Conducting a Risk Assessment

Presented by:
Debbie Troklus, CCEP-F, CHC-F, CHPC, CHRC, CCEP-I
Managing Director
Aegis Compliance and Ethics Center

Sheryl Vacca, CCEP-F, CCEP-I, CHC-F, CHPC, CHRC
SVP/Chief Risk Officer
Providence St Joseph Health

Agenda

- Discuss definitions of risk and risk assessments
- Discuss the methodologies available for risk assessment
- Discuss how to conduct a risk assessment
- Identify different methods for reporting risk assessment results
- Discuss how to execute the outcomes from the risk assessment process

What is Compliance Risk?

- Risks related to real or potential non-compliance with a rule, regulation, policy, guideline, protocol that might obstruct, prevent, delay an organization from being compliant.
- Examples?
  - No policy/Not following a policy
  - Conflict of Interest
  - Regulatory Change/Non-compliant with regulations

Things that Affect Risk

- Culture
- Management Buy-In
- Financial Demands
- Resources
- Technology
- Competition
- Laws/Rules/Regulations
- The Unknown

Compliance is management of risk

- Federal Sentencing Guidelines (US)
  - An organization "shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of its compliance and ethics program] to reduce the risk of criminal conduct identified through this process."
  - Risk management elements: standards and procedures (internal controls), monitoring, auditing, periodic evaluation

(§8B2.1(b)(1) (5))

- Federal agencies
  - Department of Labor
  - HHS OIG
  - National Institute of Health

5

Most organizations rely on multiple sources for answers
However, risk oversight and an integrated approach is usually lacking

Integrated process provides a means to better understand, communicate and respond to the risk intelligence that exists in the organization

6

Leverage Your Resources – Compliance does not have to do everything

Conducting a Risk Assessment

1. Defining your Risk Assessment Methodology
2. Identification of risks
3. Evaluation/Analysis of risks
4. Prioritization of risks
5. Management action plans for mitigation
6. Reporting/documentation
7. Auditing and monitoring mitigation plans

Considerations for defining your risk assessment methodology

- Culture of accountability
- Leadership/management involvement
- Attorney client privilege?
  - Is transparency important?
  - Is subject-matter risky to the organization if identified outside of privilege?
  - Is this mandated by a regulatory requirement?
  - Is your organization under investigation?
- Resources

Identification of Risk

- Internal audits findings
- External audits findings
- Previous baseline documents, ie: surveys, questionnaires
- Hotline log, if applicable
- Investigative findings
- CIAs for similar organizations
- Industry benchmarking
- Enforcement activity
- Regulatory mandates
- Other?

Risk Identified

- List developed
  - Privacy
  - Information security
  - Coding/billing
  - Conflicts of Interest
  - Contract
  - Third Party Relationships
  - Change in delivery system
  - Patient safety
  - Outdated policies and procedures

Evaluation/Analysis of Risk

How do the risks identified impact the company's business units which affect regulatory status, which affect reputation, which can lead to prosecution, what are enforcement trends?

- Does management already have controls in place related to the identified risk?
- Consider business culture influences, ie: tone at the top, employee trust, business metrics, compensation plans, external influence on culture
- Consider Ethical Fault Lines, ie: conflicting stakeholder obligations, state of compliance in the industry
- Is non-compliance accepted?
- Do employees believe that they can both comply and compete?

Evaluation/Analysis Outcome

Privacy

Example: Management recently had an audit of this area and have hired an external expert to help mitigate the issues.

Compliance Action: Keep as a priority and monitor for an execution of plan.

