Risk Assessment: A Practical Approach and Case Applications

Presentation By:
Dennis Smyser, CPA, MSMIS
Senior Internal Auditor
Mayo Clinic
And
Sheryl Vacca, CHC, CCEP
SVP/Chief Compliance and Audit Officer
University of California

Objectives

• To provide a practical approach to implementing Risk Assessment at a healthcare institution
• Risk Assessment Background
• Performing a Risk Assessment
• Adding Value
• Tips
• Questions

Internal Audit Standards

• 2010.A1 – The internal audit activity’s plan of engagements should be based on a risk assessment, undertaken at least annually.
• 2110-1 – Auditors should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.
• 2120.A1 – Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization’s governance, operations, and information systems.
• 2210.A1 – When planning the engagement, the internal auditor should identify and assess risks relevant to the activity under review. The engagement objectives should reflect the results of the risk assessment.
Types of Risk

Risk is viewed in four major areas:

- **Operational** (Processes and procedures) risks and activities that impact the efficiency and effectiveness of business operations.
- **Financial** (Data rolling up to internal/external statements) activities that impact the reliability of financial statements, financial reporting disclosures and other financial impacts.
- **Compliance** (Federal, State, Local, Organizational Policy) activities that impact adherence to applicable laws and regulations.
- **Strategic** (Institutional) achievement of an organization’s business objectives. Often neglected area of risk, with potential for high return.

Risk Universe

Assess Risk

COSO Exposure Draft – Guidance on Monitoring Internal Controls Systems states that the Board of Directors is responsible for:

1. Understanding the risks the organization faces, and
2. Gaining an understanding of how senior management manages or mitigates those risks that are meaningful to the organization’s objectives.

COSO suggests that Internal Audit may want to implement a policy to credit clients that self-report deficiencies as an inducement for self-reporting risks.
COSO Exposure Draft Continued-
The goal of Risk Assessment is to identify, assess, and evaluate risks across all strategic, operational, reporting, and compliance activities.

Business unit leaders, who have input into the risk assessment process, are tasked with managing or mitigating those risks within their area of responsibility.

Some Goals of Risk Assessment
- Identify, measure and, to some extent, manage or control risks
- To determine what is an acceptable level of risk?
- Strengthen corporate governance
- Improve accountability
- Increase transparency of financial reporting through improved reliability and accuracy of information
- Enhance effectiveness of internal controls
- Enhance compliance with laws and regulations
- Identifying unwanted, negative consequences to people, property, finances, etc.
How to perform a Risk Assessment

Risk assessment is the identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed.

You should:

• Prioritize Risks
• Identify Key Controls
• Identify Necessary Information
• Implement Monitoring

How to perform a Risk Assessment

• Don’t rush – “lite” may be acceptable first
• Use outcomes to improve program structure and focus
• Use it to prove program efficiency, not vice-versa
• Strive for objectivity - open-end questions (3x rule)
• Know what measures will be
• Message clear, concise and unique from IA
• Include non-compliance ideas and feedback –unique facilitating position
• Be prepared to deal with what you find – and steer leadership accordingly in ADVANCE

How to perform a Risk Assessment

Some Methods:

• Interviews
• Surveys:
  – Open-ended
  – Ranking
  – Rating
• Facilitated Sessions
• Prior Audits
• OIG Workplan
• Legal & Compliance
How to perform a Risk Assessment

Some Methods:

• Continuous Risk Assessment
  – Transaction Analysis or Trends
  – Comparisons of a process or systems over time
  – Using Technology to Monitor Activities on an Ongoing Basis, e.g. Audit Command Language (ACL)
  – Respond to Changes Timely
  – Includes interviews, control self-assessments, walkthroughs, questionnaires, etc.
  – Review Management’s Monitoring Activities

Thought Leadership Themes - Healthcare

<table>
<thead>
<tr>
<th>Business Risk</th>
<th>Industry Themes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>• Uninsured programs</td>
</tr>
<tr>
<td></td>
<td>• Charity care</td>
</tr>
<tr>
<td></td>
<td>• Accounts receivable cycle (patient billing and collections)</td>
</tr>
<tr>
<td>Operational</td>
<td>• Charge capture</td>
</tr>
<tr>
<td></td>
<td>• Facilities – seismic readiness</td>
</tr>
<tr>
<td></td>
<td>• Data integrity and security</td>
</tr>
<tr>
<td></td>
<td>• Quality of care/medical necessity</td>
</tr>
<tr>
<td>Compliance</td>
<td>• Billing government programs</td>
</tr>
<tr>
<td></td>
<td>• Joint ventures (physician contracting)</td>
</tr>
<tr>
<td></td>
<td>• Nurse/patient staffing ratio</td>
</tr>
<tr>
<td>Strategic</td>
<td>• Areas related to local/regional focus</td>
</tr>
<tr>
<td></td>
<td>• Physician Network</td>
</tr>
</tbody>
</table>
Most organizations rely on multiple sources for answers. However, risk oversight and an integrated approach is usually lacking.

