Enterprise Risk Management in Colleges and Universities

Cherry Bekaert & Holland, L.L.P.

Neal Beggan, CISA, CRISC
Shane Hester, CPA, CISA
Introduction and Learning Objectives

**Learning Objective 1**: Enterprise Risk Management (ERM) is not a one size fits all endeavor, each organization has different cultures, needs, structures, and expectations—all of which need to be considered to design the right ERM solution for your organization.

**Learning Objective 2**: ERM value proposition needs to be defined, measured and reported. There are different stakeholders to consider when approaching ERM, all of whom may have different opinions on what the value proposition is to the organization.

**Learning Objective 3**: ERM is a process that needs to be sustained, not just an annual risk assessment.
ERM Defined
ERM is a principles-based approach to manage, not eliminate risk.

ERM is a process:
• Built into routine business practices
• Designed to:
  – Identify emerging events with the potential to affect the entity,
  – Assess the potential impact consistently, and
  – Manage risk within a predetermined risk appetite
• Geared to the achievement of objectives
• Applied across the enterprise
• Tied to the organization’s strategic goals

Leading companies use ERM as a critical tool to facilitate performance management
**Background**

**Issues Driving Focus on ERM**

The business and regulatory environments have become increasingly complex, raising institutional risk profiles.

**Higher Risk Profiles**

- Increasing scope and complexity of business activities
- Increasing risks from technologies (e.g., speed of execution, data vulnerability)
- Continuous changes in regulatory requirements
- Challenging and uncertain economic environment

**Higher Expectations**

- Regulators expect risk infrastructure to be commensurate with scale of business activities
- Banks and rating agencies (e.g., S&P and Moody’s) are evaluating risk management program effectiveness

**Higher Consequences**

Strategic consequences exist if institutions are unable to manage risk, compliance and control requirements effectively.

- Financial losses and/or damaged reputation
- Regulator action/legal noncompliance resulting in damaged reputation/costs
- Regulatory enforcement actions diminish operations and strategic opportunities
It is not a system or software application

Though tools are available they are not imperative and should not be a barrier to commencing an ERM process.

Sophisticated software should not become the focus of the process rather they should be used as a tool to help administer the process.

Maintaining the:

- Awareness
- Communication
- Transparency

....across organizational activity areas, departments, business units, is more important than having a sophisticated software application.
ERM Approach

Key considerations when identifying an ERM approach:

• **Why** – What has prompted you to start discussing ERM?

• **Objective** – What is your organization trying to achieve from an ERM program?

• **Investment** – What is the level of effort required to meet the expected benefits? What are you currently doing?

• **Impact** – How can the effort be sustained over a long period of time?
Keep it Simple

1. Strategic Analysis
2. Define Risk Profile
3. Evaluate Risks
4. Prioritize Activities

Planning

Validation

Meetings
The implementation of a more formal ERM process in an organization might begin with a project.

- Information gathering phase - obtain the perceptions of key process owners, stakeholders and others through one on one interviews, focus group discussions, surveys.

- Assimilate information - begin the process of identifying and evaluating objectives, risks and the strength of mitigation strategies.

- Assess risk initially as inherent or without the application of controls and mitigation strategies.

- Assess the robustness of mitigation strategies and controls in order to arrive at residual risks.

- Use an iterative approach to discuss and refine the assessment
Practical Implementation & Maintenance Considerations

Who should participate?

- Key members of management
- Key stakeholders
- Key process owners
- Representatives from key activity areas

Participation by all key activity areas is more critical than focusing on positions or titles.
## Role and benefits of stakeholders’ at different levels within the organization

<table>
<thead>
<tr>
<th>Role</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Board/ Audit Committee</strong>&lt;br&gt;• Provide oversight and input to the process&lt;br&gt;• Ensure significant risks of the organization are being identified and managed&lt;br&gt;• Hold management accountable for managing enterprise risk</td>
<td>• A formal risk reporting structure aligned with strategy and objectives&lt;br&gt;• A consistent view of risk reported from all levels of the organization&lt;br&gt;• Assurance that significant risks are managed</td>
</tr>
<tr>
<td><strong>Executive Team</strong>&lt;br&gt;• Embed risk considerations into strategic planning, goal-setting and initiative defining processes&lt;br&gt;• Provide risk insight and feedback&lt;br&gt;• Leverage ERM information for well-informed strategic decision-making and execution</td>
<td>• A formal risk reporting structure aligned with strategy and objectives&lt;br&gt;• A consistent view of risk for prioritization and decision-making&lt;br&gt;• Proactive, real-time risk identification</td>
</tr>
<tr>
<td><strong>VP Group</strong>&lt;br&gt;• Leverage ERM information/reporting in tactical decision making&lt;br&gt;• Ensure consistent alignment with organizational strategies and goals&lt;br&gt;• Provide risk insight and feedback</td>
<td>• Increased communication of dependencies across functional groups&lt;br&gt;• Open lines of communication regarding strategy, goals and expectations&lt;br&gt;• Proactive, real-time risk identification</td>
</tr>
<tr>
<td><strong>Risk Management</strong>&lt;br&gt;• Provide direction/leadership of ERM program&lt;br&gt;• Consolidate and assess enterprise risks&lt;br&gt;• Provide periodic reporting to stakeholders&lt;br&gt;• Engage in appropriate risk management responses&lt;br&gt;• Increase risk-consciousness across the company</td>
<td>• Receive assurance that significant risks are being considered and managed at all levels&lt;br&gt;• Ability to identify emerging opportunities for risk management</td>
</tr>
<tr>
<td><strong>Internal Audit</strong>&lt;br&gt;• Leverage relationships, audit work and stakeholder conversations to gather information, consolidate and assess enterprise risks&lt;br&gt;• Provide risk insight&lt;br&gt;• Provide assurance over ERM effectiveness</td>
<td>• Leverage risk assessment to align audit activities with enterprise risks&lt;br&gt;• Proactively increase risk-consciousness across the organization&lt;br&gt;• Identify emerging opportunities for ERM</td>
</tr>
</tbody>
</table>
1. Strategic Analysis

