Analyzing Risks in Healthcare

February 12, 2014
Content

→ What is Enterprise Risk Management (ERM)
→ ERM Benefits
→ ERM Standards / ISO 31000:2009
→ ERM Process
→ Risk Register
→ ERM Governance Model
→ Risks
→ Q&A
What is Enterprise Risk Management (ERM)

“a systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk”.

- Taken from ISO Guide 73:2009 the Definitions Guide to ISO 31000
What is Enterprise Risk Management (ERM) cont.

Risk is anything that has the potential to keep the Organization from achieving its strategic objectives and plans.

ISO 31000: effect of uncertainty on objectives.
ERM Benefits

**Early Warning Systems**
- Develop process to identify vulnerabilities and challenges
- Systematically identify, assess and prioritize risks
- Develop response strategies to risks

**Integrated Infrastructure**
- Ensure bad news travels fast internally first – act decisively
- Streamline processes
- Effectively allocate resources to better align with risks and objectives and better decision making
- Improve ability to anticipate and prepare for change
- Ensure internal/external risks are understood and managed

**Effective ERM Program**
- Seek growth but ensure strategic and operational risks are mitigated
- Maximize chances of success of achieving plans
- Accelerate ability to respond to change and opportunities
- Install an appropriate control infrastructure

No Big Surprises

No Big Mistakes

No Big Missed Opportunities
ERM Standards / ISO 31000:2009

ISO 31000
(Previously Australian/New Zealand Standard AS/NZS 4360:2004)

Design Framework for Managing risks
- Understanding the organization and its context
- Establishing risk management policy
- Accountability
- Integration with other processes
- Communication and reporting mechanisms

Continual Improvement of the framework
Implementing Risk Management

Mandate and Commitment

Communication and Consultation

ERM Process

The Committee of Sponsoring Organization of the Treadway Commission (COSO)
ERM Process (ISO 31000)

- Context: Assess strategic organizational context
- Identification: What can go wrong? Missed opportunities?
- Analysis/Measurement: Assess risk likelihood and consequences, review controls
- Evaluate: Compare risks, set risk priorities
- Treatment Options: Reduce, avoid, transfer or retain

ERM Process - *Inherent vs. Residual Risk*

- **Assess Risk**
- **Assess Controls**
- **Determine Treatments**

**Inherent Risk**
- Controls
- Residual Risk
- Treatment Plan(s)
- ACCEPTABLE Residual Risk

**Desired Residual Risk Ranking**

- **Likelihood**
  - 1. Insignificant
  - 2. Minor
  - 3. Moderate
  - 4. Major
  - 5. Extreme
  - 5. Almost Certain
  - 4. Likely
  - 3. Unlikely
  - 2. Rare
  - 1. Extremely Rare

- **Impact**
  - Inherent Risk
  - Residual Risk
  - Tolerance Level

- **Controls**
- **More Controls**
ERM Process - Risk Identification

• Use organizational goals to identify those issues that could impact the ability to achieve those goals (i.e. Risk)

• Ultimately, the goal of the ERM will be to build the risk identification process into the organizational planning process thus:
  • Allowing for regular updates to the risk profile.
  • Facilitating the timely management of risks within the planning and performance.

  Identifying
  • What can go wrong?
  • What part of the organization is impacted?
  • How is it impacting objectives?
ERM Process - Risk Identification - Workshop

- Understand risks that could affect the strategic objectives (risk universe).
- At least 2 people to manage the workshop.
- Know your audience.
- Different workshops for Risk Identification and Assessment.
- Workshop duration (3-4 hours in length).
- 10 participants (maximum).
- Workshops should consider different authorities that could impact the behavior of participants. Those individuals can be interviewed in advance to capture expectations and point of views.

<table>
<thead>
<tr>
<th>APPROACH</th>
<th>ADVANTAGES</th>
<th>DISADVANTAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interview</td>
<td>• Potentially more candid discussion regarding the Region’s strategic risks.</td>
<td>• The Client resource will be required to schedule all interviews.</td>
</tr>
<tr>
<td></td>
<td>• Interview is conducted at a convenient time for the interviewee.</td>
<td>• More costly approach as compared to workshops given additional consultant hours required to complete all interviews.</td>
</tr>
<tr>
<td></td>
<td>• Interviewees are not intimidated or influenced by other people’s opinions.</td>
<td>• Will take more time overall to schedule.</td>
</tr>
<tr>
<td></td>
<td>• Establish buy-in and commitment.</td>
<td>• No interactive dialogue between participants on risks and their potential interconnectedness.</td>
</tr>
<tr>
<td>Focus Group / Workshop</td>
<td>• Dialogue between focus group participants may result in better. discussion and agreement on risks</td>
<td>• Difficult to schedule the attendance.</td>
</tr>
<tr>
<td></td>
<td>• Will require less time to complete and can likely be scheduled to be completed in a two week period.</td>
<td>• Discussion may not be as candid given the group environment and may be further limited should there be attendance in the session by executive management.</td>
</tr>
<tr>
<td></td>
<td>• Establish buy-in and commitment.</td>
<td></td>
</tr>
</tbody>
</table>
ERM Process - *Risk Assessment*

