Table of Contents

Executive Summary................................................................. 1
Introduction ................................................................................ 2
Internal Audit Roles and Engagements ................................. 4
Internal Audit's Evaluation of Key BCM Elements .......... 5
Internal Audit Activities Before a Crisis .............................. 7
Internal Audit Activities During and After a Crisis .......... 7
Appendix .................................................................................. 9
Authors & Reviewer ............................................................... 23
Executive Summary

Business continuity management (BCM) prepares organizations for future incidents or crises that could interfere with the achievement of business objectives. Crisis management (CM) is a key component of BCM and deals with communicating pertinent information about the crisis to the organization’s stakeholders.

Internal audit’s breadth and depth of skills and qualifications, position in the organization, and in-depth knowledge of organization-wide operations position it well to make meaningful contributions to the development, implementation, and assessment of an organization’s BCM and CM initiatives. Internal audit may perform a variety of key and supporting roles, depending on the existence and/or maturity of BCM and CM initiatives, as well as the severity and circumstances of the crisis.

Internal audit’s roles may involve assurance and advisory services before, during, and after a crisis. Assurance and advisory services both require expert knowledge of key BCM elements including program governance, risk management, business impact analysis, and business continuity and recovery planning (BCRP).

- Assurance engagements may be performed to verify that BCM and CM are effective.
- Advisory services may be performed to help management focus planning activities and coordinate BCM and CM with risks and controls.

During a crisis, internal auditors also may be expected and authorized to perform critical non-auditing roles to serve the needs of the organization.
Introduction

The IIA Global Technology Audit Guide (GTAG) 10: Business Continuity Management speaks to the importance of BCM, serves as a valuable reference for the key components of an effective BCM program, and provides direction for the continuity of critical IT infrastructure and business applications systems during and after a crisis. This practice guide expands on Business Continuity Management by exploring auditors’ potential roles in crisis management and providing guidance on:

- Internal audit activities before, during, and after a crisis.
- Internal audit’s evaluation of key BCM elements.

Practice aids provided in the appendix include a risk assessment checklist, sample audit programs, a glossary, and references.

Business Significance and Related Risks

All organizations will eventually face business interruptions. A well-defined BCM/CM plan is like an insurance policy for the organization — it helps to ensure that the organization will continue to be viable and meet stakeholder expectations. The BCM/CM plans also can provide internal audit with a venue to continually update and communicate effective risk management and control throughout the organization.

Crisis management plans (CMP) consolidate preventive and reactive risk management measures for acute crises situations. Deficient, poorly constructed or communicated CMPs with inadequate testing or training may elevate organizational risks from a crisis to unacceptable levels. CMPs developed post-crisis rely primarily on the recent crisis to drive content development and may not be comprehensive enough to be effective. For public sector organizations, including governments, exposures due to a crisis or incident may have broader local and international implications.

A well-communicated and comprehensive CMP may help organizations effectively navigate through a crisis and related risks. Moreover, a CMP may improve an organization’s resilience in the face of crisis. CM tools and programs, when built thoughtfully, validated periodically, and advocated and approved by management and/or the board, will enable organizations to manage events and mitigate risks to minimize overall operational, financial, reputational, regulatory, and legal exposure for key internal and external stakeholders.

Related IIA Standards and Guidance

The International Standards for the Professional Practice of Internal Auditing (Standards) related to BCM and CM include:

Standard 2100: Nature of Work

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

Standard 2110: Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.
Standard 2120: Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Standard 2400: Communicating Results

1. Internal auditors must communicate the results of engagements.

Definitions of Key Concepts

BCM is the process by which an organization prepares for future incidents or crises that could jeopardize the organization’s core mission and its short- and long-term ability to continue operations and meet stakeholder expectations. CM, considered a key component of BCM, addresses how the organization will inform the general public, its staff, its business partners, and various stakeholders of a disaster or crisis and the steps being taken to resume business operations and minimize internal/external stakeholder impact. A CMP is a consolidated portfolio of activities consisting of preventive and reactive measures executable by any organization to effectively mitigate and manage risks created by a crisis or event.

Business Continuity Management

BCM is a risk management approach based on business value. It aligns business continuity capabilities with risks. The goal of BCM is to enable any organization to restore critical operational activities, manage communications, and minimize financial and other effects of a disaster, business disruption, or other major event. BCM is a simple matter of risk management designed to create business continuity capabilities to match likely risks based on business value. While terminology in professional literature may vary, the term BCM in this practice guide addresses the overall policy/model/framework for managing various types of service interruptions that can be triggered by events internal or external to the organization. This definition also may apply to public sector organizations such as governments. For these organizations, the term business represents governing agencies, critical public operations, public safety, and the security of its constituents.

Key components of BCM include:

- Management Support – Management shows support to appropriately prepare, maintain, and exercise a business continuity plan (BCP) by assigning adequate resources, people, and budgeted funds.
- Risk Assessment and Risk Mitigation – Potential risks due to threats such as fire or flood, are identified, and the probability and potential impact to the organization are determined. This is done at the site and division level to ensure that the risks of all credible events are understood and managed appropriately.
- Business Impact Analysis (BIA) – Identifies business processes that are integral to keeping the business unit functioning in a disaster and to determine how soon these integral processes should be recovered following a disaster.
- Business Recovery and Continuity Strategy – Addresses the actual steps, people, and resources required to recover critical business processes. This also should identify key communication mechanisms and protocols. The strategy may consider company or industry benchmarks and standards.
- Plan Awareness and Training – Education and awareness of the BCP are critical to the execution of BCM. Training also may include performance of exercises and/or practice drills for portions of the BCP.
- Maintenance – The BCM capabilities and documentation are maintained to ensure that they remain effective and aligned with business priorities.

