RISK IDENTIFICATION,
ASSESSMENT AND RESPONSE

Leveraging Enterprise Risk Management techniques to
strengthen Business Continuity Management practices

Workshop Agenda

- The Professional Landscape – Standards, Guidelines and Best Practices
- The Intersection of BCM and ERM
- What is Risk Anyway?
- Risk Identification
- Risk Assessment
- Risk Response
- BCM and ERM Resources
## BCM Standards, Guidelines and Best Practices

### Common Elements

<table>
<thead>
<tr>
<th>Common Elements</th>
<th>Issues Addressed by Common Elements</th>
</tr>
</thead>
</table>
| Risk Assessment and Impact Analysis | • Identify assets, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the organization and stakeholders.  
• Identify hazards and threats.  
• Establish a process for risk identification, analysis and evaluation.  
• Evaluate the effect of uncertainty on the organization's objectives.  
• Evaluate the likelihood of a disruptive event and its consequences on assets (human, physical, environmental, information, and intangible).  
• Evaluate and establish recovery time objectives. |

- Framework for Voluntary Preparedness
## The Discipline of Business Continuity Management

### Professional Practice Areas

- Program Initiation and Management
- **Risk Evaluation and Control**
- Business Impact Analysis
- Business Continuity Strategies
- Emergency Response and Operations
- Business Continuity Plans
- Awareness and Training Programs
- BCP Exercise, Audit and Maintenance
- Crisis Communications
- Coordination with External Agencies

Determine the risks (events or surroundings) that can adversely affect the organization and its resources (example(s) include: people, facilities, technologies) due to business interruption; the potential loss of such events can cause and the controls needed to avoid or mitigate the effects of those risks. As an outcome of the above, a cost benefit analysis will be required to justify the investment in controls.

---

## The Discipline of Business Continuity Management

### Professional Practice Areas

- Program Initiation and Management
- Risk Evaluation and Control
- **Business Impact Analysis**
- Business Continuity Strategies
- Emergency Response and Operations
- Business Continuity Plans
- Awareness and Training Programs
- BCP Exercise, Audit and Maintenance
- Crisis Communications
- Coordination with External Agencies

Identify the impacts resulting from business interruptions that can affect the organization and techniques that can be used to quantify and qualify such impacts. Identify time-critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be established and approved.
The Discipline of Business Continuity Management

Professional Practice Areas
- Program Initiation and Management
- Risk Evaluation and Control
- Business Impact Analysis
- Business Continuity Strategies
- Emergency Response and Operations
- Business Continuity Plans
- Awareness and Training Programs
- BCP Exercise, Audit and Maintenance
- Crisis Communications
- Coordination with External Agencies

Leverage the outcome of the BIA and Risk Evaluation to develop and recommend business continuity strategies. The basis for these strategies includes consideration of both the recovery time objectives and recovery point objectives to assess and plan for support of the organization’s critical functions.

The Discipline of Business Continuity Management

4.1.2 Risk assessment
4.1.2.1 There shall be a defined, documented and appropriate method for risk assessment that will enable the organization to understand the threats to and vulnerabilities of its critical activities and supporting resources, including those provided by suppliers and outsource partners.

4.1.2.2 The organization shall understand the impact that would arise if an identified threat became an incident and caused a business disruption.

4.1.3 Determining choices
4.1.3.1 For each of its critical activities, the organization shall identify available risk treatments that:
   a) reduce the likelihood of a disruption;
   b) shorten the period of disruption; and
   c) limit the impact of a disruption on the organization’s key products and services.

