare Risk Management (ASHRM) have adopted the concept of ERM as the foundation for this edition of the handbook and encourage all interested in the profession of healthcare risk management to take the next step towards enterprise risk management.

* **(1,350 pages)- Published by Jossy-Bass, ISBN 0-78-79-6797-1 (**www.josseybass.com**)**

ASHRM Defines Risk Domains

ERM Consideration:

Risks do not exist or behave in "isolation" but can be identified, grouped, and catalogued in risk domains.

Risk Domains:

- **Strategic**
- **Operational**
- **Financial**
- **Human Capital**
- **Legal and Regulatory**
- **Technology**

Ten Phases of a Comprehensive Risk Assessment and Evaluation Process

1. Determine the Scope and Preliminary List of Compliance Risks to be Assessed
2. Identify Your Organization's Key Compliance Risk Related Data
3. Finalize Set of Risks to be Assessed
4. Evaluate Control Activities and Level of Risk Mitigation
5. Calculate Risk Concern Level and Rank Risk Areas

Ten Phases of Risk Assessment and Evaluation Process (continued)

6. Identify and Categorize Key Compliance Program Controls
7. Identify Control Gaps and Deficiencies
8. Confirm Risk Assessments Results with Subject Matter Experts, Senior Management, Compliance Committee, and Board Oversight Committee
9. Prepare Performance Improvement Action Plan and Follow-up Process
10. Incorporate and Translate Risk Assessment Results into Compliance and Internal Audit Planning

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

Start your compliance risk assessment process by determining a *preliminary list of compliance risks* to be assessed, as this will facilitate identification of risk related data to be gathered and evaluated.

1. Determine the Scope and Preliminary List of Compliance Risks to be Assessed (cont'd)

Preliminary List of Compliance Risks to be Assessed

1.	Your current year Compliance Department Plan for compliance auditing and monitoring is not substantially completed.
2.	Conflicts of Interests not adequately monitored and mitigated.
3.	Your Compliance Program is ineffective.
4.	Excluded physician, employee, or vendor is used.
5.	External regulatory annual reporting requirements are not met in terms of accuracy and timeliness.

1. Determine the Scope and Preliminary List of Compliance Risks to be Assessed (cont'd)

Preliminary List of Compliance Risks to be Assessed

6.	External regulatory event reporting requirements are not met in terms of accuracy and timeliness.
7.	Medicare Conditions of Participation non-compliance.
8.	OIG Annual Work Plan components not adequately evaluated and considered.
9.	OIG Settlement or Integrity Agreement provisions non-compliance.
10	Physicians receive improper payments or other types of financial gain

1. Determine the Scope and Preliminary List of Compliance Risks to be Assessed (cont'd)

Preliminary List of Compliance Risks to be Assessed

11.	Improper Relationships with Federal Health Care Beneficiaries.
12.	Privacy and Security regulations non-compliance.
13.	Whistleblowers voicing concerns directly to OIG or media, instead of compliance department
14.	Human Subjects Protection non-compliance with requirements for clinical trials.
15.	Claims submitted to a government payor are not correctly coded.

1. Determine the Scope and Preliminary List of Compliance Risks to be Assessed (cont'd)

Preliminary List of Compliance Risks to be Assessed

16.	Claims submitted to a government payor are overstated.
17.	Claims submitted to a government payor are inadequately documented.
18.	Claims submitted to a government payor for a service not medically necessary.
19.	Claims submitted to a government payor for a service not performed.
20.	Claims Submission requirements for clinical trials are non-compliant.

2. Identify Your Organization's Key Compliance Risk Related Data

One of the most important tasks in performing a compliance risk assessment is to identify relevant sources of information to be considered

You must determine your organization's business units, departments, processes, and information systems that represent the highest compliance risk to your organization and data about them is available.

2. Identify Your Organization's Key Compliance Risk Related Data

Nine Categories of Risk Related Data Sources:

- 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

2. Identify Your Organization's Key Compliance Risk Related Data

Evaluate a Broad Set of Enterprise-wide Risk Data:

- Traditionally compliance functions have focused on only a subset of the Revenue Cycle metrics and information. It is essential to evaluate a fuller set of enterprise-wide risk data 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.

