Enterprise Risk Management Application & Case Studies

Presented by Kristina Narvaez, MBA
President of ERM Strategies, LLC
Enterprise Risk Management

ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress.

By identifying and proactively addressing risks and opportunities, business enterprises protect and creates value for their stakeholders, including owners, employees, customers, regulators, and society overall.
Difference Between GRC & ERM

Governance Risk and Compliance (GRC)
Embraces compliance as a separate activity for each business silo.

Enterprise Risk Management (ERM)
Is concerned with delivering measurable business value by tying front line operational activities to goals across all business units.
Many organizations believe that they must continue to eliminate risk through compliance.

Risk has not been eradicated by regulation instead it has been driven underground.

Risk taking activities are not bad if an organization has established their risk appetite and risk tolerance levels and has the proper risk controls in place.
Risk Appetite and Risk Tolerance

- **Risk Appetite** is the manner in which an organization and its stakeholders collectively perceive, assess and treat risk.

- **Risk Tolerance** requires a company to consider in quantitative terms exactly how much of its capital it is prepared to put at risk.
ERM Is Used for Risk Optimization

- Considering both the upside and downside outcomes of risk-taking activities.
- When threats and opportunities are better understood, risk-taking is optimized, and managers, in turn, will make more informed business decisions.
- Improved decision making enables an organization to quickly meet emerging marketplace challenges.
Six Step Approach to ERM

1. Risk Identification
2. Risk Assessment
3. Risk Analysis
4. Implementation
5. Monitoring
6. Evaluation
1. Risk Identification

- The process of taking inventory of all risks in an organization and defining the potential risk event, the causes to that risk event, and the potential outcome if that risk event were to occur.

- Focus not only on hazard or operational risks, but also strategic, financial, reputational, compliance, environmental, human capital and technology, market, and supply chain risks.
Scope of Risk Identification

Define where the source of a potential risk event is coming from; Inside or Outside the organization. Establishing risk categories helps to identify the sources of a risk event.
Strategic Risk Categories

- Innovation Risk
- Customer Risk
- Market Risk
- Investor Risk
- R&D Risk
- Supply Chain Risk
- Partnering Risk
- Planning Risk
- Brand Risk
Operational Risk Categories

- Operational Risk
- Human Capital Risk
- Communication Risk
- Sustainability Risk
- Regulatory and Legal Risk
- Governance Risk
- Financial Reporting Risk
- Fraud Risk
- Emerging Risk
- Technology Risk
- Hazard Risk

1 Risk Identification
Other Risk Categories

- Reputational Risk
- Environmental Risk
- Third Party Risk
- Economic Risk
- Project Risk
- Investment Risk

Other
Identify Subcategories

Hazard Risk
Safety risk of increased slips, trips and falls accidents occurring in the organization

Operational Risk
Human capital risk of 25% of workforce is eligible for retirement in the next 5 years

Financial Risk
Credit risk of 35% of commercial loans will default in the third quarter

Strategic Risk
Sole supplier of a raw material has been acquired by competitor
Existing & Emerging Risk

Look not only at existing risks, but also the emerging risks to the organization.

- What new business processes have been added to the organization?
- What changes have been made in the organizational chart?
- What are some external risks that could impact the organization like economic, environmental, societal, geopolitical, and technological?
Know Where You Stand

1. Risk Identification

- Meet with senior management to define the strategic goals of your organization
- Review the mission and vision statements of the organization
- Define the expectations of internal and external stakeholders
Don’t Be Conflicted

GlaxoSmithKline – A study in conflicting strategic goals

This conflict caused the quality control of manufacturing to suffer.

Case in point – the Cidra Plant in Puerto Rico made 20 drugs under unhealthy conditions that lead to a $750 million FDA fine.

One of GSK’s strategic goals was to sell safe and effective prescription medication.

