Key Issues, Challenges and Resolutions in Implementing Business Continuity Projects

Business continuity management (BCM) is a holistic process to ensure uninterrupted availability of all key business resources required to support critical business activities, whether manual or IT-enabled, in the event of business disruption. Business continuity planning (BCP) involves planning and procedural aspects, encompassing emergency response, crisis communications, business continuity and disaster recovery. Disaster recovery planning (DRP) is the technical component of BCP and focuses on the continuity of information and communication technology systems that support business functions.1

BS 25999 Business continuity management establishes the process, principles and terminology of BCM and highlights the benefits and outcomes of an effective BCM program.2 BCM goes beyond BCP and also covers management aspects such as policy, training and awareness, maintenance and exercise, and continuous improvement, as well as understanding the organization and embedding BCM into its culture. An effective BCM program protects the interests of the organization’s stakeholders and reputation. The main BCM assets are the six organizational resources—people, premises, technology, information, supplies and stakeholders—for which continuity strategies may be required.

Successful execution of BCM projects results in robust BCM processes and organizational resilience. Adoption of an inappropriate approach and/or incorrect assumptions by BCM practitioners in the execution of a BCM project renders the outcome of the project—BCM documentation—unfit for use and results in a waste of scarce resources. This article describes key issues and challenges faced and observed by the author and his team during the execution of BCM projects, and suggests resolutions.

KEY ISSUES, CHALLENGES AND RESOLUTIONS

The key issues and challenges in implementing BCM projects revolve around four major areas:

1. Senior management commitment and involvement
2. Lack of thorough understanding of the data dynamics and dependencies involved in data recovery by BCM practitioners
3. Inappropriate approach in executing BCM processes
4. Incorrect and/or inappropriate assumptions in formulating business continuity and disaster recovery plans

COMMITMENT AND INVOLVEMENT

This section presents the key issues, challenges and resolutions related to senior management commitment and involvement in implementing a BCM project.

Delegation by Senior Management

In some organizations, the executive sponsor of the BCM project is too busy to oversee the project, and the responsibility is delegated to a mid-level manager. This reduces the visibility of the project at the organizational level and may also result in lack of serious cooperation from relevant departments/functions.

This challenge is resolved by setting up a cross-functional project steering committee that consists of key stakeholders. The committee should meet periodically (e.g., every one to two weeks) to resolve issues, if any, in project execution.

BCM Implementation for the Wrong Reasons

In some organizations, senior management tends to think that since a disaster has never been experienced, there is no business case for expending scarce resources. This often results in a lackadaisical attempt at implementing business continuity to satisfy only regulatory requirements or close audit observations.
This is addressed by undertaking a sustained BCM awareness campaign among key stakeholders, highlighting the benefits of achieving resilience from their perspective: meeting current and prospective customer demands and regulatory compliance, avoiding liability, and maintaining a competitive edge.

**Business/IT Disconnect**
Organizations in highly competitive industries are often compelled to respond dynamically to a competitor’s offerings. Under pressure to reduce the time to market for newly conceived products and services, business managers sometimes do not give advance notice to the infrastructure team to address capacity issues.

This failure to align technological capability with business needs and growth projections often results in solution gaps, false expectations and performance issues that adversely affect organizational reputation. These issues can be avoided by systematic planning and collaboration between business and IT.

**Technology-only Approach Toward Resilience**
When planning for organizational resilience, some organizations focus more on technology and do not give equal importance to other organizational resources such as people, premises, data, processes and supplies.

This is addressed by creating appropriate awareness among stakeholders, identifying risks and single points of failure for organizational resources, recommending suitable risk mitigation measures to ensure the continuous availability of resources, and incorporating BCM processes into day-to-day operations.

**Lack of Consensus Between Senior Management and Operations Management**
Lack of consensus between senior management and operations management is prominent when conducting business impact analysis (BIA). BS 25999-1:2006 *Business continuity management—Code of practice* expects senior management to be actively involved in BIA.

