ERM006 – ERM and Business Continuity Management: Together at Last

RIMS Annual Conference
April 13, 2016
Your presenters

Phil Samson
Principal
PricewaterhouseCoopers, Dallas

Luis Cortez
Internal Audit Manager
Falken Tire Corporation, Rancho Cucamonga
Responsible for managing the company’s ERM program and Japanese Sarbanes-Oxley compliance.
Contents

• Background & overview
• ERM and BCM – Aligned missions
• ERM and BCM integration challenges
• ERM lifecycle and BCM lifecycle synergies
• Improving ERM risk assessments with BCM insight
• ERM and BCM insight examples
• Strategies for linking ERM and BCM programs
• Conclusion
Historically, Business Continuity Management (BCM) and Enterprise Risk Management (ERM) programs operated separately.

Many BCM programs can trace their origin to single source.

A crisis event close call increased awareness that BCM capabilities were needed.

A regulatory obligation requires a formal BCM program.

Key customers insisting on BCM evidence.

Cyber risks threaten operational resilience.
ERM and BCM – Aligned missions

In its ERM framework, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) describes ERM as a process that:

1. Is established and implemented by an entity’s board of directors, management, and other personnel;

2. Is applied in a strategy setting and across the enterprise;

3. Is designed to identify potential events that could negatively affect the entity;

4. Manages risks to contain them within the organization’s risk appetite; and

5. Provides reasonable assurance regarding the achievement of entity objectives.

ERM’s mission is to identify, assess, monitor, and report major risks that could impede or otherwise negatively affect the achievement of an organization’s strategic goals and operational objectives.
**ERM and BCM – Aligned missions (continued)**

BCM can be described as a process of identifying and responding to fast-approaching, high-impact interruption risks that can overwhelm inherent operational resiliency.

**BCM’s mission is to enhance enterprise resiliency and help an organization respond and recover from both unanticipated and anticipated business interruptions.**

**BCM also helps the organization identify operational resiliency improvements that can greatly enhance the ability to weather interruptions that would otherwise significantly challenge competitors.**

ERM and BCM share the common goals of identifying, assessing, and managing interruption risks that could serve to prevent achievement of their strategic objectives.
Examples of common misalignments that reduce ERM and BCM program effectiveness include:

1. Separate ERM and BCM steering committees and supervision can lead to BCM programs that don’t address key strategic risks and are too narrowly focused on tactical execution risks.

2. Business continuity efforts only address risks of importance to a subset of the organization leaving other important interruption impact areas unaddressed.

3. The impact of relevant interruption risks on enterprise strategies are not identified punctually because BCM does not share ERM’s senior leadership visibility.

4. Business continuity recovery strategies contain approaches that are misaligned with enterprise strategy.
## ERM and BCM – Misalignment (continued)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Business continuity exercise scenarios do not address critical or emerging interruption risks the ERM program has identified</td>
</tr>
<tr>
<td>6</td>
<td>BCM-identified operational resiliency improvements are not informed by ERM-facilitated management risk tolerance decisions</td>
</tr>
<tr>
<td>7</td>
<td>ERM risk assessments are not informed by BCM-enabled resiliency and recovery capabilities</td>
</tr>
<tr>
<td>8</td>
<td>BCM-identified third-party resiliency risks are neither fully communicated to the ERM program nor integrated with overall third-party risk management</td>
</tr>
</tbody>
</table>
ERM and BCM – Misalignment (continued)

9. ERM risk scenario analysis does not consider the entirety of an interruption event’s impact and scope, which is typically described in the BCM program’s business impact analysis.

10. Separate ERM and BCM program effectiveness reporting to senior management may provide incomplete and disconnected views of the organization’s resiliency and recovery capabilities.

11. Inconsistent use of ERM and BCM risk taxonomies (i.e., impact categories/thresholds, risk appetite/acceptance) reduces the effectiveness of aggregating, normalizing and monitoring risk across the organization.

12. Disconnected ERM and BCM program management cadence increases the latency of risk identification and response.

13. Management’s fatigue from numerous and disconnected risk assessments results in assessment coverage gaps and results misinterpretation.
## ERM lifecycle and BCM lifecycle synergies

<table>
<thead>
<tr>
<th>ERM and BCM program phases</th>
<th>Integration synergy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Program Governance</strong></td>
<td>• ERM and BCM program governance is tightly coupled, sharing many of the same stakeholders</td>
</tr>
<tr>
<td></td>
<td>• The ERM and BCM program owner can be the same individual, yet supported by separate administrative teams</td>
</tr>
<tr>
<td></td>
<td>• The ERM and BCM programs report to the same risk committee and/or board of directors</td>
</tr>
<tr>
<td><strong>Risk Assessment/ Business Impact Analysis (BIA)</strong></td>
<td>• ERM and BCM risk assessment scopes align for areas related to operational interruption risks</td>
</tr>
<tr>
<td></td>
<td>• ERM risk impact categories and their thresholds are used to standardize the way BCM BIA participants describe operational interruption impacts</td>
</tr>
<tr>
<td></td>
<td>• Management’s risk appetite and tolerance decisions are informed by BIA results</td>
</tr>
</tbody>
</table>
**ERM lifecycle and BCM lifecycle synergies**

*(continued)*

<table>
<thead>
<tr>
<th>ERM and BCM program phases</th>
<th>Integration synergy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk treatments/strategies</strong></td>
<td>• Deciding whether and how to respond to interruption risks is based on management’s risk tolerance and risk appetite</td>
</tr>
<tr>
<td></td>
<td>• Resiliency improvements are made to areas that leadership identifies as critical to achieving operational and strategic goals</td>
</tr>
<tr>
<td><strong>Risk plans/business continuity plans</strong></td>
<td>• Approved strategies for responding to interruption risk are documented in actionable business continuity plans</td>
</tr>
<tr>
<td><strong>Program effectiveness monitoring and reporting</strong></td>
<td>• Responses to actual interruption events and the results of business continuity and crisis management exercises are formally evaluated against risk reduction objectives</td>
</tr>
<tr>
<td></td>
<td>• The BCM program’s effectiveness analysis provides a feedback loop to the overall ERM program, thereby providing comfort that resiliency and recoverability efforts reduce interruption risk impact</td>
</tr>
</tbody>
</table>
Improving ERM risk assessments with BCM insight

Leading ERM programs use risk scenario analysis to move beyond traditional enterprise risk assessments.

