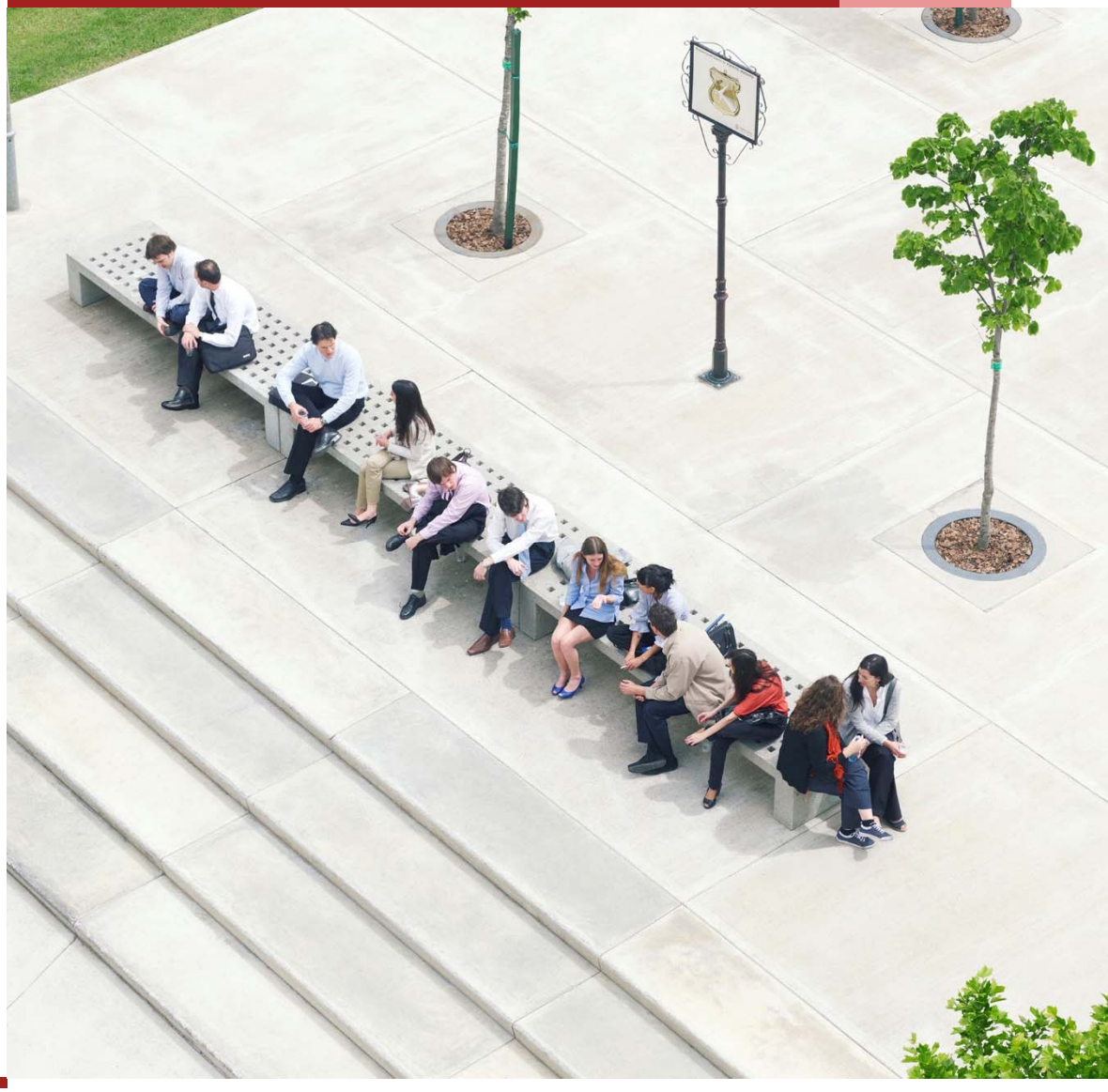
www.pwc.com

Enterprise risk management and business continuity management

Together at last

March 2016

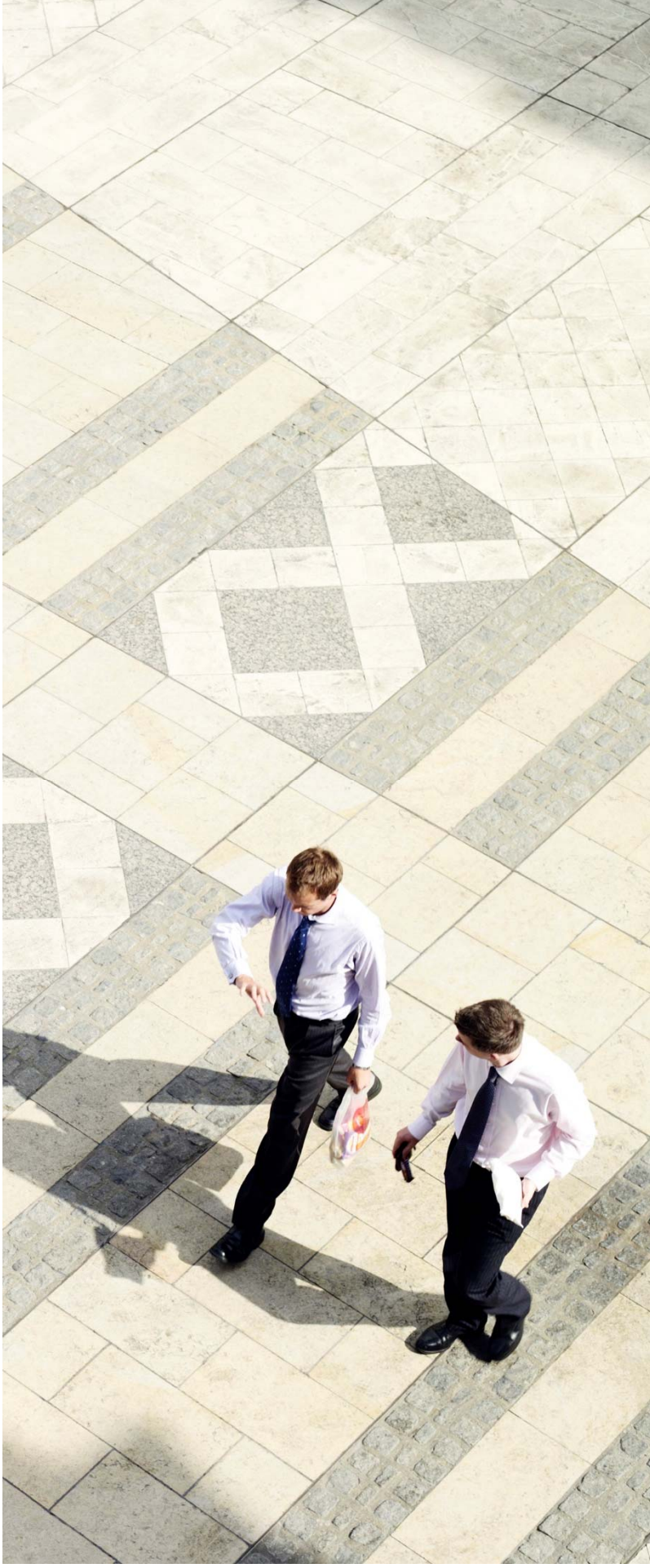


pwc

Overview

The necessity to define, create and maintain an organization's business continuity management (BCM) capabilities often arises from a singular event. It could have been, say, a close call that increased awareness that BCM improvements were needed. Or a new regulatory obligation either directly applied or strongly encouraged by a key customer might have led to efforts to improve and document recoverability capabilities. Or growing numbers of cyber threats have become catalysts for improving both BCM and crisis management capabilities. Regardless of how the BCM program gained its initial traction, its development from a narrow focus has likely resulted in wide gaps in its ability to protect the organization's strategic and operational goals.

We have found that it is far less common for an organization to holistically view its resiliency and recoverability needs from the perspective of managing interruption risk to align with strategic and operational strategies. Organizations that integrate enterprise risk management (ERM) into their strategic planning efforts have found that BCM enhances both their value creation objectives and their protection objectives. The confidence that comes from identifying and appropriately addressing interruption risks enables them to more boldly execute those strategic plans. But to gain that confidence requires the melding of ERM and BCM programs.



ERM and BCM – Aligned missions

In its ERM framework, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) describes ERM as a process (1) that is established and implemented by an entity's board of directors, management, and other personnel; (2) that is applied in a strategy setting and across the enterprise; (3) that is designed to identify potential events that could negatively affect the entity; (4) that manages risks to contain them within the organization's risk appetite; and (5) that 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 achievement of an organization's strategic goals and operational objectives. Simply put, ERM enhances an organization's ability to make risk-informed decisions.

