A Practical Approach to Risk Assessment and How it Ties to Compliance Effectiveness

Alaska Regional Compliance & Ethics Conference
Anchorage, Alaska
Feb. 27-28, 2020

Betsy Wade, MPH, CHC, CNA
Chief Compliance & Ethics Officer
Signature HealthCARE

“There are risks and costs to a program of action, but they are far less than the long-range risks and costs of comfortable inaction.”

~ John F. Kennedy
Objectives

- Understand how Risk Assessment, Monitoring and Auditing, Compliance Work Plans and Reporting drive Compliance Effectiveness
- Learn how to quantify and track results to demonstrate Compliance Effectiveness to your Compliance Committee and Board
- Tools and Resources to help you assess your organization’s Compliance Effectiveness and measure results
- References

1. HOW MANY OF YOU REPRESENT?
   • ACADEMIC HEALTH CARE
   • NON-PROFITS
   • FOR-PROFITS
   • PUBLICLY TRADED FOR-PROFITS

2. HOW MANY OF YOU CONDUCT A RISK ASSESSMENT?
What is Risk?

• Originates from:
  - the Italian *risco*, which means *danger*, and *rischiare*, which means runs into danger

• Noun that means:
  - a situation involving exposure to danger
  - a *possibility of harm* or *damage* against which something that is insured
  - the *possibility of financial loss or injury*

• Verb that means:
  - exposing someone or something valued to *danger, harm or loss*
  - to incur the risk or danger of
  - acting or failing to act in such a way as to bring about the possibility of an unpleasant or unwelcome event
What affects Risk?

- Cash flow and liquidity
- Competition
- Evolving Technology
- Financial demands
- Joint Ventures
- Laws/Rules/Regulations
- Mergers/Acquisitions/Alliances
- Organizational Ethics
- Politics
- Type of industry
- Unknown

What are common business risks?

- Cybersecurity
- Government investigations
- Litigation and other legal action
- Reductions in payment rates, unrealized or lost revenue
- Loss or destruction of assets
- Customer dissatisfaction
- Fraud and abuse
- Conflict of interest
- Unacceptable accounting prin
What are uncommon business risks?

- **Black Swan Events:**
  - an event or occurrence that *deviates beyond what is normally expected* of a situation that would be *extremely difficult to predict*
  - an outlier that carries an extreme impact, *usually catastrophic*
  - the event is a surprise to the observer

- **Examples:**
  - 9/11
  - dot com bubble (2001)
  - Brexit

WHAT WOULD BE A BLACK SWAN EVENT IN HEALTH CARE?
Risk Assessments are foundational to a Compliance Program:

- U.S. Sentencing Guidelines
- Corporate Integrity Agreements
Risk Assessment and Compliance

U.S. Sentencing Guidelines mandate the Organization shall:

(A) Assess periodically the risk that criminal conduct will occur, including assessing the following:

i. The nature and seriousness of such criminal conduct...

ii. The likelihood that certain criminal conduct may occur because of the nature of the organization’s business...

iii. The prior history of the organization...

(USSG § 8B2.1(b)(5)(7) and (c); USAM 9-28.800 Comment; OECD Handbook, B, p. 10 et seq.)

Corporate Integrity Agreements include the following Risk Assessment requirement:

• The risk assessment and internal review process shall require compliance, legal, and department leaders, at least annually, to:
  • (1) identify and prioritize risks,
  • (2) develop internal audit work plans related to the identified risk areas,
  • (3) implement the internal audit work plans,
  • (4) develop corrective action plans in response to the results of any internal audits performed, and
  • (5) track the implementation of the corrective action plan in order to assess the effectiveness of such plans.

The Covered Entity shall maintain the risk assessment and internal review process for the term of the CIA.
Risk Assessment and Compliance

• Address areas of government scrutiny
• Be proactive vs. reactive
• Improve Compliance Effectiveness
• Design controls to protect the organization
• Allocate resources
• Prevent and reduce compliance issues
• Decrease or prevent potential fines

Effective ways to conduct a Compliance Risk Assessment
Effective ways to conduct a Compliance Risk Assessment

A Risk Assessment:

- Is a five-stage systematic process of evaluating those things, situations and processes that may cause harm to the organization resulting in non-compliance with regulatory requirements.
- Is conducted by a group of individuals representing different functions in an organization to identify, assess and prioritize compliance risk to reduce the probability of occurrence and/or impact unfortunate events.
- Analyzes what can go wrong, how likely it is to happen, what the potential consequences are, and help an organization determine risk mitigation steps and establish controls.
- Helps the organization judge “the tolerability of the risk on the basis of a risk analysis” while considering influencing factors.