4.1.3.2 The organization shall choose and implement appropriate risk treatments for each critical activity in accordance with its level of risk acceptance.
Enterprise Risk Management
Conceptual Frameworks

- COSO’s Enterprise Risk Management – Integrated Framework
- The Australian/New Zealand Risk Standard
- Turnbull Report
- South Africa’s King Report on Corporate Governance
- Standard & Poor’s Enterprise Risk Management for Financial Institutions: Rating Criteria and Best Practices
- Casualty Actuarial Society’s Overview of Enterprise Risk Management

The Discipline of Enterprise Risk Management

<table>
<thead>
<tr>
<th>ERM – Integrated Framework</th>
<th>The Five Steps of ERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Internal Environment</td>
<td>1. Identifying the Risks</td>
</tr>
<tr>
<td>□ Objective Setting</td>
<td>2. Assessing the Risks</td>
</tr>
<tr>
<td>□ Event Identification</td>
<td>3. Evaluating the Risks</td>
</tr>
<tr>
<td>□ Risk Assessment</td>
<td>4. Mitigating the Risks</td>
</tr>
<tr>
<td>□ Risk Response</td>
<td>5. Monitoring the Plan</td>
</tr>
<tr>
<td>□ Control Activities</td>
<td></td>
</tr>
<tr>
<td>□ Information and</td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td></td>
</tr>
<tr>
<td>□ Monitoring</td>
<td></td>
</tr>
<tr>
<td>□ Roles and Responsibilities</td>
<td></td>
</tr>
</tbody>
</table>
Risk – the Intersection of BCM and ERM

What is a risk anyway?
Events or Uncertainty

An event is an incident or occurrence emanating from internal or external sources that affects implementation of strategy or achievement of objectives.

Events may have positive or negative impact, or both.

- Events with negative impact represent risks, which require management’s assessment and response.
- Events with positive impact represent opportunities, which management channels back into the strategy and objective-setting processes.

What Counts as Risk Management

Definition of Risk

- Long definition: The probability and magnitude of a loss, disaster, or other undesirable event
- Shorter (equivalent) definition: Something bad could happen

- Douglas W. Hubbard, The Failure of Risk Management
### What Counts as Risk Management

#### Definition of Management

- **Long definition:** The planning, organization, coordination, control, and direction of resources toward defined objective(s)

- **Shorter, folksier definition:** Using what you have to get what you need

  - Douglas W. Hubbard, *The Failure of Risk Management*

---

#### Definition of Risk Management

- **Long definition:** The identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events

- **Shorter definition:** Being smart about taking chances

  - Douglas W. Hubbard, *The Failure of Risk Management*
Risk Identification

Risk Identification, Assessment and Response

Risk Identification Techniques

Any number of techniques can be used to identify potential events affecting achievement of objectives:

- Risk Inventories
- Facilitated Workshops
- Interviews
- Questionnaires and Surveys
- Process Flow Analysis
- Leading Event Indicators and Escalation Triggers
- Loss Event Data Tracking
Risk Identification

Risk Inventories

- Use listings of potential risks common to a specific industry or functional area, developed by personal within the organization or from generic lists generated externally.

GM's ERM team assembled a four-quadrant map of vulnerabilities, documenting more than 100 types of events that had impacted the organization.

Facilitated Workshops

- Risk Identification workshops typically bring together cross-functional or multi-level individuals for the purpose of drawing on the group's collective knowledge.

Prior to the Workshop
- Identify experienced facilitator
- Establish and agree on ground rules
- Recognize the different participant styles and personality types
- Identify which category of risks on which to focus
- Invite an appropriate number of participants – normally 15 or fewer
- Set realistic expectations up front with respect to what the workshop is intended to achieve

Workshop Agenda

Introduction
- Explain background of workshop and why each participant has been invited
- Explain ground rules

Explain workshop process
- Risk are to be considered against corporate objectives
- The facilitator will prompt discussion on risks emanating from various factors, such as:
  - External
  - Economic
  - Environmental
  - Political
  - Social
  - Internal
  - Infrastructure
  - Personnel
  - Process
  - Technology
  - Technological
Interviews

- Typically conducted in a one-on-one setting, or sometimes two-on-one, where the interviewer is accompanied by a colleague taking notes. The purpose is to ascertain the individual's candid views and knowledge of actual past risks and potential risks.