Revenue Cycle Information

(*with focus on government payors*)

- OIG Annual Work Plan initiatives and Compliance Guidance (s)
- 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/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

External Reviews

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

3. 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.**
- **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.**

4. 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, Subject Matter Experts (SME), to evaluate relevant risk related information, control activities, and results of interviews to determine the extent the organization is mitigating each risk.

4. Evaluate Control Activities and Level of Risk Mitigation (continued)

Where to Begin:

- Meet with the SME's and key stakeholders to assess the level of risk, considering:
  - Relevant regulations
  - The complexity of related business processes
  - The controls in place (using COSO model)
  - The reliability of those controls

4. Evaluate Control Activities and Level of Risk Mitigation (continued)

Where to Begin (cont'd):

- You should consider and assess
  - **Likelihood**: The 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, considering existing controls

4. Evaluate Control Activities and Level of Risk Mitigation (continued)

Examples of understanding risk data and mitigation activities for a risk area.

Complete the following evaluation for each identified risk.

Determine the "*Risk Factor*" for Each Risk Area through both Objective and Subjective Measures

***(Risk Factor* = The estimated percentage of unmitigated risk)**

Risk # x

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Risk Factor = xx%

✓ Regulations were discussed and reviewed with Marketing in 2004 who confirmed that the value of any individual gift does not exceed the threshold.

List key control activities in black

❑ **There are no explicit policies addressing this area.**

Identify and document control deficiencies red

Action: Based on considering the aggregate impact of controls and gaps/ deficiencies, assign a Risk Factor % as **your estimate of unmitigated risk.**

Example of evaluating a risk area

Risk #2.

Risk Factor = 20%

Conflicts of Interests not adequately monitored and mitigated.

- ✓ Company has policies requiring conflicts disclosures by Board of Trustees members, managers and supervisors, medical directors, and principal investigators on clinical trials.
- ✓ Annual disclosure and mitigation processes are in place for Board of Trustees and managers and supervisors.
- ✓ IRB's have review mechanisms for evaluating and monitoring disclosures by principal investigators.
- ❑ Disclosure process for medical directors is incomplete and possibly ineffective.
- ❑ No policy for medical staff members to disclose vendor relationships.

5. Calculate Risk Concern Level and Rank Risk Areas

- There is not one generally accepted approach to calculate Risk Concern Level.
- The most important parts of the evaluation are consistency in application of the process, the multi-disciplinary "**group think**" and relative weighting of risk areas.
- The risk oversight group (Subject Matter Experts) 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.
- Ranking allows the risks to be categorized and prioritized to permit both better focus and more cost-beneficial mitigation.

5. Calculate Risk Concern Level and Rank Risk Areas (continued)

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

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

- 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.

- 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

5. Calculate Risk Concern Level and Rank Risk Areas (continued)

NOTE:

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.

5. Calculate Risk Concern Level and Rank Risk Areas (continued)

- Develop a risk matrix and use it as a tool to assess the impact and likelihood
- Summarize your results and prioritize 20 risk areas from the highest to the lowest
  - Rank by significance (Risk Concern Level)
  - Plot in quadrants
- Obtain confirmation / buy-in from senior management and your organization's governance committee or board
- Use department level metrics obtained (such as total medical revenues, employee satisfaction surveys, and turnover) to risk rank all your depts (cost centers) for further review.

6. Identify and Categorize Key Compliance Program Controls (*simulated results*)

Control Category	#	Primary	Secondary
Authorization	54	29	25
Edit/Exception Reporting	2	1	1
Config/Acc Mapping	7	4	3
Key Performance Indicators	2	1	1
Mgmt Review	45	14	31
Reconciliation	1	1	0
Segregation of Duties	1	1	0
System Access	1	0	1
Totals	**113**	**51**	**62**

6. Identify and Categorize Key Compliance Program Controls (*simulated results*)

Control Type	#	Primary	Secondary
Manual Detective	40	14	26
Manual Preventive	66	32	34
System Detective	4	2	2
System Preventive	3	3	0
Totals	113	51	62