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 has the added value of helping the organization identify operational resiliency improvements that can greatly enhance their 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.

ERM and BCM integration challenges

Symptoms of misaligned ERM and BCM programs are not difficult to identify once you know what to look for. Following are examples of common misalignments that reduce ERM and BCM program effectiveness.

- 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.
- Business continuity efforts only address risks of importance to a subset of the organization (e.g., information technology [IT], supply chain, customer experience, regulatory compliance), leaving other important interruption impact areas unaddressed.
- The impact of relevant interruption risks on enterprise strategies are not identified punctually because BCM does not share ERM's senior leadership visibility.
- Business continuity recovery strategies contain approaches that are misaligned with enterprise strategy (e.g., reliance on decentralized operating locations when centralization strategies are being executed).
- Business continuity exercise scenarios do not address critical or emerging interruption risks the ERM program has identified.
- BCM-identified operational resiliency improvements are not informed by ERM-facilitated management risk tolerance decisions.
- ERM risk assessments are not informed by BCM-enabled resiliency and recovery capabilities.
- BCM-identified third-party resiliency risks are neither fully communicated to the ERM program nor integrated with overall third-party risk management.
- 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.
- Separate ERM and BCM program effectiveness reporting to senior management may provide incomplete and disconnected views of the organization's resiliency and recovery capabilities.
- 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.
- Disconnected ERM and BCM program management cadence increases the latency of risk identification and response.
- Management's fatigue from numerous and disconnected risk assessments results in assessment coverage gaps and results misinterpretation.