2. Define Risk Profile

3. Evaluate Risks

4. Prioritize Activities
ERM concerns itself with objectives, risks and mitigating strategies.

Therefore, organizational discussions of risk **should** be a natural part of strategy and objective setting:

- Weekly, monthly management meetings to discuss strategic plans, operational activities, financial results.
- Annual budgeting/forecasting process
- Management monitoring processes related to operational and financial results
- Strategic and activity planning processes

ERM does not have to be and probably should not be in most cases a separate set of processes.
Mitigating Strategies - the organization’s activities performed to accomplish its objectives.

- Board policies that define authorized management actions.
- Management policies that define authorized employee actions.
- Communication processes and systems that are implemented to provide policy, objectives, strategies, mission, core beliefs, etc. to key stakeholders of the organization (employees, students, alumni, vendors, government agencies, etc.).
- Control activities that management implements to ensure that organizational objectives are met.
- Monitoring activities performed by management to ensure that control activities are consistently implemented across the organization, properly designed for optimized effectiveness, performed by internal audit function at direction of Board to ensure that mitigating strategies are effectively operating.
1. Strategic Analysis

2. Define Risk Profile

3. Evaluate Risks

4. Prioritize Activities
Practical Implementation & Maintenance Considerations

Risk Appetite

Risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity’s risk management philosophy, and in turn influences the entity’s culture and operating style. Many entities consider risk appetite qualitatively, with such categories as high, moderate, or low, while others take a quantitative approach, reflecting and balancing goals for growth, return, and risk. A company with a higher risk appetite may be willing to allocate a large portion of its capital to such high-risk areas as newly emerging markets. In contrast, a company with a low risk appetite might limit its short-term risk of large losses of capital by investing only in mature, stable markets.

Risk appetite guides resource allocation. Management allocates resources among business units and initiatives with consideration of the entity’s risk appetite and the unit’s plan for generating desired return on invested resources. Management considers its risk appetite as it aligns its organization, people, and processes, and designs infrastructure necessary to effectively respond to and monitor risks.
Scenario

Down by 2
2 minutes left in the 4th quarter
4th down and goal 7 yards to go

What do you do?
ERM concerns itself with objectives, risks and mitigating strategies.

**Risks** – external and internal events that might occur or might not occur that have the potential to in some way affect the organization’s ability to achieve its objectives.

- Congress passes tax reform legislation that eliminates the deductibility of charitable contributions.
- Your President is arrested for making obscene phone calls from his University office.
- Your IT systems are compromised by hackers who remove medical, credit card and other personal data that you have collected from students, parents, etc.
- A major public university opens a branch campus within your footprint.
- Your accreditation is lost due to being unable to hire a sufficient number of PhD’s to replace retiring professors.
The depth and breadth of a risk assessment depends on the organization’s objectives and priorities

- Institutions should consider what is relevant to its objectives and perform the necessary risk assessments
- The risk assessment will provide a risk profile which is a comprehensive view of a set of risks which shows the impact and probability of each risk
- Risk profiles can be developed at different levels in the organization such as:
  - Enterprise level
  - Specific business unit/s
  - Specific function/s
  - Specific risk types
  - The entire organization
- Top-down versus bottom-up approach

Examples of Risk Assessment Types:
- Strategic risk assessment
- Operational risk assessment
- Compliance risk assessment
- Financial statement risk assessment
- Fraud risk assessment
- Market risk assessment
- Credit risk assessment
- Customer risk assessment
- Supply chain risk assessment
- Product risk assessment
- Security risk assessment
- Information technology risk assessment
- Project risk assessment
- Internal audit risk assessment
- Enterprise risk assessment
1. Strategic Analysis
2. Define Risk Profile
3. Evaluate Risks
4. Prioritize Activities
How Might an Organization Evaluate Risk?

**Inherent Risk** - the nature of a risk element without the application of controls or mitigating strategies.

- **Likelihood** - How likely is the event to occur.
- **Impact** - The severity of the event’s impact of the event should it occur.