Another goal was to increase profitability by outsourcing manufacturing to other parts of the world.
Next Steps

1. Risk Identification

- Identify the risk management objectives to support the strategic goals of the organization
- Review the Risk Policy of the organization
- Create a SWOT Analysis (Strengths, Weaknesses, Opportunities, and Threats) reviewing the internal and external content of the organization
SWOT Analysis

- **Helpful** to achieving the objective
- **Harmful** to achieving the objective

**Internal origin (attributes of the organization)**
- **S**: Strengths
- **W**: Weaknesses

**External origin (attributes of the environment)**
- **O**: Opportunities
- **T**: Threats
Risk Identification Activities

**Brainstorming**
Can effectively generate lots of ideas of potential risk scenarios that could take place

**Structured Interviews**
Uses a risk survey or questionnaire to ask specific questions related to different types of potential risk events facing a particular risk owner or risk center

**Top Down / Bottom Up Approach**
Establish Risk Criteria

1. Risk Identification

- External and internal parameters for managing risk in an organization
- Responsibilities of risk owner
- Risk centers assigned to risk owner
- Determine critical risks in the organization.
- Prioritize the critical risks from greatest to least
The University of California has developed an ERM Work Plan for its employees. Within the context of campus/medical center’s mission, the management team establishes strategic goals, selects strategy and aligns ERM objectives to the strategic plan. The enterprise risk management framework is geared to achieving objectives in four categories:

- **Strategic**
  - High-level goals, aligned with and supporting their mission

- **Operations**
  - Effective and efficient use of their resources

- **Reporting**
  - Reliability of reporting

- **Compliance**
  - Compliance with applicable laws and regulations
Key Performance Indicators (KPI)

KPIs help you understand how well you are performing in relation to your strategic goals and objectives. In order for KPIs to be effective, they need to be measurable.

- % of customer attrition
- % of employee turnover
- Rejection rate
- Meantime to repair IT problems
- Customer order waiting time
- Profitability of customers by demographic segments
Key Risk Indicators (KRI) are leading indicators of risk to business performance. They give us an early warning to identify a potential event that may harm continuity of the activity/project.

<table>
<thead>
<tr>
<th>% of suppliers with no business continuity management</th>
<th>% of mission-critical recovery plans not exercised with the last 12 months</th>
<th>% turnover of mission-critical IT personnel</th>
<th>% of mission – critical business processes with a backup/recovery architecture</th>
</tr>
</thead>
</table>

1 Risk Identification
Some sources of risk are not directly under the control of the organization, but are a part of their supply chain.

March 11, 2011 - A massive tsunami devastated the coastline of Japan. GM, who might had a competitive advantage to their Japanese competitors, had a transmission that was manufactured in Japan for its Chevy Volt.
Cascading Effects

Business is interrupted

Loss of employees

Quality and productivity goes down

Competitor takes market share due to business interruption
**Tools and Techniques**

1. **Risk Identification**
   - Define business or process drivers of the organization
   - Conduct HAZOP and “what if” scenarios
   - Review what is said about your organization on social media networks

Tools and Techniques:

- **Flowcharts**
- **Personal Inspections**
- **Interview Subject Matter Experts**
- **Financial Statements**
- **Loss Histories**
- **Questionnaire & Risk Survey**
Create A Risk Register

1. Risk Identification

- Identify a potential risk event
- Categorize the risk event
- Identify potential causes
- Assign risk owner
- Determine the likelihood
- Determine the consequences
- What is the financial impact
- Risk treatment
- Date to review risk
## Sample Risk Register