ERM lifecycle and BCM lifecycle synergies

The following table describes ERM and BCM program lifecycle integration opportunities:

ERM and BCM program phases	Integration synergy
Program governance	• ERM and BCM program governance is tightly coupled, sharing many of the same stakeholders • The ERM and BCM program owner can be the same individual, yet supported by separate administrative teams • The ERM and BCM programs report to the same risk committee and/or board of directors
Risk assessment/business impact analysis (BIA)	• ERM and BCM risk assessment scopes align for areas related to operational interruption risks • ERM risk impact categories and their thresholds are used to standardize the way BCM BIA participants describe operational interruption impacts • Management's risk appetite and tolerance decisions are informed by BIA results
Risk treatments/strategies	• Deciding whether and how to respond to interruption risks is based on management's risk tolerance and risk appetite • Resiliency improvements are made to areas that leadership identifies as critical to achieving operational and strategic goals
Risk plans/business continuity plans	• Approved strategies for responding to interruption risk are documented in actionable business continuity plans
Program effectiveness monitoring and reporting	• Responses to actual interruption events and the results of business continuity and crisis management exercises are formally evaluated against risk reduction objectives • 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

Improving ERM risk assessments with BCM insight

Leading ERM programs use the technique of risk scenario analysis to move beyond traditional enterprise risk assessments. Risk scenario analysis is a structured process that leads to a better understanding of the ways multiple factors can combine to both cause vulnerabilities and create opportunities. It is often applied as a way of expanding perceptions—before formulating specific business plans—by its focus on factors that sometimes get dismissed or shortchanged. It differs from other strategy tools such as (1) analysis of strengths, weaknesses, opportunities, and threats, and (2) risk assessments because it is a forward-looking perspective that directs its attention to the repercussions of disparate events and their likely chain reactions within the organization. BCM program management's participation in the risk scenario analysis process can help by enhancing the robustness of each scenario's potential impact and providing insight into the organization's current preparedness to reduce that impact. Risk scenario analysis results are then used to identify additional resiliency and business continuity improvements that protect operational imperatives and enterprise strategy.

For more information on Risk Scenario Analysis, see How to achieve excellent Enterprise Risk Management series,

www.pwc.com/us/ermexcellenceseries

Article 4: September 2015

ERM and BCM insight examples

Better risk insight emerges and is optimally addressed when ERM and BCM programs are aligned. Following are two examples in which such alignment resulted in organizations significantly improving their resiliency and response capabilities for dealing with key risks.

1. *An organization's ERM program identified that the business strategy of migrating consumers to online centric, omnichannel interactions could be extremely jeopardized by cyber-related threats (e.g., a data breach, reliance on third-parties, an operations interruption, online fraud). The ERM risk committee requested a closer inspection of the organization's capabilities for carrying out data and systems protection, customer activity monitoring, vendor risk management, IT resiliency and recovery, and operational resilience. Business continuity program management and the organization's information security function looked through a cyber threat lens to examine their business continuity planning, crisis management, and IT disaster handling capabilities. They presented the results of the examination 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, as well as its business continuity responses to cyber--related business interruptions. A cyber threat exercise was conducted to validate crisis management and business continuity capabilities, the results of which were presented to the ERM committee.*

2. *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 seen as a key risk and reported as a risk factor in the company's most recent Form 10-K submission. However, that 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. Vendor interruption resiliency and recovery improvement opportunities were presented to the ERM risk committee and operational leadership, which resulted in the approval of several initiatives for improving vendor management and sourcing, inventory management, supply chain status monitoring, and operational interruption responses.*

Strategies for linking ERM and BCM programs

Executing a series of well-coordinated ERM and BCM integration activities makes it possible to realize the full value of optimized business continuity management. Example leading-practice integration examples include:

- Consider ERM and BCM program integration
  - 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.
- Involve BCM management in the ERM risk assessment process
  - 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.
- Involve ERM management in BCM interruption risk assessment planning and analysis
  - 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.
- 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.
- 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.
- 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.
- 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.

Contact us

For further information on this topic, please contact:

Phil Samson
Business Continuity Management Solution Leader
phil.samson@pwc.com

Julia Holden
Risk Management & Compliance Solutions Director
julia.c.holden@pwc.com

Brett Williams
Risk Management & Compliance Solutions Director
brett.m.williams@pwc.com

Stephen V. Zawoyski
Enterprise Risk Management Solution Leader
stephen.v.zawoyski@pwc.com

Neil Kaufman
Risk Management & Compliance Solutions Director
neil.kaufman@pwc.com

Geoffrey Carnes
Risk Management & Compliance Solutions Director
geoffrey.h.carnes@pwc.com