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
<th>Inherent Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1=Low</td>
<td>1=Very Unlikely</td>
<td></td>
</tr>
<tr>
<td>3=Med</td>
<td>3-Possible</td>
<td></td>
</tr>
<tr>
<td>5=High</td>
<td>5=Highly Probable</td>
<td></td>
</tr>
<tr>
<td>4.000</td>
<td>4.500</td>
<td>4.250</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Inherent Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0 0 0 0 4 0</td>
</tr>
<tr>
<td>4</td>
<td>0 0 0 0 0 0</td>
</tr>
<tr>
<td>3</td>
<td>0 0 0 0 0 0</td>
</tr>
<tr>
<td>2</td>
<td>0 0 0 0 0 0</td>
</tr>
<tr>
<td>1</td>
<td>0 0 0 0 0 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4 5</td>
</tr>
</tbody>
</table>
How Might an Organization Evaluate Risk?

**Residual Risk** - the remaining risk after the application of risk mitigating strategies and controls.

- Inherent Risk - the uncontrolled nature of a risk element, determined by assessing likelihood and impact.
- Strength of controls and mitigating strategies applied to the risk.

<table>
<thead>
<tr>
<th>Inherent Risk</th>
<th>Mitigation Controls</th>
<th>Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1=Well Controlled</td>
<td></td>
</tr>
<tr>
<td>4.250</td>
<td></td>
<td>3.500</td>
</tr>
<tr>
<td>3=Average</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5=Not Controlled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Residual Risk</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inherent Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
</tbody>
</table>
How Might an Organization Evaluate Risk?

Uses of inherent risk and residual risk information:

- Provide management with a structured process for prioritizing activities and resources
- Identify areas requiring additional mitigating strategies, improvement in policy, procedural design
- Identify activity areas requiring enhancements in monitoring activities
- Identify areas for internal audit activities
A Third Dimension For Assessing Inherent Risk

Inherent Risk - The nature of a risk element without the application of controls or mitigating strategies.

- **Likelihood**: How likely is the event to occur.
- **Impact**: The severity of the event’s impact if it should occur.
- **Velocity**: How rapidly a risk event attains its maximum severity level.....Penn State?
Enterprise Risk Management in Colleges and Universities

1. Strategic Analysis
2. Define Risk Profile
3. Evaluate Risks
4. Prioritize Activities
Practical Implementation & Maintenance Considerations

ERM requires some degree of documentation showing the relationships among objectives, risks and mitigating strategies.

- How many objectives should be documented?
- How many risks should be documented?
- How many mitigating strategies and controls should be documented?

The answer is based on the characteristics of the organization and the organization’s environment, requires judgment, should be enough to continue a meaningful process, but not so many that the process is not maintainable.
Value of an Effective ERM

• Development of a framework that is applied across critical strategies/initiatives to build cross functional awareness regarding critical success factors.

• Development of a sustainable process that delivers clear value at all levels of the organization by embedding risk management principles throughout the organization and relying on minimal ERM-focused resources.

• Assessment of key risks tied to the goals and objectives of the organization at an enterprise level.

• Alignment of the senior leadership team and the board as to how the organization defines key risks and the education process of the importance of understanding the impact to the organization’s strategy

• Ability to embed risk management ownership and accountability into business process and planning.

• Integration of risk functions to improve risk and performance information availability, timeliness and transparency.
Is there an ERM vision for the future?

- Communicate the vision
- Define the roles
- Align it to the organization’s vision
- Have a compelling value proposition
## Common Pitfalls

Companies that do not adequately address the following areas are often not able to extract optimal value from their ERM programs

<table>
<thead>
<tr>
<th>Area</th>
<th>Issues</th>
<th>Impact</th>
</tr>
</thead>
</table>
| Focus of ERM Program      | • ERM process is solely focused on output to the Board; not utilized as a tool for management  
• ERM is focused solely on WCG or hazards                                | • Risk assessment is not embedded in strategic planning and business process  
• Management is disengaged from the process, because they don’t feel a value add |
| Risk Analysis             | • Risk appetite is not adequately defined and communicated  
• Risk levels are not measured against risk tolerance levels  
• Risk does not define inherent vs. residual risk  
• Risk impact is not quantified                                   | • Board/management lacks transparency to determine if risk levels are appropriate; if risks require further mitigation action or possible exploitation; and whether certain activities should be continued given risk levels and current mitigation steps |
| ERM Reporting             | • Reporting is limited to enterprise level and/or only a subset or risks are reported | • Risk reported to the Board are reported out of context  
• Board lacks transparency into overall risk profile/specific business unit risk |
| Managing Risks            | • Action/ mitigation plans and owners are not assigned to high risk areas | • Lack of clear accountability and proactive action plans may lead to risks going unattended |
Contact: Neal Beggan | Senior Manager
nbeggan@cbh.com | 703.584.8393 |

Shane Hester | Senior Manager
shester@cbh.com | 404.733.3329 |
www.cbh.com

Cherry, Bekaert & Holland, L.L.P.