Risk Assessment Steps

1. Risk Identification
2. Risk Ranking
3. Work Plans
4. Results / Action Plans
5. Reporting Results
Effective ways to conduct a Compliance Risk Assessment

• All healthcare providers that participate in federal healthcare programs, including but not limited to:
  • Durable Medical Equipment companies
  • Emergency transport services
  • Hospitals and health systems
  • Home health agencies
  • Hospice
  • Pharmaceutical manufacturers
  • Physician practices
  • Skilled Nursing Facilities
  • Etc.

• Risk Assessments are a team effort:
  • Compliance
  • Internal Audit
  • Legal
  • Risk Management
  • Operations
WHO ELSE WOULD YOU INCLUDE IN THE PROCESS?

Effective ways to conduct a Compliance Risk Assessment

- Risk Assessments can be performed anytime:
  - Usually about the same time annually
  - Usually started during budget planning cycle
  - Typically done during the third and fourth quarters of the organization’s fiscal year
  - Continuous process year after year
Sample steps and timeline for Risk Assessment process

• Q2 – Planning and Risk Identification
• Q3 – Risk Ranking / Prioritization and Develop Work Plans
• Q4 – Compliance Committee and Board approval of Work Plans
• Q1 – Q4 Begin Monitoring and Auditing, analyze outcomes and develop action plans, and report results
• Repeat Cycle

Effective ways to conduct a Compliance Risk Assessment

• There is not one way to do a Risk Assessment.
• Develop the best method for your organization.
• Scale it to the organization’s size and complexity.
• Points to decide:
  • Compliance risks only vs. Enterprise Risk Management
  • Internal vs. external third-party
  • Manually vs. risk assessment software
Risk Assessment Process

- **Adopt Risk Assessment Policy that details:**
  - **Who** is responsible for the Risk Assessment process
  - **What** process or framework is used to conduct the assessment (e.g., compliance only, Enterprise Risk Assessment, COSO, RIMS)
  - **When** the annual assessment is conducted
  - **The scope** of the assessment (what entities or departments will be included)
  - **How** the results will be ranked and prioritized
  - **How** the results will be used to create the Internal Audit Plan and Compliance Monitoring Plan
  - **How** the Risk Assessment results, Internal Audit Plan and Compliance Monitoring Plan will be approved by the Compliance Committee and the Board
## Risk Identification

### Simple
- Compliance
- Risk Assessment focused on regulatory requirements
- Interviews
- Interviews + Surveys
- Interviews + Surveys + Document Review
- Data mining

### Complex
- Enterprise Risk Assessment following COSO or RIMS*

* Sources:
  - Sarbanes-Oxley requires this for publicly traded companies
  - COSO (Committee of Sponsoring Organizations of the Treadway Commission) (2004)
  - RIMS Risk Maturity Model for Enterprise Risk Management (2006)

### Review Documents
- OIG Audits
- OIG Work Plan and updates
- OIG Fraud Alerts
- PEPPER Reports
- Previous Audits and Reviews
- Regulations
- Special Advisory Bulletins
- State and federal survey results
- Third Party Litigation
- Review Documents
  - Compliance Program Guidance
  - Corporate Integrity Agreements
  - Court documents
  - Government Agency Priorities
  - Industry Newsletters
  - Interviews
  - Laws
  - NCDs/LCDs
  - New Payment Models
Risk Identification

- Conduct Interviews
  - Board members
  - Senior management
  - CEOs
  - VPs
  - Department leaders

WHAT OTHER AREAS WOULD YOU INCLUDE?
Risk Identification

- Conduct Data Mining
  - PEPPER Reports
  - Denials data
  - CMS Open Payments Database
  - Excluded providers
  - Licensure
  - Star ratings
  - Survey data
  - Litigation data
  - Etc.