**Interview Agenda**
1. Introduction
2. Provide background on the interview process
3. Confirm the person's current role and responsibilities
4. Confirm they received and read background material

**Strategies and Objectives**
1. Identify key business functions
2. Determine the established risk tolerances
3. Discuss factors related to potential events relative to business function
4. Identify potential events creating risks to business
5. Consider how the interviewee prioritizes these events, considering likelihood and impact
6. Identify events that have occurred in the past 12 months
7. Consider whether risk identification mechanisms need to be enhanced

---

Questionnaires and Surveys

- Use questionnaires and surveys to address a range of issues to be considered by participants, focusing their thinking on internal and external factors that have given rise, or may give rise, to risks.
Process Flow Analysis

- Typically involves the diagrammatic representation of a process, with the goal of better understanding the interrelationships of its component inputs, tasks, outputs and responsibilities. Once mapped, risks can be identified and considered against process objectives.

| Inputs | Tasks | Outputs |

Leading Event Indicators & Escalation Triggers

- Leading risk indicators are qualitative or quantitative measures that provide insight into potential risks. To be useful, they must be available to management on a timely basis, which, depending on the information, might be daily, weekly, monthly, or in real time.
- Escalation triggers typically focus on day-to-day operations and are reported, on an exception basis, when a pre-established threshold is passed.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Measure</th>
<th>Target / Tolerance</th>
<th>Potential Risk</th>
<th>Leading Indicator</th>
<th>Escalation Trigger</th>
</tr>
</thead>
</table>
Loss Event Data Tracking

- Monitoring relevant data can help an organization identify past risks and quantify the associated losses, in order to predict future occurrences. While event data typically are used in risk assessment – based on actual experience with likelihood and impact – they also can be useful in risk identification by providing a basis for fact-based discussion.

Talking to People

- “The best way to understand a risk and the things driving it is to jump down into the trenches and meet with the people who deal with that risk as part of their daily jobs.”

- “Take a survey, schedule some meetings, or just drop by to talk to the people throughout the enterprise, and ask a simple question: “What are the most important risks you believe the company faces?””

- Enterprise Risk Management for Dummies
Risk Assessment

Risk Identification, Assessment and Response

- No matter which method or methods you employ for Risk Identification, you'll most likely find yourself with a long list of risks – so many that it may seem overwhelming...

- Risk assessment techniques help focus attention on those risks that are most significant.
**Risk Assessment**

**Likelihood and Impact**

- Risks are typically assessed from two perspectives – *likelihood* and *impact* – and normally with a combination of qualitative and quantitative methods.

- Likelihood (%) – the probability that a given event will occur...

- Impact ($) – the potential effect on revenue, net operating profit, margin...

**Risk Appetite**

Determining an acceptable level of exposure represents the gist of the matter...

- *Inherent risk* refers to the risk that exists before you address it – the risk in the absence of any actions you might take to alter either the likelihood or impact

- *Residual risk* is also known as your “vulnerability” or “exposure” – the risk that remains after you have attempted to mitigate the inherent risk (see Risk Response)
Qualitative versus Quantitative

- Qualitative assessment techniques are typically employed where risks do not lend themselves to quantification or when sufficient credible data required for quantitative assessments is not practically available.
  - Risk Ranking
  - Questionnaires

- Quantitative assessment techniques bring more precision and are used in more complex and sophisticated activities to supplement qualitative techniques.
  - Value at risk, Cash Flow at Risk, Earnings at Risk
  - Loss Distributions
  - Back-Testing

### Likelihood of Events Affecting Computer Operations

<table>
<thead>
<tr>
<th>Level</th>
<th>Descriptor</th>
<th>Likelihood of Occurrence</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rare</td>
<td>Very low</td>
<td>Technology systems shut down for prolonged periods by terrorist or other intentional action</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>Low</td>
<td>A natural disaster or third party (e.g., utility) event requires invoking the business continuity plan</td>
</tr>
<tr>
<td>3</td>
<td>Possible</td>
<td>Moderate</td>
<td>Hackers penetrate our computer security</td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td>High</td>
<td>Internal staff use company resources to access inappropriate information from the Internet</td>
</tr>
<tr>
<td>5</td>
<td>Almost certain</td>
<td>Very high</td>
<td>Internal staff use company resources for personal messaging</td>
</tr>
</tbody>
</table>
### Impact of Hazardous Materials Release

