Internal Audit’s Role in Enterprise Risk Management
Outline

• Why Enterprise Risk Management
• Definition
• Difference between traditional risk management and ERM
• Roles
• Maturity model
• Enterprise Risk Management - Frameworks
• Enterprise Risk Management - key terms
• Enterprise Risk Management - Risk Categories
• Enterprise Risk Management - Risk Implementation
• Enterprise Risk Management Process
• Enterprise Risk Management – Tools
• Summary
• Conclusion
Why Enterprise Risk Management?
Definition

ERM deals with risks and opportunities affecting value creation or preservation, defined as follows:

COSO

ERM is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

ERM is the leading approach to managing and optimizing risks, enabling an organization to determine how much uncertainty and risk are acceptable to an organization.
# Difference between traditional risk management and ERM

<table>
<thead>
<tr>
<th>Traditional risk management</th>
<th>Enterprise Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragmented</td>
<td>Integrated</td>
</tr>
<tr>
<td>Ad hoc</td>
<td>Continuous</td>
</tr>
<tr>
<td>Historical focused</td>
<td>Forward focused</td>
</tr>
<tr>
<td>Cost based</td>
<td>Value-based</td>
</tr>
<tr>
<td>Risk silos</td>
<td>Systematic</td>
</tr>
<tr>
<td>Functionally-driven</td>
<td>Process-driven</td>
</tr>
</tbody>
</table>
Roles – Three Lines of Defense

Source: The Institute of Internal Auditors, Inc.
Roles – Groups involved in Enterprise Risk Management

<table>
<thead>
<tr>
<th>Risk Governance</th>
<th>Board of Directors (and the Audit Committee)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Foster a risk Intelligent culture</td>
</tr>
<tr>
<td></td>
<td>• Approve risk appetite</td>
</tr>
<tr>
<td></td>
<td>• Ratify key components of the Enterprise Risk Management (ERM) programme</td>
</tr>
<tr>
<td></td>
<td>• Discuss enterprise risks with executive management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Infrastructure and Management</th>
<th>Executive management:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Define the risk appetite</td>
</tr>
<tr>
<td></td>
<td>• Evaluate proposed strategies against risk appetite</td>
</tr>
<tr>
<td></td>
<td>• Provide timely risk-related information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enterprise risk group:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Aggregate risk information</td>
</tr>
<tr>
<td>• Identify and assess enterprise risks</td>
</tr>
<tr>
<td>• Monitor risks and risk response plans</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internal Audit:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide assurance on effectiveness of the ERM programme, and the controls and risk response plans for significant risks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Management:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Create a common risk framework</td>
</tr>
<tr>
<td>• Provide direction on applying framework</td>
</tr>
<tr>
<td>• Implement and manage technology systems</td>
</tr>
<tr>
<td>• Provide guidance and training</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technology (all pervasive):</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide periodic/real-time dashboards to oversee risks</td>
</tr>
<tr>
<td>• Make monitoring and reporting easier</td>
</tr>
<tr>
<td>• Support timely maintenance and pre-empt problems</td>
</tr>
<tr>
<td>• Facilitate risk escalations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Ownership</th>
<th>Business units:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Take intelligent risks</td>
</tr>
<tr>
<td></td>
<td>• Identify and assess risks</td>
</tr>
<tr>
<td></td>
<td>• Respond to risks</td>
</tr>
<tr>
<td></td>
<td>• Monitor risks and report to enterprise risk group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Support functions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide guidance/support to the enterprise risk group and business units</td>
</tr>
</tbody>
</table>

Source: [https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-erm-a-risk-intelligent-approach.pdf](https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-erm-a-risk-intelligent-approach.pdf)
Roles – Internal auditing’s role in ERM

Internal auditors will normally provide assurances on three areas:

1. Risk management processes, both their design and how well they are working;
2. Management of those risks classified as ‘key’, including the effectiveness of the controls and other responses to them; and
3. Reliable and appropriate assessment of risks and reporting of risk and control status.