The types of risk varies based on type of entity and the departments within the entity. Here are some examples:
- Bad debt
- Billing and coding
- Clinical quality
- Clinical research
- Cost reports
- Credentialing
- Credit balances
- Documentation
- Emergency Preparedness
- Environmental
- Excluded providers
- Finance
- HIPAA Privacy and Security
- Information Technology
- Licensure
- Marketing
- Medical Necessity
- Mergers, Acquisitions and Divestitures
- Physician Transactions (Stark)
- Policies and Procedures
- Record retention
- Regulatory
- Reimbursement
- Staffing and Payroll Based Journal
- State and federal surveys
Once risks have been identified, there are various ways to rank them to present the highest risk areas to the company:

- Red, yellow, green
- Low, moderate, high
- Numeric ranking
- By likelihood of occurrence – improbable, remote, occasional, frequently, all the time
- Impact of occurrence – minimal/negligible, slight, moderate, critical/serious, catastrophic
- Categorically by type of impact, such as compliance, financial, legal and reputational
## Risk Ranking

### Risk Assessment Scorecard

<table>
<thead>
<tr>
<th>Risk Rating Scale</th>
<th>Threat Category</th>
<th>Risk Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Shirk Laws &amp; Kickback</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Privacy and Security</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Disaster Recovery</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Antitrust/Competition Laws</td>
<td>Low</td>
</tr>
<tr>
<td>5</td>
<td>Corporate Culture</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

### Likelihood
- **High**
- **Moderate**
- **Low**

### Consequence
- **Moderate**
- **High**
- **Low**

---

*How Risk Assessment relates to Monitoring and Auditing*
How Risk Assessment relates to Monitoring and Auditing

• Use prioritized results from the Risk Assessment to develop work plans:
  - Compliance Monitoring Plan
  - Internal Audit Plan
• Have Compliance Committee and Board approve all plans

How Risk Assessment relates to Monitoring and Auditing

• What should you include in monitoring and auditing?
  • Education completion
  • Hotline call analysis (types of calls, number of calls, by entity/region/state)
  • Whether hotline calls were logged within 2 business days
  • Repayments within 60 days (government audits, internal audits, compliance monitoring, investigations)
  • Excluded providers
  • ETC....
How Risk Assessment relates to Monitoring and Auditing

- Conduct auditing and monitoring and report out findings to management, the Compliance Committee and the Board
- Develop Corrective Action Plans with owner
- Conduct follow up to test effectiveness of Action Plans
- Document, document, document

How Risk Assessment and Compliance Effectiveness Tie Together
How Risk Assessment and Compliance Effectiveness Tie Together

1. Risk Assessment
2. Monitoring and Auditing
3. Compliance Work Plans
4. Measuring and Reporting

Risk Assessment is a key component of measuring Compliance Program effectiveness:

- *Evaluation of Corporate Compliance Programs* (U.S. Department of Justice Criminal Division, April 2019)
- *Evaluation of Corporate Compliance Programs* (U.S. Department of Justice, February 2017)
How Risk Assessment and Compliance Effectiveness Tie Together

How Risk Assessment and Compliance Effectiveness Tie Together

Measuring Compliance Program Effectiveness: A Resource Guide

| 2.56 | Compliance Resource knowledge and competence | Survey, focus groups and interviews |
| 2.57 | Compliance staff knowledge of current regulatory changes and laws | Document review and interviews. Review certificates of attendance at conferences/other educational events, tools used to keep compliance staff current, compliance budget (to support access to current regulatory changes and laws) |
| 2.58 | Monitoring of regulations that impact the organization | Document and process interviews (Refer to Guide for list of questions) |
| 2.59 | Risk Assessment Cycle | Audit adherence to risk assessment cycle and annual documented risk assessment has been communicated to oversight committee |
| 2.6 | Risk based work plan that covers compliance plan elements with board approval and regular reporting on those projects to board | Compliance Committee and board minutes review |
| 2.61 | Work plan development based on risk assessment | Process and document review |
| 2.62 | Prioritization of risk and consultation with applicable risk partners (legal, HR, IT, risk management) | Documentation and process review. Is there a risk based plan? How was it developed? |
| 2.63 | Exit interview | Compliance concerns that come up in exit interviews are addressed |