<table>
<thead>
<tr>
<th>Level</th>
<th>Relative Impact</th>
<th>Measures</th>
</tr>
</thead>
</table>
| 1     | Insignificant     | • No reportable incidents  
         | • Minimal loss of production hours  
         | • No injuries                    |
| 2     | Minor             | • 1-2 reportable incidents  
         | • Materials contained on-site by staff  
         | • Effect less than 5% of day's production hours  
         | • No or minor injuries          |
| 3     | Moderate          | • Several reportable incidents  
         | • Materials contained off-site with outside assistance  
         | • Effect between 5% and 20% of day's production hours  
         | • Out-patient medical treatment required |
| 4     | Major             | • Major reportable event  
         | • Material released into environment, but without real/perceived detrimental effects  
         | • Significant loss of production – between 20% and 100% of day's production  
         | • Limited in-patient care required |
| 5     | Catastrophic      | • Multiple major reportable events or a single catastrophic event  
         | • Release into environment with significant detrimental effect, requiring significant third party resources  
         | • Substantial loss of production capability – more than two days' production hours  
         | • Significant injuries            |

### Risk Exposure Maps

![Risk Exposure Maps Diagram](image-url)
To mitigate a risk is to moderate or alleviate a risk – to lessen it in some way.

It is common in risk management to think of a choice among four basic alternatives for managing a given risk:

1. Avoid.
2. Reduce.
3. Share / Transfer.
4. Retain / Accept.
Risk Responses

- **Avoidance** – Exiting the activities giving rise to risk. Risk avoidance may involve exiting a product line, declining expansion to a new geographical market, or selling a division.

- **Reduction** – Action is taken to reduce risk likelihood or impact, or both. This typically involves a myriad of everyday business decisions.

- **Sharing** – Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common techniques include purchasing insurance products, engaging in hedging transactions, or outsourcing an activity.

- **Acceptance** – No action is taken to affect risk likelihood or impact.

Examples of Risk Responses

<table>
<thead>
<tr>
<th>Avoidance</th>
<th>Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Disposing of a business unit, product line, geographical segment</td>
<td>• Insuring significant unexpected loss</td>
</tr>
<tr>
<td>• Deciding not to engage in new initiatives/activities that would give rise to the risks</td>
<td>• Entering into joint venture/partnership</td>
</tr>
<tr>
<td></td>
<td>• Entering into syndication agreements</td>
</tr>
<tr>
<td></td>
<td>• Hedging risks through capital market instruments</td>
</tr>
<tr>
<td></td>
<td>• Outsourcing business processes</td>
</tr>
<tr>
<td></td>
<td>• Sharing risk through contractual agreements with customers, vendors, or other business partners</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reduction</th>
<th>Acceptance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Diversifying product offerings</td>
<td>• “Self-insuring” against loss</td>
</tr>
<tr>
<td>• Establishing operational limits</td>
<td>• Relying on natural offsets within a portfolio</td>
</tr>
<tr>
<td>• Establishing effective business processes</td>
<td>• Accepting risk as already conforming to risk tolerances</td>
</tr>
<tr>
<td>• Enhancing management involvement in decision making, monitoring</td>
<td></td>
</tr>
</tbody>
</table>
Costs versus Benefits

- Virtually every risk response will incur some direct or indirect cost that is weighed against the benefits it creates. The initial cost to design and implement a response is considered, as is the cost to maintain the response on an ongoing basis.

BCM and ERM Resources

- Enterprise Risk Management for Dummies, Beaumont Vance and Joanna Makomaski
- The Framework for Voluntary Preparedness, Briefing Regarding Private Sector Approaches to Title IX of H.R. 1 And Public Law 110-53 “Implementing Recommendations of the 9/11 Commission Act of 2007”
- Professional Practices for Business Continuity Practitioners, DRI International
- The Failure of Risk Management, Douglas W. Hubbard
- The Resilient Enterprise, Yossi Sheffi
Your Biggest Risk

“How do we know our risk management efforts work?”

“…doing nothing about risk management is not actually the worst case.”

- Douglas W. Hubbard, The Failure of Risk Management