Internal audit activity may undertake are the following consulting roles:

1. Making available to management tools and techniques used by internal auditing to risks and controls;
2. Being a champion for introducing ERM into the organization, leveraging its expertise in risk management and control and its overall knowledge of the organization;
3. Providing advice, facilitating workshops, coaching the organization on risk and control and promoting the development of a common language, framework and understanding;
4. Acting as the central point for coordinating, monitoring and reporting on risks; and
5. Supporting managers as they work to identify the best way to mitigate a risk.
Roles – Internal auditing’s role in ERM

Source: IIA position paper: The role of internal auditing in Enterprise-wide Risk Management
Roles – Internal auditing’s role in ERM

Safeguards

Internal auditing may extend its involvement in ERM, as shown in the previous figure, provided the following conditions apply:

1. It should be clear that management remains responsible for risk management.
2. The nature of internal auditor’s responsibilities should be documented in the internal audit charter and approved by the audit committee.
3. Internal auditing should not manage any of the risks on behalf of management.
4. Internal auditing should provide advice, challenge and support to management’s decision making, as opposed to taking risk management decisions themselves.
5. Internal auditing cannot also give objective assurance on any part of the ERM framework for which it is responsible. Such assurance should be provided by other suitably qualified parties.
6. Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.
Maturity model

ERM Maturity Model

Level 1
Initial
- The organization has minimal/no awareness of risk management
- Risk Management and processes are performed on an ad hoc basis by individuals

Level 2
Emerging
- Risk Management applied inconsistently with limited standardization
- Some formal processes in place

Level 3
Conforming
- A risk management framework exists with documented risk management principles.
- Risk management applied consistently throughout
- Most processes are implemented

Level 4
Advanced
- The organization is proactive in risk management
- Risk management is consistently and fully implemented across the organization
- Key risk indicators (KRI) are used for major risks
- Risk management processes are monitored and reviewed for continuous improvements.

Level 5
Optimal
- Risk Management is considered a value driver and proactively used for day to day decision making and pursuit of opportunities
- KRI and predictive risk analytics are proactively used to identify and monitor risk
- Advanced and sophisticated risk management processes are used

Source: www.morganfranklin.com
There are two well known frameworks:

1. COSO ERM framework
2. ISO 31000
Enterprise Risk Management – Key terms

Risk - A potential event with an undesirable/negative outcome, including the potential failure to capitalize on an opportunity.

Impact - Estimated financial cost that would be realized if a risk event were to occur. It is determined using the impact on revenue over a 36 month period.

Likelihood - The probability that a risk will occur.

Risk appetite - A target level of loss exposure that the organization views as acceptable, given business objectives and resources

Risk tolerance - Degree of variance from the it’s risk appetite that the organization is willing to tolerate

Risk owner - The Risk Owner is the individual identified to lead the development and implementation of the Risk Mitigation plan

Risk management framework - components that support and sustain risk management throughout an organization.

Risk profile - A comprehensive view of the risks faced by the organization.

Risk assessment - The process of identifying and analyzing risk.

Risk retention - If an identified Risk is within Risk Retention, then current controls are retained, maintained, and the identified Risk is monitored.

Threat - Something with the potential to cause damage, injury, or loss.
Enterprise Risk Management – Risk Categories

**Category 1: Preventable Risks**
- Risks arising from within the company that generate no strategic benefits

**Risk Mitigation Objective**
- Avoid or eliminate occurrence cost-effectively

**Control Model**
- Integrated culture-and-compliance model:
  - Develop mission statement; values and belief systems; rules and boundary systems; standard operating procedures; internal controls and internal audit

**Category 2: Strategy Risks**
- Risks taken for superior strategic returns

**Risk Mitigation Objective**
- Reduce likelihood and impact cost-effectively

**Control Model**
- Interactive discussions about risks to strategic objectives drawing on tools such as:
  - Maps of likelihood and impact of identified risks
  - Key risk indicator (KRI) scorecards
  - Resource allocation to mitigate critical risk events

**Category 3: External Risks**
- External, uncontrollable risks

**Risk Mitigation Objective**
- Reduce impact cost-effectively should risk event occur

**Control Model**
- “Envisioning” risks through:
  - Tail-risk assessments and stress testing
  - Scenario planning
  - War-gaming
Enterprise Risk Management Implementation