- Risk scenario analysis leads to a better understanding of the ways multiple factors can combine to both cause vulnerabilities and create opportunities.
- It expands perceptions—before formulating specific business plans—by its focus on factors that sometimes get dismissed or shortchanged.
- It is a forward-looking perspective that focuses on the repercussions of disparate events and their likely chain reactions within the organization.

BCM involvement in risk scenario analysis enhances the robustness of each scenario’s potential impact and provides insight into the organization’s current preparedness to reduce that impact.

Risk scenario analysis results are used to identify resiliency and business continuity improvements that protect operational imperatives and enterprise strategy.
ERM and BCM insight examples

**Cyber risk exposures threaten growth strategies**

ERM program identified that the business strategy of migrating consumers to online centric, omnichannel interactions could be extremely jeopardized by cyber-related threats

- Business continuity and the information security functions examined their business continuity planning, crisis management, and IT disaster handling capabilities
- Results were presented to the ERM risk committee, which evaluated and approved a variety of cyber risk management improvement recommendations

The BCM program was directed to improve its crisis management capabilities and business continuity responses to cyber-related business interruptions

A cyber threat exercise was conducted to validate crisis management and business continuity capabilities
The ERM program identified that the business strategy of gaining market share by offering the lowest-cost products relied extensively on (1) sole-sourced supplier relationships to achieve significant volume discounts and (2) just-in-time supplier shipments to manage inventory costs.

- The related supply chain resiliency risk was not sufficiently analyzed until the BCM program quantified the interruption impact during its annual business impact analysis and risk assessment.
- A subsequent, thorough review was performed to assess the key supplier’s BCM capabilities and the organization’s overall resiliency with regard to supply chain interruptions.

The ERM risk committee and operational leadership approved several initiatives to improve vendor management and sourcing, inventory management, supply chain status monitoring, and operational interruption responses.
## Strategies for linking ERM and BCM programs

<table>
<thead>
<tr>
<th>Integration Idea</th>
<th>Integration Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consider integrating the ERM and BCM programs</td>
<td>• Position BCM within the ERM organization or governance structure as a subgroup. If the combination is not possible, align the BCM program to the ERM program by sharing governance and steering committee members.</td>
</tr>
<tr>
<td>Involve BCM management in the ERM risk assessment process</td>
<td>• Assist in interview preparation • Participate in stakeholder interviews by “listening” for interruption risks, perceived impacts, and weighting in order to improve business continuity planning • Support risk assessment analysis</td>
</tr>
<tr>
<td>Involve ERM management in BCM interruption risk assessment planning and analysis</td>
<td>• Assist in reviewing the interruption risk focus to help narrow scope to the more critical threats and key operating locations • Provide input into the draft BCM risk assessment so it better aligns with ERM’s view of risk and risk tolerance</td>
</tr>
</tbody>
</table>
## Strategies for linking ERM and BCM programs (continued)

<table>
<thead>
<tr>
<th>Integration Idea</th>
<th>Integration Actions</th>
</tr>
</thead>
</table>
| **Perform a BCM business impact analysis (BIA) that is informed by the ERM program’s impact categories, weighting, and thresholds** | • Leverage ERM risk impact information to keep BIA interviews focused on relevant impacts of operational process interruption  
• Apply the BIA’s detailed quantification of interruption risks to improve the ERM program’s determination of risk tolerance and acceptance  |
| **Develop ERM-informed risk resiliency improvement recommendations**               | • Obtain ERM input on suggested resiliency improvements and possible recovery strategies to keep the right focus on cost-versus-risk reduction benefits  |
| **Enhance risk scenario analysis**                                               | • Obtain BCM enterprise interruption impact insight when planning and performing ERM risk scenarios analysis  |
| **Link BCM and ERM program effectiveness reporting**                             | • Use the BCM program’s resiliency and recovery capability assessment reporting to improve the ERM program’s analysis and reporting of overall risk management effectiveness |
## Strategies for linking ERM and BCM programs (continued)

<table>
<thead>
<tr>
<th>Integration Idea</th>
<th>Integration Actions</th>
</tr>
</thead>
</table>
| **Conduct BCM capability examination and post-incident analysis** | • Use the more impactful and more likely ERM-identified interruption risks as the basis for BCM exercise scenarios  
• Perform post-interruption event analysis to determine the effectiveness not only of BCM program response capabilities but also of ERM program risk identification and management |
| **Leverage governance, risk management, and compliance (GRC) technology** | • Use GRC technology to help integrate the ERM and BCM programs, as well as to facilitate closer linkages between other important functions such as policy management, vendor risk management, and compliance |
PwC’s Business Continuity Management Solutions

How to Achieve Excellent ERM Article Series
www.pwc.com/us/ermexcellenceseries
www.pwc.com

PwC Guidance

All of the materials contained in this document, unless specifically attributed to others, have been created by, contain valuable trade secrets of, and belong solely to, PricewaterhouseCoopers LLP (“PwC”). All such materials, including those attributed to others, are owned exclusively by PwC, and may not be used or distributed with the prior written consent of PwC.