### Risk Identification

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>T/O</th>
<th>Title</th>
<th>Probability</th>
<th>Schedule</th>
<th>C...</th>
<th>Score</th>
<th>Quality</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>T</td>
<td>Number of rigs just 31 against 54 agreed</td>
<td>VH (60%)</td>
<td>VH (60)</td>
<td>L...</td>
<td>VH</td>
<td>L</td>
<td>72</td>
</tr>
<tr>
<td>49</td>
<td>T</td>
<td>Dosing skids</td>
<td>VH (60%)</td>
<td>VL (2)</td>
<td>VL...</td>
<td>H</td>
<td>H</td>
<td>38</td>
</tr>
<tr>
<td>3</td>
<td>T</td>
<td>Tubing tongs</td>
<td>VH (60%)</td>
<td>VL</td>
<td>VL...</td>
<td>M</td>
<td>M</td>
<td>72</td>
</tr>
<tr>
<td>4</td>
<td>T</td>
<td>Organizational changes</td>
<td>L (15%)</td>
<td>L (7)</td>
<td>L...</td>
<td>L</td>
<td>M</td>
<td>18</td>
</tr>
<tr>
<td>5</td>
<td>T</td>
<td>Review and Approvals</td>
<td>H (60%)</td>
<td>H (30)</td>
<td>L...</td>
<td>L</td>
<td>VL</td>
<td>28</td>
</tr>
<tr>
<td>7</td>
<td>T</td>
<td>Maintenance</td>
<td>VH (60%)</td>
<td>N (0)</td>
<td>N...</td>
<td>VL</td>
<td>VH</td>
<td>72</td>
</tr>
<tr>
<td>X1</td>
<td>O</td>
<td>Shift rigs</td>
<td>M (30%)</td>
<td>VH (120)</td>
<td>L...</td>
<td>L</td>
<td>40</td>
<td>56</td>
</tr>
<tr>
<td>8</td>
<td>T</td>
<td>Weather</td>
<td>H (60%)</td>
<td>H (20)</td>
<td>L...</td>
<td>L</td>
<td>L</td>
<td>28</td>
</tr>
<tr>
<td>9</td>
<td>T</td>
<td>Injuries</td>
<td>L (15%)</td>
<td>L (7)</td>
<td>L...</td>
<td>L</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>10</td>
<td>T</td>
<td>Information and communication</td>
<td>VH (90%)</td>
<td>VH (60)</td>
<td>L...</td>
<td>L</td>
<td>L</td>
<td>72</td>
</tr>
<tr>
<td>11</td>
<td>T</td>
<td>Equipment availability</td>
<td>M (90%)</td>
<td>VH (120)</td>
<td>L...</td>
<td>L</td>
<td>40</td>
<td>56</td>
</tr>
<tr>
<td>12</td>
<td>T</td>
<td>Material, Equipment performance reliability</td>
<td>VL (5%)</td>
<td>N (0)</td>
<td>N...</td>
<td>M</td>
<td>H</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>T</td>
<td>Service, Technical performance reliability</td>
<td>L (15%)</td>
<td>H (30)</td>
<td>M...</td>
<td>M</td>
<td>H</td>
<td>12</td>
</tr>
<tr>
<td>14</td>
<td>T</td>
<td>Environment exposure</td>
<td>H (60%)</td>
<td>H (30)</td>
<td>M...</td>
<td>L</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>15</td>
<td>T</td>
<td>Maintenance training</td>
<td>VL (5%)</td>
<td>VL (2)</td>
<td>VL...</td>
<td>VH</td>
<td>VL</td>
<td>8</td>
</tr>
</tbody>
</table>

### Pre-Mitigation (Data Date = 25 Oct 07)

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>T/O</th>
<th>Title</th>
<th>Probability</th>
<th>Schedule</th>
<th>C...</th>
<th>Score</th>
<th>Quality</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>T</td>
<td>Number of rigs just 31 against 54 agreed</td>
<td>VH (60%)</td>
<td>VH (60)</td>
<td>L...</td>
<td>VH</td>
<td>L</td>
<td>72</td>
</tr>
<tr>
<td>49</td>
<td>T</td>
<td>Dosing skids</td>
<td>VH (60%)</td>
<td>VL (2)</td>
<td>VL...</td>
<td>H</td>
<td>H</td>
<td>38</td>
</tr>
<tr>
<td>3</td>
<td>T</td>
<td>Tubing tongs</td>
<td>VH (60%)</td>
<td>VL</td>
<td>VL...</td>
<td>M</td>
<td>M</td>
<td>72</td>
</tr>
<tr>
<td>4</td>
<td>T</td>
<td>Organizational changes</td>
<td>L (15%)</td>
<td>L (7)</td>
<td>L...</td>
<td>L</td>
<td>M</td>
<td>18</td>
</tr>
<tr>
<td>5</td>
<td>T</td>
<td>Review and Approvals</td>
<td>H (60%)</td>
<td>H (30)</td>
<td>L...</td>
<td>L</td>
<td>VL</td>
<td>28</td>
</tr>
<tr>
<td>7</td>
<td>T</td>
<td>Maintenance</td>
<td>VH (60%)</td>
<td>N (0)</td>
<td>N...</td>
<td>VL</td>
<td>VH</td>
<td>72</td>
</tr>
<tr>
<td>X1</td>
<td>O</td>
<td>Shift rigs</td>
<td>M (30%)</td>
<td>VH (120)</td>
<td>L...</td>
<td>L</td>
<td>40</td>
<td>56</td>
</tr>
<tr>
<td>8</td>
<td>T</td>
<td>Weather</td>
<td>H (60%)</td>
<td>H (20)</td>
<td>L...</td>
<td>L</td>
<td>L</td>
<td>28</td>
</tr>
<tr>
<td>9</td>
<td>T</td>
<td>Injuries</td>
<td>L (15%)</td>
<td>L (7)</td>
<td>L...</td>
<td>L</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>10</td>
<td>T</td>
<td>Information and communication</td>
<td>VH (90%)</td>
<td>VH (60)</td>
<td>L...</td>
<td>L</td>
<td>L</td>
<td>72</td>
</tr>
<tr>
<td>11</td>
<td>T</td>
<td>Equipment availability</td>
<td>M (90%)</td>
<td>VH (120)</td>
<td>L...</td>
<td>L</td>
<td>40</td>
<td>56</td>
</tr>
<tr>
<td>12</td>
<td>T</td>
<td>Material, Equipment performance reliability</td>
<td>VL (5%)</td>
<td>N (0)</td>
<td>N...</td>
<td>M</td>
<td>H</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>T</td>
<td>Service, Technical performance reliability</td>
<td>L (15%)</td>
<td>H (30)</td>
<td>M...</td>
<td>M</td>
<td>H</td>
<td>12</td>
</tr>
<tr>
<td>14</td>
<td>T</td>
<td>Environment exposure</td>
<td>H (60%)</td>
<td>H (30)</td>
<td>M...</td>
<td>L</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>15</td>
<td>T</td>
<td>Maintenance training</td>
<td>VL (5%)</td>
<td>VL (2)</td>
<td>VL...</td>
<td>VH</td>
<td>VL</td>
<td>8</td>
</tr>
</tbody>
</table>