Evaluation of Corporate Compliance Programs (U.S. Department of Justice Criminal Division, April 2019, p. 2-3)

- Risk Management Process – What methodology has the company used to identify, analyze and address the particular risks it faced? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company’s compliance program?
- Risk-tailored Resource Allocation – Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas? Does the company give greater scrutiny as warranted to high-risk transactions ... than more modest and routine hospitality and entertainment?
- Updates and Revisions – Is the risk assessment current and subject to periodic review? Have there been any updates to policies and procedures in light of lessons learned? Do these updates account for risks discovered through misconduct or other problems with the compliance program?
How Risk Assessment and Compliance Effectiveness Tie Together

“We recognize that each company’s risk profile and solutions to reduce its risks warrant particularized evaluation. ... The starting point for a prosecutor’s evaluation of whether a company has a well designed compliance program is to understand the company’s business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks.”

~ Evaluation of Corporate Compliance Programs (U.S. DOJ Criminal Division, Updated April 2019)

POLL

IF YOU WEREN’T DOING RISK ASSESSMENT BEFORE WILL YOU NOW?
Sample Tools and Resources

- Risk Assessment policy
- Risk Assessment questions
- Internal Audit Plan
- Compliance Monitoring Plan
- Compliance Program Effectiveness Gap Analysis Tool
- Compliance Committee and Board Reporting Scorecard

ALL OF LIFE IS THE MANAGEMENT OF RISK, NOT ITS ELIMINATION

WALTER WRISTON
Policy and Gap Analysis Tool

Draft Risk Assessment Policy and Process

In accordance with Office of Inspector General (OIG) Compliance Program Guidance, the U.S. Sentencing Guidelines and in support of the eighth element of an effective compliance program, Risk Assessment Plans and Gap Analysis approaches are utilized to identify areas for improvement and to support the development of subsequent plans and programs. This document provides an overview of the methodology and key components of the Risk Assessment Plan that identifies areas of non-compliance based on the identified program's risk factors, and provides guidance on the development of subsequent plans and activities. The approach is designed to be flexible and scalable to meet the needs of various organizations and their specific requirements. The Risk Assessment Plan is a critical tool that helps organizations assess their current compliance status, identify areas for improvement, and develop effective remediation plans.

Auditing and Monitoring Plans

<table>
<thead>
<tr>
<th>File</th>
<th>Home</th>
<th>Insert</th>
<th>Dates</th>
<th>Page layout</th>
<th>Formulas</th>
<th>Data</th>
<th>Review</th>
<th>Win</th>
</tr>
</thead>
<tbody>
<tr>
<td>A02</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Developing a risk assessment plan to identify potential risk areas and assessment of risk and potential impact, and identify actions required.
- Developing a gap analysis plan to identify areas for improvement and prioritize those activities.
- Establishing an internal audit plan to include internal controls, procedures, and processes to ensure compliance with established policies and procedures.
- Developing an internal control plan to identify potential areas for improvement and prioritize those activities.
- Establishing an internal control plan to include internal controls, procedures, and processes to ensure compliance with established policies and procedures.
- Developing an internal control plan to include internal controls, procedures, and processes to ensure compliance with established policies and procedures.
**Compliance Scorecard**

**Compliance Risk Assessment and Effectiveness Resources**

- *Evaluation of Corporate Compliance Programs Guidance* (U.S. Department of Justice Criminal Division, April 2019)


- *Evaluation of Corporate Compliance Programs* (U.S. Department of Justice, February 2017)

Compliance Risk Assessment Take Aways

- Risk Assessment isn’t a whether or not to do it, it’s a must
- Risk Assessments are scalable to the complexity and size of the organization
- There is not one way to do a risk assessment and organizations should determine what works best for them
- Risk Assessment requires a collaborative team
- Risk Assessment is a continuous cycle that is completed annually
- Risk Assessment can help an organization identify potential risks and implement measures to prevent them from occurring
- Risk Assessment is an indication of an effective Compliance Program
Betsy Wade, MPH, CHC, CNA
Corporate Compliance Officer
bwade@shccs.com
(502) 568-7748