In some organizations, senior management may prefer to understand the ground realities before committing any values for the maximum tolerable period of disruption (MTPOD) and recovery time objectives (RTOs) because it is aware of the financial implications of such decisions. In such cases, breaking the BIA into two parts makes sense. The first part of the BIA should be conducted with senior management to obtain MTPOD values for all services/products and respective functions that support the delivery of the services/products. The second part of the BIA has to be conducted with operational management in a more detailed way at the department level to identify department-specific MTPOD values and RTOs.

The department-specific MTPOD values given by senior management should be treated as preliminary values and need to be validated by the operational management of respective departments. Any difference in the MTPOD values of senior management and operational management need to be resolved by achieving consensus of opinion.

**Absence of a Single BCM Framework Across Multiple Offices**
The BCM framework followed across all offices may not be consistent for organizations that have multiple locations in multiple countries. Consistency in approach and BCM documentation can be achieved by adopting an international BCM standard/framework across the enterprise.

**LACK OF UNDERSTANDING**
This section presents the key issues, challenges and resolutions related to a lack of thorough understanding of the data dynamics and dependencies involved in data recovery by BCM practitioners.

**Incomplete Understanding of Data Recovery Requirements**
Many organizations check only whether their core data are backed up and recoverable, and few consider the data dynamics and dependencies involved in data recovery.
These include:

- Are there any end-user computing systems outside enterprise backup? Some organizations depend on end-user computing resources such as department-developed scripts, spreadsheets and local databases to support ad hoc business requests that may be part of business-critical operations. These end-user computing resources need to be incorporated into the backup cycle to ensure that data backup is available for retrieval when required. Alternatively, the functionality provided by the end-user computing systems should be incorporated into the enterprise applications.

- Is there a need for synchronized recovery of lost data, backed-up data and data from any continuing business transactions during an outage?

- At what rate do unprocessed backlogs accumulate for continuing business transactions during an outage?

- How much of a backlog can be accumulated before local disk storage capacity is exceeded?

- Is there a means to pull data from remote transaction sources (e.g., automatic teller machines or points of sale) out of the normal processing windows and on a metered basis?

- What are the assumptions about the sudden spurt in data volumes that will hit the systems post recovery? Are there any capacity or processing time/speed issues that will impair the speed of data recovery or require metering to avoid overwhelming any applications that cannot cope with the volume? If so, are these factors considered in the estimation of total time to full recovery?

**Failure to Consider Full Recovery**

Most business continuity and disaster recovery plans address failover to a hot site or alternate site. Very few address the need to move operations back to a restored primary location, which can be as problematic as the failover itself.

**INAPPROPRIATE APPROACH**

This section presents the key issues, challenges and resolutions related to an inappropriate approach in executing BCM processes.

**Location-based Risk Assessments**

Tailoring a risk assessment to suit an organizational context is a challenge faced in some BCM projects. Conducting a buildingwide risk assessment may not always be sustainable.

For example, some organizations may not have a single owner for a building (such as a data center) in which each team takes care of its own systems or common units/agencies may be provided by facilities management (e.g., physical security, cleaning, cooling, heating).

In such cases, adopting a service/product-based approach for risk assessment is more effective and sustainable. This approach is also in line with the BS 25999 requirement of evaluating threats to critical activities and activities that support the delivery of products/services within an organization. In this approach, each team conducts a risk assessment for its resources, including technology, data, people, processes, premises and supplies. A corporate team such as a BCM organization can coordinate the risk assessments; consolidate and analyze the results; and facilitate selection, approval and deployment of risk mitigation measures at the enterprise level.