### Post-mitigation

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>T/O</th>
<th>Title</th>
<th>Probability</th>
<th>Schedule</th>
<th>C...</th>
<th>Score</th>
<th>Quality</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>T</td>
<td>Number of rigs just 31 against 54 agreed</td>
<td>VH (60%)</td>
<td>VH (60)</td>
<td>L...</td>
<td>VH</td>
<td>L</td>
<td>72</td>
</tr>
<tr>
<td>49</td>
<td>T</td>
<td>Dosing skids</td>
<td>VH (60%)</td>
<td>VL (2)</td>
<td>VL...</td>
<td>H</td>
<td>H</td>
<td>38</td>
</tr>
<tr>
<td>3</td>
<td>T</td>
<td>Tubing tongs</td>
<td>VH (60%)</td>
<td>VL</td>
<td>VL...</td>
<td>M</td>
<td>M</td>
<td>72</td>
</tr>
<tr>
<td>4</td>
<td>T</td>
<td>Organizational changes</td>
<td>L (15%)</td>
<td>L (7)</td>
<td>L...</td>
<td>L</td>
<td>M</td>
<td>18</td>
</tr>
<tr>
<td>5</td>
<td>T</td>
<td>Review and Approvals</td>
<td>H (60%)</td>
<td>H (30)</td>
<td>L...</td>
<td>L</td>
<td>VL</td>
<td>28</td>
</tr>
<tr>
<td>7</td>
<td>T</td>
<td>Maintenance</td>
<td>VH (60%)</td>
<td>N (0)</td>
<td>N...</td>
<td>VL</td>
<td>VH</td>
<td>72</td>
</tr>
<tr>
<td>X1</td>
<td>O</td>
<td>Shift rigs</td>
<td>M (30%)</td>
<td>VH (120)</td>
<td>L...</td>
<td>L</td>
<td>40</td>
<td>56</td>
</tr>
<tr>
<td>8</td>
<td>T</td>
<td>Weather</td>
<td>H (60%)</td>
<td>H (20)</td>
<td>L...</td>
<td>L</td>
<td>L</td>
<td>28</td>
</tr>
<tr>
<td>9</td>
<td>T</td>
<td>Injuries</td>
<td>L (15%)</td>
<td>L (7)</td>
<td>L...</td>
<td>L</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>10</td>
<td>T</td>
<td>Information and communication</td>
<td>VH (90%)</td>
<td>VH (60)</td>
<td>L...</td>
<td>L</td>
<td>L</td>
<td>72</td>
</tr>
<tr>
<td>11</td>
<td>T</td>
<td>Equipment availability</td>
<td>M (90%)</td>
<td>VH (120)</td>
<td>L...</td>
<td>L</td>
<td>40</td>
<td>56</td>
</tr>
<tr>
<td>12</td>
<td>T</td>
<td>Material, Equipment performance reliability</td>
<td>VL (5%)</td>
<td>N (0)</td>
<td>N...</td>
<td>M</td>
<td>H</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>T</td>
<td>Service, Technical performance reliability</td>
<td>L (15%)</td>
<td>H (30)</td>
<td>M...</td>
<td>M</td>
<td>H</td>
<td>12</td>
</tr>
<tr>
<td>14</td>
<td>T</td>
<td>Environment exposure</td>
<td>H (60%)</td>
<td>H (30)</td>
<td>M...</td>
<td>L</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>15</td>
<td>T</td>
<td>Maintenance training</td>
<td>VL (5%)</td>
<td>VL (2)</td>
<td>VL...</td>
<td>VH</td>
<td>VL</td>
<td>8</td>
</tr>
</tbody>
</table>

