What Every Executive Should Know About Enterprise Risk Management

Angela C. Dudones, C.P.A.
Director Finance – Enterprise Risk Management
CSX Corporation
Background on CSX Corporation

CSX is one of the nation's leading rail-based transportation companies

- Approximately $10 B Revenue
- 35,000 Employees
- 21,000 route mile rail network
- Serves 23 states & 70 ports in the U.S. and Canada
- 1,200 trains per day / 20,000 rail carloads per day
- 3,800+ locomotives and 101,000 freight cars maintained
Corporate leaders are facing unprecedented challenges

- Unparalleled economic conditions
- Increased complexity of transactions
- Vast financial pressures
- Heightened political / governmental influence
- Boundless technological advances (and complexity)

**Historical approaches to risk have proven inadequate in the new environment**
Effective Enterprise Risk Management is an increasingly essential imperative

Enterprise Risk Management is a comprehensive process used to reduce exposure from financial, business and strategic risk

Objectives:

- Establish and communicate consistent risk strategies, policies and processes
  - Develop clear risk management roles, accountability and governance
  - Identify and manage risk in accordance with corporate strategies and objectives
  - Promote a risk aware culture
ERM requires tailoring an approach to fundamental concepts

- Establishes consistent process across the enterprise
- Incorporates foundational corporate principals
- Originates from specific business strategies and objectives
- Assumes a holistic approach and a portfolio view
- Provides explicit accountability and course of action
- Offers insight into the breadth of outcomes
- Establishes clear governance over business risk
CSX ERM provides for a consistent, corporate-wide process

**Process**

**Capture**
Identifying risks to the company's goals and objectives

**Monitor**
Supporting oversight functions of management and the BOD

**Mitigate**
Implementing mitigation actions

**Evaluate**
Assessing and measuring corporate risks

**Content**

- Strategy
- Financial
- Operations
- Government
- External
- Climate
- Business
- Conditions
- Information
- Technology
- Compliance
- Human
- Capital
Every employee has a role in ERM

**Business Risk Management Roles**

- **BOD**
  - Overseeing ERM process and Key Enterprise Risks

- **E - Team**
  - Assessing and assigning responsibility for Key Enterprise Risks

- **Risk Oversight Committee (ROC)**
  - Establishing the ERM framework, process and integration within CSX

- **Process Owners (ERM, IT & IA&C)**
  - Conducting individual risk assessments and aligning with ERM

- **Functional Leadership / Risk Owners**
  - Identifying, assessing and monitoring risks within their area of responsibility

- **Employees**
  - Identifying risks and executing risk mitigation strategies
ERM establishes appropriate action and accountability for each risk

<table>
<thead>
<tr>
<th>Risk Name:</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mitigation Strategy:</strong></td>
<td></td>
</tr>
<tr>
<td>E-Team Lead:</td>
<td></td>
</tr>
<tr>
<td>Owner:</td>
<td></td>
</tr>
<tr>
<td>Mitigation Team:</td>
<td></td>
</tr>
</tbody>
</table>

**Risk Assessment Statement:**

<table>
<thead>
<tr>
<th>Risk Condition</th>
<th>Key Mitigation Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Condition</td>
<td>Mitigation Action 1</td>
</tr>
<tr>
<td>Risk Condition</td>
<td>Mitigation Action 2</td>
</tr>
<tr>
<td>Risk Condition</td>
<td>Mitigation Action 1</td>
</tr>
<tr>
<td>Risk Condition</td>
<td>Mitigation Action 2</td>
</tr>
</tbody>
</table>

**Risk Potential:**

<table>
<thead>
<tr>
<th>Threat Level:</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
</table>

**Risk Interdependencies:**
The process results in a comprehensive portfolio of risks

Sample Risk Universe

<table>
<thead>
<tr>
<th>Business Conditions</th>
<th>External Climate</th>
<th>Financial</th>
<th>Governmental</th>
<th>Human Capital</th>
<th>Operations</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competition</td>
<td>Economic Uncertainty</td>
<td>Counter-party</td>
<td>Legislative Issue A</td>
<td>Compensation</td>
<td>Operations Initiative A</td>
<td>IT Security</td>
</tr>
<tr>
<td>Reputaition</td>
<td>Acts of Terrorism</td>
<td>Leverage / Capital Structure</td>
<td>Legislative Issue B</td>
<td>Workforce Planning</td>
<td>Catastrophic Accident</td>
<td>Data Integrity</td>
</tr>
<tr>
<td>Supply Chain Disruption</td>
<td>Natural Disaster</td>
<td>Financial Flexibility</td>
<td>Regulatory Compliance</td>
<td>Safety &amp; Security</td>
<td>Key Infrastructure Loss</td>
<td>IT Operations</td>
</tr>
<tr>
<td>Legal</td>
<td>Public Health Emergency</td>
<td>Financial Reporting</td>
<td></td>
<td></td>
<td>Strategic Initiatives</td>
<td>IT Strategy</td>
</tr>
</tbody>
</table>

Tier I - High
Tier II - Moderate
Tier III - Low
Non-ERM Level
Reporting ensures appropriate oversight of key issues

"The role of the board of directors in enterprise-wide risk oversight has become increasingly challenging as expectations for board engagement are at all time highs."

Committee of Sponsoring Organizations of the Treadway Commission (COSO)
Common challenges of ERM can be avoided

- Get the right parties to the table
- Establish accountability upfront
- Ascertain and communicate the expected value
- Streamline with existing norms and processes
- Link to strategic and operational goals and objectives
- Establish as an ongoing process embedded within the organization
- Avoid over-managing uncertainty with limited potential value
Effective Enterprise Risk Management provides value to the organization

- Reflects complexity and variability of the business landscape
- Exposes vulnerability and opportunity in uncertainty
- Reduces surprises and minimizes negative impacts
- Better positions the company to capitalize on opportunity
- Ensures management is operating within corporate principles
- Aids leadership in fact-based decision making
- Provides transparency and reassurance to C-Suite and Board members
Closing ERM thoughts

• Effective Enterprise Risk Management better positions the company to avoid pitfalls and capitalize on opportunity.

• Risk *assessment* will not prevent the next big failure – action and governance is critical.

• The purpose of ERM is NOT to eliminate risk, but to manage it within the corporate principles and strategy.
Feel free to contact me with follow-up thoughts or questions

Angela C. Dudones, CPA
Director Finance – Enterprise Risk Management
Angela_Dudones@CSX.com