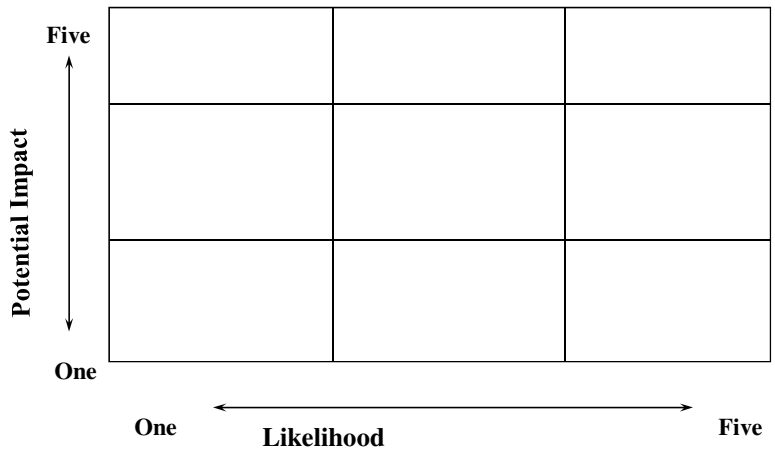
Prioritization of Risk

- Management should be involved in the ranking process.
- Common criteria to use in prioritization is ranking likelihood and impact.
  - High, Medium and Low with definitions for objectivity or ranking by numbers (1 to 5 scale, Likert research).

Risk Ranking example

	Reputation	Legal/Regulatory	Financial
High	Systemic loss of public/client confidence resulting in loss of clients; major media coverage – headline news for several days	Major infraction resulting in criminal or civil prosecution and/or significant discipline; loss of ability to operate in one or more countries	Significant financial impact with widespread liability
Moderate	Loss of confidence among large number of clients and a segment of the general public; major media coverage for 1-2 days	Infraction resulting in civil prosecution and/or discipline; loss of ability to operate within local jurisdiction	Considerable financial impact with regional liability
Low	Loss of confidence among a limited number of clients, limited local media coverage	Minor infraction that is readily remediated; no loss of ability to operate	Minimal financial impact with localized liability

Example of a Risk Prioritization Graph



Kaplan & Walker

Risk Prioritization Example

- Privacy – during analysis we said this was already being handled. It ranked high Or 25 pts (5 for likelihood and 5 for impact) but because management is working on mitigation we will monitor
- Coding/billing- this ranked high and 25 points because during analysis we determined no management controls are in place and it hasn't been audited for the past 2 years
- Patient safety- this ranked high and 15 points because it is on everyone's mind and the organization is constantly monitoring this area and auditing it.

The remaining risks, after review and ranking, at this time are not on the plan and will remain a focus for ongoing management monitoring and compliance consideration in the future, if needed.

- Outdated policies and procedures
- Conflicts of Interest
- Contract
- Third Party Relationships
- Change in delivery system

Part 2

Management Action Plans for Mitigation

- Management owns the risk.
- Management is responsible for the development and implementation of mitigation plans.
- Management decides on the response.
- Compliance assists management in facilitating, educating and providing advise.
- Compliance must maintain independence but may have to disagree with management and escalate concern.

Reporting/Documentation

- Compliance needs to document the process from start to finish.
- Compliance needs to provide the rationale for the approach it took.
- Compliance needs to communicate the results to management.
- Compliance needs to report to senior leadership and the board the results.
- The results of a risk assessment are the basis for:
  - Education plan
  - Auditing and monitoring plan

Example of Dashboard for Reporting

Risk Area	High	Med	Low	Who Owns?**
Billing and Coding	25 pts Q1	15 points Q2	Mitigation plan executed 5 points Q3	Management
Patient Safety		15 pts Low because of current activity		Management, Quality, Risk…
Privacy	25 pts Low, external expert helping management			Management, Legal…
Etc.				

21

Reporting of Results

- Depends on who you are reporting to:
  - Board
  - Management
  - Risk Area
- Considerations
  - Public entity
    - Intranet vs. public website
  - What would someone say if they saw your results? Ie: shareholders, customers, staff, etc.
  - Business concerns, ie: due diligence occurring, catastrophic event occurring
  - What format will you use, ie: paper or electronic, summary version or detail, etc.

Interactive Exercise

- You are a compliance officer in a small rural clinic. You have limited resources. Your leadership has asked you to identify the compliance risks for the organization. What steps would you take to provide this information to leadership?

Questions?