### Risk Details

<table>
<thead>
<tr>
<th>ID</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Number of rigs just 31 against 54 agreed</td>
<td>1) operating areas claim that they have production losses and that wells are waiting for intervention or that other work over jobs are in progress and so they cannot provide additional rigs. During a presentation on 22nd of March 2016 it was agreed that the project will get 54 rigs, approximately 45 would work on new completions and 9 rigs would have to go back and perform interventions on wells. 1st delay of schedule in September expected, effect on project total 4 - 6 month.</td>
</tr>
</tbody>
</table>
Sample Risk Heat Map

WYCRR Heat Map 2011

Not Protectively marked

Relative Impact

Relative Likelihood

Risk rating

Very High
High
Medium
Low

Limited

Low
Medium Low
Medium
Medium High
High
Risk Tornado Diagram

Risk1
Risk2
Risk3
Risk 4
Risk 5

Tornado Diagram

Project Cost

-12000 -9000 -6000 -3000 0 3000 6000 9000 12000
Risk Assessment is a process to determine the cause of the risk event, the risk event itself, and the impact and the velocity of the risk event.

**Root Cause Analysis** - Find the root cause of a potential risk event

**Quantitative Assessment** - Measures the value of the impact

**Qualitative Assessment** - Recognizes the source of the risk event
## Causes of Risk

### Three Basic Causes

<table>
<thead>
<tr>
<th>Physical causes</th>
<th>Human causes</th>
<th>Organization causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A tangible or material item failed in some way.</td>
<td>People did something wrong or did not do something required.</td>
<td>A system, process or policy that people use to make decisions in doing their work is faulty.</td>
</tr>
<tr>
<td>Brakes stop working on a car</td>
<td>No one check the condition of the brakes</td>
<td>No procedure for checking the maintenance of the cars</td>
</tr>
</tbody>
</table>
Root Cause Analysis

Methods

- The "5-Whys"
- Barrier Analysis
- Change Analysis
- Parent Analysis
- Casual Factor Tree Analysis
- Fish-Bone Diagram or Ishikawa Diagram
- Fault Tree Analysis
- Management Oversight and Risk Tree
- Failure Mode Effect Analysis

2
Risk Assessment
Fault Tree Analysis

Very useful in examining the possible conditions that may lead to a desired or undesired event.

Top event will be placed at the top of the tree and all subsequent events that lead to the main event will be placed as branches.

Symbols provide a pictorial representation of the event and how it interacts with other events on the tree.
Qualitative Analysis

Positive Fault Tree Analysis
Will identify the events necessary to achieve a top desired event for example no accident in manufacturing facility

Negative Fault Tree Analysis
Constructed to show those events or conditions that will lead to a top undesired risk event such as a fire in the manufacturing facility

Risk Assessment
Quantitative Analysis

When the likelihood of an event is know and a probability value has be assigned, then analysis of these events on a fault tree will also yield quantitative results.

Financial impact can be added to each stage of the Fault Tree Analysis.

Risk correlation can be demonstrated.
State of Washington’s Nine Step Approach to Root Cause Analysis

1. Verify the incident and define the problem
2. Map a timeline of events
3. Identify critical events

- Analyze the critical event’s cause and impact
- Identify root causes
- Support each root cause with evidence

4. Identify and select the best solutions
5. Develop recommendations
6. Track implementation of solutions
3. Risk Analysis

Understand

Risk aggregation and risk correlation in an organization’s risk portfolio

Determine

The interrelationship of risk exposures to a potential risk event

Formulate

The best risk strategies for the organization from risk assessments
DHS plays a leadership role in the Nation’s unified effort to manage risk working across the homeland security enterprise which includes Federal, state, local, tribal, territorial, non-governmental and private sector entities.