**Risk likelihood** is the *possibility* or frequency of a risk event happening.

**Risk consequence** is the *outcome of a risk event* or situation expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain.
## ERM Process - Risk Assessment - Likelihood

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5</strong> Almost Certain</td>
<td>Event is expected to occur in most circumstances (likely to occur in a one year period)</td>
</tr>
<tr>
<td><strong>4</strong> Likely</td>
<td>Event will probably occur in most circumstances (i.e., has occurred or is expected to occur in two year time period).</td>
</tr>
<tr>
<td><strong>3</strong> Unlikely</td>
<td>Event might occur at some time (i.e., the event could occur or is expected to occur once every three years).</td>
</tr>
<tr>
<td><strong>2</strong> Rare</td>
<td>Event could occur at some time (i.e., the event has not yet occurred but could occur at some time, or is expected to occur once every five years).</td>
</tr>
<tr>
<td><strong>1</strong> Extremely Rare</td>
<td>Event may occur only in exceptional circumstances (i.e., you have heard of this occurring elsewhere or is expected to occur once every 10 years).</td>
</tr>
</tbody>
</table>
## ERM Process - Risk Assessment - Consequence

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Rating</th>
<th>Financial</th>
<th>Reputational / Strategic</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extreme</td>
<td>5</td>
<td>&gt; X Million</td>
<td>- Failure to meet key strategic objectives  &lt;br&gt;- Organizational viability threatened  &lt;br&gt;- Major financial overrun</td>
<td>- Severe impact on all aspects of the organization’s operations  &lt;br&gt;- Unexpected/ unplanned loss of a whole team</td>
</tr>
<tr>
<td>Major</td>
<td>4</td>
<td>$ XM to $ XM</td>
<td>- Major impact on strategy  &lt;br&gt;- Major reputational sensitivity  &lt;br&gt;- Sustained national media coverage</td>
<td>- Major impact on numerous key departments for a significant period of time  &lt;br&gt;- Unexpected/ unplanned loss of a few key VP’s</td>
</tr>
<tr>
<td>Moderate</td>
<td>3</td>
<td>$ XM to $ XM</td>
<td>- Moderate impact on strategy  &lt;br&gt;- Moderate reputational sensitivity  &lt;br&gt;- National media coverage - one off</td>
<td>- Moderate impact, affecting several key departments  &lt;br&gt;- A significant event to any area, which can be managed under normal circumstances  &lt;br&gt;- Unexpected/ unplanned loss of a VP considered to be key</td>
</tr>
<tr>
<td>Minor</td>
<td>2</td>
<td>$100K to $2M</td>
<td>- Minor impact on strategy; minor reputational sensitivity  &lt;br&gt;- Regulatory breach with minimal consequences but which cannot be readily rectified  &lt;br&gt;- Local news, short term interest, targeted internal communication, no customer/patient impact/uptake</td>
<td>- Minimal impact, affecting one department only, lasting one day or less  &lt;br&gt;- An event affecting all areas, the impact which can be absorbed but management effort is required to minimize the impact  &lt;br&gt;- Unexpected/ unplanned loss of a key Manager/ VP</td>
</tr>
<tr>
<td>Insignificant</td>
<td>1</td>
<td>&lt; 100K</td>
<td>- Minimal impact on strategy  &lt;br&gt;- Minimal reputational sensitivity  &lt;br&gt;- Regulatory breach with minimal consequences and readily rectified  &lt;br&gt;- No media coverage or interest, operations as usual, restricted to internal communication only</td>
<td>- An event to all areas, the impact of which can be absorbed through normal activity  &lt;br&gt;- Negligible impact on operations  &lt;br&gt;- Unexpected/ unplanned loss of a single staff member  &lt;br&gt;- Outage resolved within routine operations</td>
</tr>
</tbody>
</table>
ERM Process - *Risk Assessment*

- Document a simple risk criteria to be used and cover the full spectrum.