6. Identify and Categorize Key Compliance Program Controls (*simulated results*)

Control Occurrence	#	Primary	Secondary
Annually	17	7	10
Bi-Weekly	1	0	1
Daily	1	0	1
Transaction-Based	81	36	45
Monthly	9	5	4
Quarterly	4	3	1
Totals	**113**	**51**	**62**

7. Identify Control Gaps and Deficiencies

(*simulated results*)

Issues	#	Control Gap	Design Deficiency	Operating Deficiency
Issues - Primary	37	10	20	7
Issues - Secondary	39	14	12	13
Totals	76	24	32	20

8. **Confirm Compliance Risk Assessment results *(risk rankings, controls by categories, and controls gaps and deficiencies)* with Subject Matter Experts, Senior Management, Compliance Committee, and Board Oversight Committee for their understanding and confirmation of process results.**

9. **Prepare Performance Improvement Action Plan…….**
***(equivalent to an audit report with recommended action, responsible management person for completing action*, and target completion date)**
and communicate Follow-up Process.

10. Incorporate and Translate Risk Assessment Results into Compliance and Internal Audit Planning

In Summary – The Key Outputs from Your Compliance Risk Assessment Process

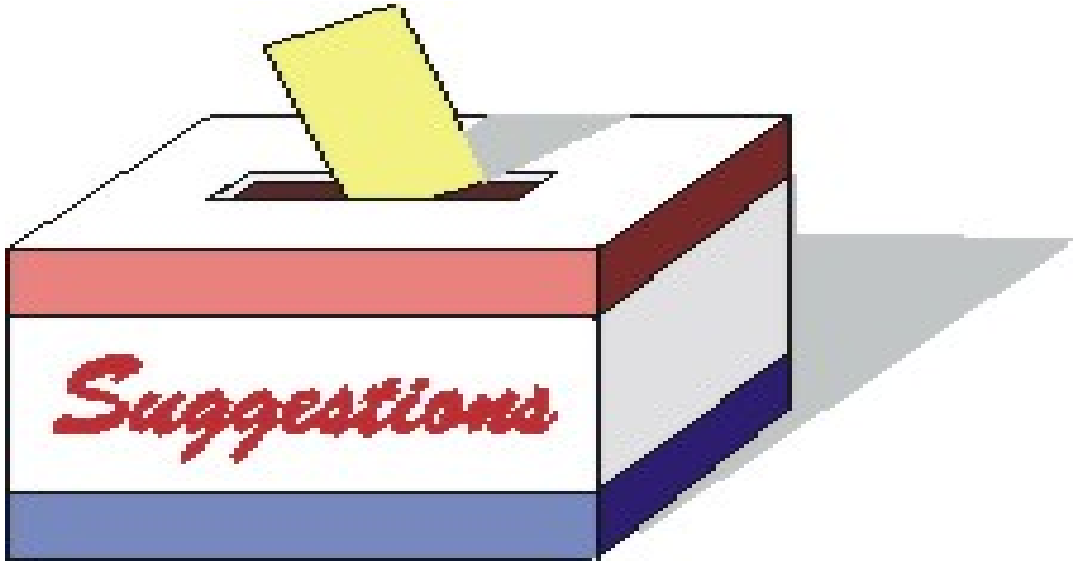
- ✓ **Risk Concern Levels for the 20 Compliance Risk Areas Assessed**
- ✓ **Determination of 10-15 cost centers (Departments) with the highest compliance risk concern for targeted 40-80 hours compliance diagnostic reviews for your annual plan.**
- ✓ **Identification and categorization of your "primary" and "secondary" key compliance program controls and the individuals responsible for them. This allows for more targeted auditing and monitoring that these controls are functioning as intended.**
- ✓ **Identification of control gaps and deficiencies to be addressed**
- ✓ **Performance Improvement Plan with recommendations and management's planned corrective actions to strengthen your compliance program and target dates.**

A lot of hard work has been completed and then Next Year…

Update your understanding

and do it again !!

We are interested in sharing approaches and understanding what others are doing in the area compliance risk assessments, so let us know your thoughts.



Randall K. Brown
Baylor Heath Care System
RandalBr@BaylorHealth.edu

Glen C. Mueller
Scripps Health
mueller.glen@scrippshealth.org