BCM’s Role in Effective Risk Management: A Risk Manager’s Point of View

Date: March 24, 2015
Presenter: Randall Davis, MBA, IBD, CPCU, ERM, ARM, ARM-E, ABCP

Agenda for this session

Explore the case for integration of Business Continuity Management (BCM) & Risk Management (RM).

- Competition between RM & BCM functions
- Comparing the RM & BCM Frameworks
- Convergence of RM & BCM
- Practical tips for successful integration
What got me thinking? From BCP 501:

Course Topic 1. Project Initiation and Management
“Establish the need for a Business Continuity Management (BCM) Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organizing and managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative.”

Threats & Crises…BCM or RM issues?
- Terrorism
- Fire
- Explosion
- Disease
- Earthquake
- War
- Labor strike
- Hurricanes
- Environmental pollution
- Lawsuits
- Cyber risk
- Polar Vortex!
The RM & BCM Explosion!

A constant stream of crises over the past 15 years has created a strong drive for Risk and Continuity evolution.

Failures in managing risks effectively have triggered efforts by:
- Regulators
- Stock exchanges
- Rating agencies
- Activist investors
- NGOs
- Governance bodies

They insist that organizational management proactively manage risks and critical disruption on an enterprise-wide basis.

Conflicts between RM & BCM

- Separate and often competitive functions
- Overlapping responsibilities
- Different objectives and methodologies
Origins of RM & BCM

IT departments, with the IT Disaster Recovery Program

Insurance Buying or Hazard Risk Management

Converging

BCM ➔ RM

Both RM & BCM have significantly expanded in scope and methodology

Expanding the scope of RM

Create Lasting and Intentional Stakeholder Value

Protect Operations

Scope Increase

Finance Losses

Financial & Hazard
Operational
Strategic

Risk management has expanded from value protection to value creation
Expanding the scope of BCM

- Business continuity is expanding from IT recovery to enterprise loss control (prevention and reduction)

RM & BCM Best Practices & Standards

**BCM Standards**
- ISO 22301:2012 – Societal security – Business continuity management systems (International)
- BS 25999:2007 – Business Continuity Management (BSI/UK)
- NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs (ANSI/US)

**RM Standards**
- Rating Agencies Frameworks – S&P, Moody’s
- COSO:2004 – Integrated ERM Framework (US)
Some definitions...

- **Risk**: effect of uncertainty on objectives
  - An effect is a deviation from the expected — positive and/or negative.
  - Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
  - Risk is often characterized by reference to potential events and consequences, or a combination of these.
  - Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
  - Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

- **Risk Management**: coordinated activities to direct and control an organization with regard to risk

Source: ISO 31000

---

Some definitions...

- **Business Continuity**: capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident

- **Business Continuity Management**: holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

Source: ISO 22301
K.I.S.S….my simplification

- Risk: deviation from expectation (+ or -)
- Risk Management: you better be deliberate about risk taking
- Business Continuity: resilience to losses (- only)
- Business Continuity Management: you better prepare for losses

RM vs BCM

Risk can have either Negative or Positive impacts...

<table>
<thead>
<tr>
<th>Catastrophic Threats (black swans)</th>
<th>Unexpected Threats</th>
<th>Expected Threats</th>
<th>Expected Opportunities</th>
<th>Unexpected Opportunities</th>
<th>Transformational Opportunities (out-of-the-blue swans)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOSSES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>GAINS</td>
</tr>
</tbody>
</table>
RM vs BCM Area of Focus & Objectives

RM – Ensure Sustainable Stakeholder Value

BCM – Ensure Business Continuity and Resilience

Catastrophic Threats (black swans)

Unexpected Threats

Expected Threats

Expected Opportunities

Unexpected Opportunities (out-of-the-blue swans)

GAINS

LOSSES

RM process – ISO 31000

Context: Corporate Objectives & Risk Appetite

1 – Identify Risks

2 – Evaluate Likelihood x Impact

3 – Treat Risks

4 – Review & Monitor

Low Priority

Throw Away
BCM Process - ISO 22301

Context: Operational Planning and Control

1 – Business Impact Analysis/Risk Assessment
1a – Screen Based On Criticality
2 – Identify & Evaluate BC Strategies
3 – Establish & Implement BC Procedures
4 – Exercise and Test

RM process – Intersect with BCM

Context: Corporate Objectives & Risk Appetite

1 – Identify Risks
2 – Evaluate Likelihood x Impact
3 – Treat Risks
4 – Review & Monitor
BCM Process - Intersect with RM

Context: Operational Planning and Control

1 – Business Impact Analysis/Risk Assessment
1a – Screen Based On Criticality
2 – Identify & Evaluate BC Strategies
3 – Establish & Implement BC Procedures
4 – Exercise and Test

In from RM

Out to RM

In Summary: BCM vs. RM

**BCM**
- Key functions and processes
- Balance sheet and P&L
- Increase preparedness
- Medium to long term
- Impact
- High impact losses
- Ensure Enterprise Resiliency

**RM**
- Organizational objectives and risk appetite
- Stakeholder value
- Risk communication/cost of risk
- Short to long term
- Likelihood and impact
- Medium to high impact events with medium to low frequency
- Ensure Achievement of Objectives
### Negative consequences of the lack of integration of RM & BCM

- Duplicate activities/efforts to manage the same risk issues
- Waste and inefficient operations
- Increased expense, budget constraints
- Unhealthy competition for management attention
- Increased likelihood of missed opportunities/threats

### RM & BCM each add value

**BCM provides RM:**
- A better understanding of critical activities with the BIA
- A stronger focus on exercising and testing
- Technical expertise that is missing in risk control
- Support from the IT organization

**RM provides BCM:**
- A broader view of risk
- A better value proposition aligned with the priorities of management and the board
- Systematic approach of consistently and continuously monitoring and managing risk
- A better view of emerging threats
- An much larger annual budget with ability to allocate costs to operations
Practical Tip of the Session

- Risk Management Departments typically manage a large annual budget that cannot be allocated elsewhere (insurance *has* to be purchased every single year).
- As such, BCM programs can be supported and funded easily as part of the internal RM allocation process.
- Also, RM inherently has C-level support and the ear of the board of directors...capitalize on our relationships!

It’s more than time for a change!

There are at least 3 ways RM & BCM are to be handled:

- **STATUS QUO** – keep separate silos for both (different teams, methods, reporting, etc.)
- **COORDINATION** – use a common management unit that coordinates BCM and RM
- **INTEGRATION** – fully integrate BCM into the RM framework

“What if we don’t change at all ... and something magical just happens?”