As part of the analysis in their ERM program, DHS used an integrated risk management structure to share risk information and analysis.

The goal of using integrated risk management structure is to be able to work with its partners to address uncertainty inherent in their complex mission space, and help make the tough decisions necessary to keep the nation resilient and secure with limited resources.
DHS Analysis Tools

DHS uses Influence Diagrams to analyze the interrelationships and interdependencies of risks across the enterprise.
DHS uses analytic tools like RAPID-Risk Assessment Process for Informed Decision-Making to manage risks associated with their strategic goals.
Data analysis allows for more transparent and defensible decisions.

Contextualizes homeland security threats, showing which are the most likely and which have the highest impact.

Helps prioritization decisions among terrorism, natural disasters, cyber, pandemics, and border security hazards.

Provides a performance measure for programs across the homeland security mission space.

Identifies opportunities for reducing risk exposures of potential risk events.

Allows for understanding of the impact of combined risk exposures taking place at the same time.
4. Implementation

Implementation - incorporating an ERM structure, practices, and strategies to fulfill the goals of the organization.

- ERM framework
- Risk controls
- Risk champions and risk centers
- Risk communication structure
- Crisis management protocol
- Business Continuity
ERM Frameworks

**COSO II**
- Focus is to establish ERM goals as part of the strategic management process. It does not dive into the details of risk management approaches and process, but addresses threats to the organization and the need for proper controls.

**ISO 31000**
- Rooted in risk management principles and designed to provide an organized methodology to evaluate risk exposures and react to the environment.
Risk Controls

Management is responsible for implementing appropriate controls to reduce risk and to achieve operational objectives.

Some Areas for Risk Controls:
- IT Systems
- Financial & Operations
- Property & Assets
- Safety & Liability
Risk Champions and Risk Centers

**Risk Champions**

- Accountable for ensuring accuracy within their department or business unit around the identification, assessment, management and monitoring of risk
- They are the eyes and ears of risk information for the risk manager who is in charge of assessing risk across the enterprise
- Not necessarily responsible for performing the actual risk management activities

**Risk Center**

- A department or unit within the organization charged with the risk exposures that are related to their duties and responsibilities
“When we talk about growth strategies for the company, we talk deliberately about both risks and opportunities”

Janet Nasburg, Chief Risk Officer at Intuit

CRO and ERM program office have ownership and accountability for Intuit’s ERM program and drive Intuit’s ERM capabilities

Ownership and accountability for identified risks are shared by executive and business unit level leaders

Risk communication is not only to report progress, but also so that business units can share and leverage risk knowledge
Risk Communication Structure

Simple State System
The event can be resolved through routine decisions

Complicated State System
The event is more difficult to resolve than a simple system, but it not unusual

Complex State System
The event is unusual, and potentially critical to the organization

Chaotic State System
The event is a dramatic, unforeseen situation that threatens the organization’s survival

Implementation
Crisis Management

Risk communication becomes a key component in surviving a crisis situation.

Messages to all stakeholders must be clear, address the pressing issues and engage all the stakeholders to be diligent in plans of recovery.

Communication must demonstrate that senior management is committed to maintain an environment of transparency in its decision making.
Elements of Continuity Plan

- Statement of acceptable level of functioning
- Recovery time objectives, resources needed and potential failure points
- Task and activities required
- Structure to support the plan
- Supporting documentation and information
- Procedures and processes
- Description of personnel duties and responsibilities
- Describe interdependencies among the various departments
Monitoring involves communication of risk both upstream and downstream across the organization. It includes periodic reporting and follow-up on the risks by various levels of management, risk committees, and internal auditors.

