ERM: Risk Maps and Registers

Performing an ISO 31000 Risk Assessment
Agenda

• Following a Standard?
• Framework First
• Performing a Risk Assessment
• Assigning Risk Ownership
• Data Management
• Questions?
Following a Standard?
ISO 31000

The International Risk Management Standard

ISO 31000 Provides the Architecture
The International Risk Management Standard

ISO 31000

Scalable and Tailorable
ISO 31000 Risk Management Model

**Principles**
- Creates value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured and timely
- Based on best available information
- Tailored
- Takes human and cultural factors into account
- Transparent and inclusive
- Dynamic, iterative and responsive to change
- Facilitates continual improvement and enhancement of the organization

**Framework**
- Mandate & Commitment
- Design framework for managing risk
- Continuously improve the framework
- Implement risk management
- Monitor and review the framework

**Process**
- Establish the context
- Communicate and consult
- Risk assessment
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Monitor and review
Framework First
Written Risk Management Framework

• Best way to get everyone on board
• Answers the questions:
  “Why do we manage risk at ABC?”
  “How do we manage risk at ABC?”

• Sections can cover:
  - Framework objective
  - Mandate & commitment
  - Risk appetite
  - Guiding principles
  - Roles & accountabilities
  - Applying the framework
  - Performance monitoring
  - Reporting
  - Quality & improvement
  - Committee charge
Incorporated Into Strategy, Operations & Decisions

- Three levels of risk to consider

- Strategic
- Operational
- Decision-Making
Governance

Risk as Pillar of Governance
Governance

Mission

The board sets the overall mission and objectives of the organization and insists that its culture and values are aligned with that mission.
Risk as Pillar of Governance

**Governance**

**Strategy**

Senior leadership, in conjunction with the board, develop strategic plans to carry out the organization’s mission and objectives.
Risk as Pillar of Governance

**Governance**

**Mission**

**Strategy**

**Stewardship**

Financial resources are developed and maintained to ensure the mission and strategic plans are adequately funded.
Risk as Pillar of Governance

Quality
The quality of the organization’s programs are planned for and tested in order to maintain demand for the “product” in the long-term.
Risk as Pillar of Governance

Risk
Risks to the organization in meeting its organizational objectives, including threats and opportunities, are identified, assessed, and treated.
Risk as Pillar of Governance

**Compliance**
Risks to the organization for failing to comply with its legal, regulatory, industry, and internal standards are identified, assessed, and managed.
Risk as Pillar of Governance

A strong management structure and culture is maintained to ensure proper reporting and accountability, and internal and external audits are utilized to bring board assurance.
Performing a Risk Assessment

ISO 31000 RM Process

- Establish the context
- Risk assessment
  - Risk identification
  - Risk analysis
  - Risk evaluation
  - Risk treatment
- Communicate and consult
- Monitor and review
Risk Assessment Considerations

- What is the context of this risk assessment?
- Who should be there?
  - Senior leadership
  - Risk committee
  - Ad hoc team
  - Risk management
- Identification of internal and external stakeholders
- How precise to be
  - ISO 31000 details 31 risk assessment methods
  - But normally looking for reasonable consensus and “gut feel”
- Agree on risk criteria
Risk Assessment Process

- **Risk Identification**
  - Risk register
  - Developed through:
    - Brainstorming
    - Interviews
    - Surveys
    - Other institutions
    - Associations

- **Risk Analysis**
  - Ranking based on likelihood and consequence (impact)
  - Use of heat maps

- **Risk Evaluation**
  - Prioritization
Risk (Heat) Maps

- Visual tool to plot likelihood and impact scores
  - Let’s the viewer easily identify top risks
  - Highlights need for risk treatment and to drive risks from top right to bottom left
- A risk tolerance line can easily be drawn
- Excellent for senior leadership and Board presentations
Risk Assessments – Day Of

- Use of technology
  - Survey tools
  - Spreadsheet
- Have “placemat” ready
- Usually start with subject matter expert
  - Then rest of group agrees or challenges
- Can also agree on risk ownership at same time
What Happens After the Risk Assessment?

• Each risk turned over to owner
  - To draft risk treatment plan
  - To determine team needed
• Risk owners report back to leadership for approval of plan
  - Through committee
  - Through management structure
• Risk owners work their plans with accountability to central oversight
• Rerank risks as treatment plans are implemented
• Report to senior leadership, audit committee, and/or full board
Assigning Risk Ownership
Employment of “Ownership” Model is Critical

• Pushing work out to subject matter experts is essential to success

• Risk owners:
  - Develop risk treatment plans
  - Assemble work teams
  - Communicate and report
  - Monitor and evaluate

• At what level of the organization should ownership reside?
Central Oversight/Decentralized Implementation

<table>
<thead>
<tr>
<th>Oversight</th>
<th>Centralized</th>
<th>Decentralized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decentralized</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Where some have developed, but centralized implementation requires significant staff and does not take advantage of current subject matter expertise. Decentralized oversight is at highest levels, including board, but implementation is pushed out to experienced subject matter experts through risk and compliance "ownership." Where most institutions have been, although with some limited departmental oversight, but does not incorporate board-level reporting and accountability.
### Central Oversight/Decentralized Implementation

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Decentralized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centralized</strong></td>
<td>Where some have developed, but centralized implementation requires significant staff and does not take advantage of current subject matter expertise</td>
</tr>
</tbody>
</table>

**Decentralized**

Oversight is at highest levels, including board, but implementation is pushed out to experienced subject matter experts through risk and compliance “ownership”.

Where most institutions have been, although with some limited departmental oversight, but does not incorporate board-level reporting and accountability.
## Central Oversight/Decentralized Implementation

<table>
<thead>
<tr>
<th>Oversight</th>
<th>Centralized</th>
<th>Decentralized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
<td>Where some have developed, but centralized implementation requires significant staff and does not take advantage of current subject matter expertise</td>
<td></td>
</tr>
<tr>
<td>Decentralized</td>
<td>Where most organizations have been, although with some limited departmental oversight, but does not incorporate board-level reporting and accountability</td>
<td></td>
</tr>
</tbody>
</table>
## Central Oversight/Decentralized Implementation

<table>
<thead>
<tr>
<th>Oversight</th>
<th>Centralized</th>
<th>Decentralized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation</td>
<td>Centralized: Where some have developed, but centralized implementation requires significant staff and does not take advantage of current subject matter expertise.</td>
<td>Decentralized: Oversight is at highest levels, including board, but implementation is pushed out to experienced subject matter experts through risk “ownership”. Where most organizations have been, although with some limited departmental oversight, but does not incorporate board-level reporting and accountability.</td>
</tr>
</tbody>
</table>
Reporting & Accountability Clearly Addressed

Accountability and “Surveillance” Pushes Down

Reporting Flows Up
Data Management
Administrative Tools

• Spreadsheets
• Enterprise software
• Governance, Risk & Compliance (GRC) software
  - As part of RMIS
  - As stand-alone cloud system

Functions to look for:

• Detailed risk and compliance obligation registers with multiple data points
• Dashboards for each risk and obligation with the ability to rank risks and catalogue treatment plans
• Risk rankings that flow into interactive, institutional heat maps
• Ability to manage delegations using email assignments and workflow through calendars
• Reporting tools for use at all levels of the organization
Questions?