- 5x5 risk matrix (instead of 3x3). 5x5 matrix allows less "centralization" of the risk assessments - more detail and clarity.

- Consider different levels for High Risks.

- Ensure risk criteria is used during risk assessment.

- Awareness about risk criteria.
ERM Process - *Risk Assessment*

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
<th>Within Tolerance</th>
<th>Above Tolerance</th>
<th>Mitigate</th>
<th>Transfer</th>
<th>Avoid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should Occur</td>
<td>1. Insignificant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Minor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Moderate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Extreme</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unexpected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk assessment strategies:
- Mitigate
- Transfer
- Avoid
## Risk Register

### Section 1: Risk Identification

<table>
<thead>
<tr>
<th>Risk # and Title</th>
<th>Risk Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Goals</td>
<td></td>
</tr>
<tr>
<td>Description of Risk</td>
<td></td>
</tr>
<tr>
<td>Unit/Team</td>
<td></td>
</tr>
<tr>
<td>Risk Factors</td>
<td></td>
</tr>
<tr>
<td>Risk Consequences</td>
<td></td>
</tr>
</tbody>
</table>

Existing Mitigating Strategies:

<table>
<thead>
<tr>
<th>RISK RATING</th>
<th>INHERENT RISK</th>
<th>RESIDUAL RISK</th>
<th>RESIDUAL RISK TREND</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk Level</td>
</tr>
<tr>
<td></td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk Level</td>
</tr>
</tbody>
</table>

### Section 2: Risk Mitigation

**RISK TREATMENT:**

- Possible Mitigation Options
- Analysis Result (Accept/Reject)

**RISK MITIGATION STRATEGIES**

<table>
<thead>
<tr>
<th>Action Item</th>
<th>Action By</th>
<th>Timeline</th>
</tr>
</thead>
</table>

Resource Requirement:

Reporting and Monitoring Required:

Completed By:  Date:
ERM Governance Model

**Executive Team/Board**
- Provide risk management philosophy direction.
- Approve risk management approach, strategies and key policies.
- Be aware of and concur with risk appetite.
- Provide leadership to the organization in respect of the ERM program.
- Approve frameworks, methodologies, and tools for the identification, assessment, management and monitoring of business risks.
- Monitor effectiveness of the ERM Framework.

**Audit and Risk Management Committee**
- Approve frameworks, methodologies, and tools for the identification, assessment, management and monitoring of business risks.
- Develop ERM policies, including defining roles and responsibilities.
- Develop a common risk management language.
- Develop processes, procedures and tools for the identification, assessment, measurement, management and monitoring of business risks.
- Accountable for mitigation of individual risks.
- Mitigate/monitor individual risks.
- Report risk status.

**ERM Participants**
- Execute risk management activities in accordance with the ERM Framework.
- Assess adequacy of and compliance to ERM policies and procedures.
- Provide independent evaluation of compliance with the ERM Guidelines, Framework and Process.
- Use the risk assessment as input in the preparation of a risk-based Internal Audit Plan.

**Internal Audit**
- Assess adequacy of and compliance to ERM policies and procedures.
- Provide independent evaluation of compliance with the ERM Guidelines, Framework and Process.
- Use the risk assessment as input in the preparation of a risk-based Internal Audit Plan.

**Risk Management (Office / Role / SME)**
- Risk Owners Accountability

**Risk Owner**
- Accountable for mitigation of individual risks.
- Mitigate/monitor individual risks.
- Report risk status.

**Internal Audit**
- Assess adequacy of and compliance to ERM policies and procedures.
- Provide independent evaluation of compliance with the ERM Guidelines, Framework and Process.
- Use the risk assessment as input in the preparation of a risk-based Internal Audit Plan.

**Risk Owner**
- Accountable for mitigation of individual risks.
- Mitigate/monitor individual risks.
- Report risk status.
Risks

• High occupancy.
• Wrong identification of patients.
• Staff credentialing / Employing temporary staff.
• Floating nurses.
• Employee theft.
• Unauthorized access to medical records.
• Medical waste.
• Failure of critical equipments.
• Infection Control.
• Disaster planning.
• Lack of funding.
• Compliance with federal / local regulations.
Q&A

Gustavo Meschler, IS Eng, CISA, PMP, CRMA, ABCP
Enterprise Risk Services
DIRECT 204.927.3097
CELL 204.229.0585

FAX 204.783.8329
2500 - 201 Portage Ave.
Winnipeg, MB
R3B 3K6

Gustavo.meschler@mnp.ca
mnp.ca