KPIs and KRIs are a valuable way to monitor key risks linked to improved cash flows and earnings.
Tools Used for Monitoring

- **Spreadsheets**: Like risk registers
- **Balanced Scorecards**: Captures company’s strategy by
  - Customer
  - Internal Processes
  - Innovation and Learning
  - Financial
- **Dashboards**: Pictorial reporting of risks
- **Governance Risk and Compliance Software**: Focus on audit and compliance
- **Enterprise Risk Management Software**: ERM focus on software solutions
## Critical Risk: Mitigation Plan

<table>
<thead>
<tr>
<th>Project name</th>
<th>Project Impact Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM</td>
<td>Impact/Trigger Date</td>
</tr>
<tr>
<td>Risk Coordinator</td>
<td>Max Cost</td>
</tr>
<tr>
<td>Risk owner</td>
<td>Min Cost</td>
</tr>
<tr>
<td>Risk Score</td>
<td>Most likely Cost</td>
</tr>
</tbody>
</table>

| Risk Statement | (3 C’s format - Condition, Cause, Consequence) |
|               |                                               |

<table>
<thead>
<tr>
<th>Closure Criteria/Closure Statement</th>
<th>Closure Date</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Change Control Approved</th>
<th>Yes or No (circle one)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Mitigation action (Preventive)</th>
<th>Actionee</th>
<th>Action Deadline date</th>
<th>Action Deadline phase</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Contingency action</th>
<th>Use the chart below to show the risk score before and after mitigation</th>
</tr>
</thead>
</table>

5 Monitoring
Case Study: Walmart

Developed KPI and KRI metrics incorporated in a balanced scorecard.

Metrics used to track performance on risk and to determine the company’s progress in managing the risk.

Walmart also uses these metrics to determine the value added by the ERM process.

### KPI Selector

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Response Time Metric</th>
<th>Visiblity Metric</th>
<th>Productivity Metric</th>
<th>Shrinkage Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic value driver</td>
<td>x</td>
<td>function driven</td>
<td>x</td>
<td>function driven</td>
</tr>
<tr>
<td>Executive defined</td>
<td>x</td>
<td>function defined</td>
<td>x</td>
<td>function defined</td>
</tr>
<tr>
<td>Organization cascade</td>
<td>x</td>
<td>no</td>
<td>x</td>
<td>no</td>
</tr>
<tr>
<td>Enterprise standard</td>
<td>x</td>
<td>function specific</td>
<td>x</td>
<td>function specific</td>
</tr>
<tr>
<td>Quantifiable metric</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Based on valid data</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Easy to comprehend</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Relevant over time</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Provide context</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Empower user</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Promote positive action</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>KPI Status</td>
<td>KPI</td>
<td>Metric</td>
<td>KPI</td>
<td>Metric</td>
</tr>
</tbody>
</table>

5 Monitoring
6. Evaluation

Ascertaining the strengths and weaknesses of the ERM program with regard to the organization’s strategic goals

Risk Optimization / Value Creation

Evaluation

Return on Investment

ERM’s Role in Governance
Risk Optimization

Balance between taking on too much risk and not taking on enough risk to explore opportunities for growth

Explore various risk-return outcomes

Evaluate risk controls in place and decide the best use of financial resources to provide needed protection
Cost of Risk

Each year University of California holds an Annual ERM Summit focused on their continuous effort in improving their ERM program by reducing their Cost of Risk.

Case Study: University of California

Since 2003-2004 fiscal year, they have reduced Cost of Risk by $493 million dollars

Reduced the Cost of Risk from $18.46 per $1,000 of operating budget to $13.31 per $1,000 of operating budget
Risk Governance

Key drivers of success and risks in the company’s strategy

Crafting the right relationship between the board and its standing committees as to risk oversight

Establishing and providing appropriate resources to support risk management systems

Monitoring potential risks in the company’s culture and incentive systems

Developing an effective risk dialogue with management

Guidance principles for board risk oversight

National Association of Corporate Directors report, “Risk Governance: Balancing Risk and Reward”
The Executive Risk Committee Provides the Board of Directors with:

- A structure that provides the board with the appropriate information that defines the firm’s risk profile.
- A system that provides an audit of the effectiveness of the risk management process.
- A system that affords an evolving understanding of key risks to the company.

“Boards are now finally asking management about the nature of the risk information process in place. Boards want to gather information about new or emerging risks and the extent to which these risks require a more in-depth analysis. This is being done to ensure future opportunities and threats to the company’s performance are appropriately managed”.- John Bugalla, James Kallman, Chris Mandel and Kristina Narvaez in *The Corporate Board*
Thank you. Questions?

Presented by
Kristina Narvaez
President & CEO
ERM Strategies
www.erm-strategies.com