**Equal Weight Assigned to All Risk Attributes**

Another challenge relating to risk assessment is the risk assessment approach itself. There are different methodologies to carry out a risk assessment. When the Failure Modes and Effects Analysis (FMEA) methodology is used for risk assessment, a risk priority number (RPN) is computed. RPN is the product of three attributes of risk—severity, likelihood and nondetectability—that are given equal weight. If the RPN is used alone to denote risk acceptance criteria, it may result in unnecessary investments for low-severity risks. To avoid this, another parameter, criticality—the product of severity and likelihood—is suggested.

**Figure 1** illustrates three risk scenarios with the same RPN.

<table>
<thead>
<tr>
<th>Risk No.</th>
<th>Severity</th>
<th>Likelihood</th>
<th>Nondetectability</th>
<th>RPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>1</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>25</td>
</tr>
</tbody>
</table>

The third risk in **Figure 1** is more critical than the other two risks. When risks are prioritized for treatment, this risk should be given higher priority than the other risks that have equal RPN values. Therefore, the effective way to establish risk acceptance criteria is to use both RPN and criticality.
Inappropriate BIA Approach

BIA tools lead BCM practitioners to conduct analysis in silos by functional area, out of context of the impact of a disaster on the entire location. This kind of approach will ultimately skew all BIA findings to a higher availability and cost of strategies and solutions, and will lead to a significant and consistent failure of BIA efforts because the management of individual business functions will tend to overstate the importance of its function. However, if questioned correctly, management will give an entirely different answer about its relative importance in the context of a broader disaster impact. BIA has to be approached in the context of a sitewide disaster that affects all business functions at the site.

Challenge in the Deployment of a BCM Tool

Some organizations deploy a BCM tool to manage the BCM life cycle. Depending on the BCM tool and the version deployed, this may not be a challenge for enterprises. It is possible that the approach adopted by the BCM team when conducting certain activities (such as BIA and risk assessment) may not map exactly with the approach built into the tool. For example, during BIA, a business impact owing to an outage is determined for different durations. The durations used by the BCM team may be different from those used in the tool.

Knowledge of the tool and its workflows at the time of developing BCM documentation will help in avoiding rework during implementation of the BCM tool.

INCORRECT AND/OR INAPPROPRIATE ASSUMPTIONS

This section presents the key issues, challenges and resolutions related to incorrect and/or inappropriate assumptions in formulating business continuity and disaster recovery plans.

Failure to Consider All Relevant Assumptions and Limiting Factors

Many business continuity plans are built on assumptions that may not include all relevant assumptions and limiting factors. For example, many plans are predicated on an unstated assumption that only the organization in question will be impacted by a disaster. In reality, many disasters can be local or regional in nature and impact a number of organizations, businesses, infrastructures and transportation types. The competition for scarce resources, as well as travel limitations, can greatly impair recovery efforts.

Another typical assumption is that employees will go long distances to support operations at an alternate site. Local area or regional disasters, especially those that may result in injury and death, can make employees reluctant to go far from home.

Plans need to address an organization’s expectations and the permissions or requirements it will communicate to its employees. A hard-line, help-the-enterprise approach will not be well received, but one that tells employees to first take care of themselves and their families during a disaster may garner more employee support. Business continuity planners should recognize and document relevant assumptions and factors that may limit recovery from a business disruption event and bring such assumptions and limiting factors to the attention of management.4

CONCLUSION

BCM is a business-owned and business-driven process and is a good corporate governance practice. However, there is no one-size-fits-all approach to implement BCM. BCM practitioners need to adapt relevant standards and best practices to suit their organizational cultures and requirements, which leads to certain challenges in implementing BCM projects. Resolving the relevant issues and challenges appropriately based on organizational context helps in establishing a sustainable BCM program and in enhancing an organization’s BCM maturity.

ACKNOWLEDGEMENT

The author wishes to thank Brian V. Cummings for his review of and feedback on the article.

ENDNOTES


2 For a detailed description of the process, principles and terminology of BCM and the benefits and outcomes of an effective BCM program, please see British Standards Institution, BS 25999-1:2006 Business continuity management—Code of Practice, UK, 2006.