Figure 1: ERM Implementation Steps

The implementation in five phases as shown below:

1. Planning
2. Designing ERM Framework
3. Implementing ERM
4. Measuring
5. Learning
Phase one – Planning the Project:

1. Planning

Focuses on identifying the project implementation team, establishing and reviewing agreements, planning and organizing the tasks.
Phase two – Designing ERM Framework:

Focuses on the design and development of overarching ERM governance including org. structure, ERM policy, risk classification system, common risk terminology, and tools and templates.
Phase three – Implementing ERM:

Focuses on identifying, evaluating, documenting and reviewing the organization’s risk portfolio. It also involves developing and monitoring responses to the identified risks. Activities in this phase are as shown in the following diagram:
1. **Context Identification** – Leadership identifies the context with reference to which risks will be identified e.g. strategic objectives, business process, auditable entities, or entire enterprise.

2. **Risk Identification** – Leadership identifies enterprise risks and their sub-related risks within the identified context.

3. **Risk Evaluation** – Leadership prioritizes risks based on impact, likelihood and/or other dimension.

4. **Risk Response** – Leadership assesses the controls in place, determines and implements appropriate activities, tools or other mechanism to modify the risks to a tolerable level.

5. **Monitoring & Communication** – Leadership reviews risks and risk action plans for ongoing effectiveness, communicating with stakeholders, and learning from experience.
Phase four – Measuring:

4. Measuring

Focuses on identifying the effectiveness of the ERM framework. Activities in this phase include:

b. Review the risk awareness within the enterprise.
c. Review the alignment of risk management within the organization’s activities.
Phase five – Learning:

Focuses on identifying the effectiveness of the ERM framework. Activities in this phase include:

a. Report ERM implementation results to stakeholders.
b. Use feedback to make improvements to the ERM framework.
c. Align ERM with other management tasks.
The organization uses risk event cards to assess its strategy risks. First, managers document the risks associated with achieving each of the company’s strategic objectives. For each identified risk, managers create a risk card that lists the practical effects of the event’s occurring on operations. Below is a sample card looking at the effects of an interruption in deliveries, which could jeopardize the organization’s strategic objective of achieving a smoothly functioning supply chain.

Risk Report Card

The organization summarizes its strategy risks on a Risk Report Card organized by strategic objectives (excerpt below). Managers can see at a glance how many of the identified risks for each objective are critical and require attention or mitigation. For instance, the organization identified 11 risks associated with achieving the goal “Satisfy the customer’s expectations.” Four of the risks were critical, but that was an improvement over the previous quarter’s assessment. Managers can also monitor progress on risk management across the company.
<table>
<thead>
<tr>
<th>Risks</th>
<th>Current Management and Mitigation</th>
<th>Risk Rating with Existing Controls</th>
<th>Changes to Controls</th>
<th>Change to Control Effectiveness</th>
<th>Risk Rating after Changes to Controls</th>
<th>Accountable Person/Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domestic terrorism (animal rights activists, eco-terrorists, stem-cell research opponents, etc.)</td>
<td>System-wide liaison with law enforcement; additional training of campus law enforcement; improved security measures; hardening of buildings; communication and response protocols</td>
<td>Adequately controlled</td>
<td>Continue current efforts with current controls.</td>
<td>No Change</td>
<td>Adequately controlled</td>
<td>UC Police</td>
</tr>
<tr>
<td>Catastrophic natural event (earthquake, fire, etc.)</td>
<td>Mission continuity UC Ready; seismic safety and retrofitting programs; emergency management</td>
<td>Potentially poorly controlled</td>
<td>Continue current efforts with current controls.</td>
<td>No Change</td>
<td>Potentially poorly controlled</td>
<td>EH&amp;S</td>
</tr>
<tr>
<td>Pandemic</td>
<td>Mission continuity UC Ready</td>
<td>Potentially poorly controlled</td>
<td>Creation of specific pandemic plans and emergency management protocol.</td>
<td>Moderate improvement</td>
<td>Adequately controlled</td>
<td>EH&amp;S</td>
</tr>
<tr>
<td>Laboratory safety</td>
<td>ISEM Policy; safety programs; BSAS funding; Safety Program Guidelines for Principal Investigator; hazardous waste management programs</td>
<td>Potentially over-controlled</td>
<td>Move BSAS funds to other priorities</td>
<td>Moderate decrease</td>
<td>Adequately controlled</td>
<td>EH&amp;S</td>
</tr>
<tr>
<td>Facilities and grounds safety</td>
<td>Building Maintenance Services; Grounds and Landscape Service, focused on operations.</td>
<td>Poorly controlled</td>
<td>Increase BSAS funding</td>
<td>Moderate improvement</td>
<td>Potentially poorly controlled</td>
<td>PPCS</td>
</tr>
<tr>
<td>Conflicts of Interest in financial transactions and agreements</td>
<td>Annual Conflict of Interest Reporting Systemwide by Designated Officials; Business Contract Policies; Conflict of Interest Coordinators; Whistle Blower system; Administrative Responsibilities Handbook (Principles of Conflict of Interest)</td>
<td>Potentially over-controlled</td>
<td>Continue current efforts with current controls.</td>
<td>No Change</td>
<td>Potentially over-controlled</td>
<td>Administration</td>
</tr>
<tr>
<td>Budget Impairment</td>
<td>General ad-hoc interaction with Legislature and Governor.</td>
<td>Poorly controlled</td>
<td>External financing program; Budget Officers; UC President working with Governor and Legislature</td>
<td>Significant Improvement</td>
<td>Potentially poorly controlled</td>
<td>Senior leadership</td>
</tr>
</tbody>
</table>
Questions to Board is interested in:

1. Is there an ERM process?
2. Who is leading that process?
3. Is it a board agenda item, how often, how much time?
4. Is there a common risk language that fosters communication?
5. Is there a process for assessing, prioritizing and risks?
6. Is there a gap analysis of the current and desired risk management capabilities, and what vision along with goals and objectives?
7. Is there a structured process to update the risk profile, appetite, and tolerances as new changes enter the environment?
8. How effective are those changes communicated to internal and external stakeholders?
Enterprise Risk Management – Tools

Specific questions:

1. Has an ERM glossary been created?
2. Have employee orientations related to risk management been done?
3. Is monitoring assigned to specific individuals who also communicate the results of the monitoring activity to appropriate levels in the organization?
4. Have formal communication mechanisms, such as a central web site or newsletter, been established? Is communication occurring on a regular basis?
5. Have management discussions occurred, with decisions made about how much risk the organization is willing to accept in key areas?
6. Has systematic documentation of risks and controls occurred in all functional areas of the organization?
7. Has the risk analysis resulted in the identification of the organization’s top risks?
8. Have alternative risk management strategies been identified for all of the identified top risk areas? Do strategies respond to changing social, environmental, and legislative conditions?
9. Do strategies respond to changing social, environmental, and legislative conditions?
10. Have any risk-management-related or other internal control measures/activities been identified for elimination?
11. Have benefits of assuming additional risk been identified?
12. Have competitive needs or reputation been discussed at a strategic level?
Enterprise Risk Management – Additional resources

- IIA position paper: The role of internal auditing in enterprise-wide risk management
- Deloitte whitepaper: Enterprise Risk Management, A ‘risk-intelligent’ approach
- A Risk Practitioners Guide to ISO 31000: 2018
- University of Wisconsin System: Enterprise Risk Management Handbook
Enterprise Risk Management is an integral part of governance.

The board is ultimately responsible for risk management but has delegated to management the role of establishing and operating the Enterprise Risk Management program.

Internal audit's key role is to provide assurance to management and the board. It may provide consulting services but should apply safeguards.

Any internal auditor who cannot demonstrate the appropriate skills and knowledge should not undertake work in the area of risk management.
Conclusion

Contact Information:

Gregory Kigen

Day time phone: 940-369-7560

Principal Auditor, UNT System

Email: Gregory.Kigen@untsystem.edu