**Major Types of Risk for Healthcare Providers**

**Financial Operations**
- Accounting / Cost Reports / Revenue Cycle – Patient Accounting
- Philanthropy / Grant Management
- Treasury & Investments
- Tax – UBI, Payroll Withholding, Intermediate Sanctions, Returns - 990s, and 501C3 Status
- Financing – Bonds, Public
- Internal Controls – Internal Audit
- Contracting / Purchasing (Materials Management) – Group Purchasing Organization Relationships
- Construction

**Compliance and Legal Matters**
- Federal and state regulations
- Stark
- IRS Tax
- Anti-Kickback
- HIPAA
- Anti Trust

**Security**
- Risks to property and people

**Internal Audit**
- Risk informed audits, risks to internal control, key exposures and vulnerabilities, and assurance

**Information Management**
- IT Security, Data Integrity, Information Adequacy, Business Process/Continuity Risks

**Operations**
- Quality of care, Customer Relations, Prices, and Pricing, Competitiveness, Inside/Outside Risk
- Performance, Environmental and Health Risks

**Internal Controls**
- Internal Audit

**Business Development**
- Market and Strategy Risks

**Insurance**
- Property, Casualty, Liability, and Hazards

**General Counsel**
- Legal and Intellectual Property

**Compliance and Ethics**
- Ethics and Business Conduct, and Regulatory Compliance Risks

**Integrated approach provides a means to better understand, communicate and respond to the risk knowledge that exists in the organization.**
Major Types of Risk for Healthcare Providers

Health Care Delivery
The risks associated with the delivery of health care services across the continuum of care.
- Quality - Safeguarding of Practice
- Patient Safety
- Regulatory Compliance - EMTALA, Medical Necessity, HIPAA Privacy, Robinson/Patman
- Research/IRB
- Institution Licensing & Accreditation – COPS, CLIA, JCAHO, Patient Rights, Consent
- Marketing/Community Outreach

Employment and Staffing
The risks associated with the organization's delivery and management of its human resources including employed, contracted and credentialed providers.
- Labor Relations
- Wage & Hourly - Compensation
- Employment Practices – Hiring & Firing, EEO, ADA
- Education, Training, Development
- Staffing – Retention, Recruitment, Performance Evaluations, Levels
- Pension & Benefits - Insurance
- Worker’s Compensation
- Contract Labor – Agency, Nurses

Organization and Strategic Environment
The risks associated with external factors, strategic direction and issues related to organizational structure and culture.
- Strategy – M&A
- Advocacy – Tax Exempt Limitations
- Public Relations
- Organization & Governance
- Mission
- Market Forces (Competition)
- Disaster Planning
- Physical Security
- Canon Law
- Emerging Technologies (Innovations)
- Systems Integration
Risk Identification

Please identify the highest exposure risks to the organization overall, providing information regarding current risk minimization activities and opportunities for improvement. Also provide any recommendations regarding suggested internal audit support.

<table>
<thead>
<tr>
<th>Highest Exposure Risks</th>
<th>Current Risk Minimization Activities</th>
<th>Opportunities for Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Assessment

How to Measure Risk

- Three components of Risk Assessment
  - What could go wrong?
  - What is the likelihood of something going wrong?
  - What is the impact if something goes wrong?

- Likelihood of Occurrence
  1 = improbable
  2 = Remote
  3 = Occasional
  4 = Frequently

- Impact of Occurrence
  1 = Minimal/Negligible
  2 = Slight
  3 = Moderate
  4 = Critical/Serious
  5 = Catastrophic

Likelihood X Impact = Risk Priority
Impact vs. Probability

<table>
<thead>
<tr>
<th>High Impact</th>
<th>Medium Risk</th>
<th>High Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share</td>
<td>Mitigate &amp; Control</td>
<td></td>
</tr>
<tr>
<td>Low Impact</td>
<td>Low Risk</td>
<td>Medium Risk</td>
</tr>
<tr>
<td>Accept</td>
<td>Control</td>
<td></td>
</tr>
</tbody>
</table>

| Low Probability | High |

Example: Call Center Risk Assessment

<table>
<thead>
<tr>
<th>High Impact</th>
<th>Medium Risk</th>
<th>High Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Loss of phones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Loss of computers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Low Impact</th>
<th>Medium Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Fraud</td>
<td></td>
</tr>
<tr>
<td>- Lost transactions</td>
<td></td>
</tr>
<tr>
<td>- Employee morale</td>
<td></td>
</tr>
</tbody>
</table>

| Low Probability | High |

Risk Analysis

- Risk Assessment
  - Identification
  - Measurement
  - Prioritization

- Risk Management
  - Control It
  - Share or Transfer It
  - Diversify or Avoid It

- Risk Monitoring
  - Process Level
  - Activity Level
  - Entity Level
Reporting Your Outcomes

- Consider the audience, format should vary
- Make sure to state the outcomes as objectively as possible
- Vary the level of the presentation by the audience, i.e.: senior management could receive executive summary vs. granular information
- Attorney Client Privilege considerations

Risk is Dynamic

- Risk assessments are a process, not a project (Cultures evolve and risk assessments must also).
- Do mini evaluations each quarter on the priority risks identified – does it still need to be focus?
- Focus on “add value” to the organization, i.e.: does what you are doing make any difference to the organization?

Internal Auditors Can Add Value By:

- Reviewing critical control systems and risk management processes.
- Performing an effectiveness review of internal controls.
- Providing advice in the design and improvement of control systems and risk mitigation strategies.
- Implementing a risk-based approach to planning and executing the internal audit process.
- Ensuring that internal audit resources are directed at those risk areas most important to the organization.
- Challenging the basis of management’s risk assessments and evaluating their risk treatment strategies.
Tips

• Make sure that you’ve connected with the right people, meaning:
  – Who knows the business processes?
  – Who has authority to decide?
  – Who can be a Risk Assessment champion?
  – What is the tone at the top?
  – Who monitors risk in the organization

Tips

• Considerations in developing your risk assessment should include:
  – Where else has this been done in the organization?
  – How can you leverage the previous work?
  – Are there any sensitive areas to consider?
  – Seeking risk management, compliance and legal input before starting?
  – Have you discussed your approach with Senior Management

Questions?