Crisis Management

CM is a key component of BCM that is triggered when the disruption of business service rises to the level of a crisis or disaster. CM documents methods used to respond
to the reality and perception of crises. CM also involves establishing metrics to define what scenarios constitute a crisis and should consequently trigger the necessary response mechanisms. It consists of the communication that occurs within the response phase of emergency management scenarios.

**Types of Interruptions**

BCM seeks to manage internally and externally generated threats. Each threat can have varying degrees of impact on the organization’s business processes, which could adversely affect regulatory compliance, personnel safety, protection of the environment, the ability to maintain operating standards and satisfy contractual requirements, and the organization’s brand/reputation. Types of interruptions include:

- Cyberattack.
- Disease/pandemic.
- Earthquake/tsunami.
- Fire.
- Flood.
- Hurricane/tornado.
- Labor disruption.
- Production failure/outage.
- Product contamination.
- Sabotage.
- Service or product outage for key business partners/vendors.
- System failure.
- Terrorism.
- Utility outage.

**Internal Audit Roles and Engagements**

**Internal Audit’s Role Defined**

Internal auditors are positioned to contribute to crisis management by providing organizations with practical insights into operations. The chief audit executive (CAE) should define internal audit’s roles before, during, and after a crisis, taking care not to assume responsibility for the ownership or management of crisis-related risks. Often, the internal audit function may have a seat at the table during the crisis management planning process. As an initial action, the CAE, along with key internal audit management, should become familiar with leading BCM practices through external references and standards. Resources are provided in Practice Aid III of this guide. Once roles are developed, they should be documented and communicated within the function and to key external stakeholders who will be directly impacted.

If internal audit or the CAE do not have a role in the crisis management process, the audit committee should be notified to avoid gaps in expectations. When internal audit serves in an advisory role to management in the context of BCP/CMP development, the potential impact on internal audit’s independence and objectivity should be explicitly addressed. As roles are identified, they should be approved by the CAE’s administrative and functional reporting lines and potentially documented in the internal audit charter.

**Advisory or Assurance Engagements Regarding BCM**

The internal auditor’s responsibility to add value and improve an organization’s operations and risk management efforts should extend to BCM assurance or advisory engagements, depending on the maturity of the organization’s BCM program. The inclusion of the internal audit activity in BCM and CM planning or refinement process may be key to the program’s success. This is especially the case for organizations with a low level of maturity in this
space. Given its interaction with, and understanding of, the needs of the organization’s board and executive management, internal audit can provide perspective and help focus planning activities. Ensuring that key BCM focus areas are aligned with board and executive management level needs is critical to success.

Assurance Engagements

Internal audit may perform periodic assurance engagements to verify that the BCP and CMP are comprehensive, relevant to the current business operating environment, and communicated to the appropriate internal and external stakeholders. The frequency, nature, and extent of work performed will be driven by risks or requests from stakeholders to validate the effectiveness and relevance of planned efforts.

The scope of assurance engagements may include a comprehensive BCM program or specific elements (e.g., testing the occurrence and update frequency of the BCP, and the maturity of the CMP). Internal audit’s knowledge of the risks mitigated by the BCP or CMP and prior involvement in an advisory capacity during plan development may promote a more efficient engagement planning process.

Assurance engagements may include:

- Requests for review by the audit committee or executive management on the BCM program or portions thereof, including vendor or business partner reviews.
- BCM reviews to evaluate plan completeness, maturity, and appropriateness based on organizational risks, growth, or divestitures.
- Program risk assessments.
- Reviews of existing provisions of an organization’s or a business partner’s BCP/CMP as defined by contractual terms (i.e., right to audit clauses or defined service-level agreements).

See Practice Aid I for additional guidance on assurance engagement programs.

Advisory Engagements

The focus of BCM can quickly turn toward the review and analysis of IT infrastructure because data access and transfer are considered core business functions. However, when providing BCM/CM advisory services, internal audit should consider broad organizational objectives and risks and not limit the engagement’s emphasis to IT issues. BCM advisory engagements should not compromise internal audit’s objectivity. Care should be taken not to accept responsibility for ownership or management of business continuity risks.

Internal Audit’s Evaluation of Key BCM Elements

BCM programs include common elements such as program governance, risk management, business impact analysis (BIA), and business continuity and recovery planning (BCRP). It is critical that each element involve the right sponsors, stakeholders, and business partners to help ensure the development of a comprehensive, supported, and actionable plan. Overall communication elements within, and information about, the plans should be shared with key stakeholders. Internal audit activity may include evaluating the effectiveness of BCM and the CMP.

Program Governance

The key to successful BCM is the support and sponsorship of executive management. Internal audit can help identify and forge relationships between key internal BCM stakeholders. The following activities may be performed by internal audit during the initial stages of BCM evaluation:

- Determining whether key leadership positions have been documented and approved to help ensure ownership and accountability for the organization’s
programs. Leadership is critical to identifying plan interdependencies, promoting continuous improvement, and learning from post-crisis activities.

- Recommending the development of a BCM charter. The charter helps to establish program sponsorship and support within the highest levels of the organization. In addition to validating the BCM program’s existence, a well-defined charter establishes a BCM governance structure (i.e., BCM committee) and guidance regarding periodic re-evaluation of the charter. A governance structure approves BCM or CM decisions and provides a forum for visibility into organizationwide BCP or CMP development, revisions, and associated internal and external communications.

- Evaluating whether an established BCM and CM governance structure is adequately funded, appropriate, and effective in serving the needs of the board, audit committee, or executive management. Internal audit may play a nonvoting member role or attend meetings to provide feedback on the role, charter, and efforts of such a body.

- Communicating and advising on whether BCM governance appropriately and effectively serves the needs of the board, audit committee, and executive management.

- Apprising the board (audit committee) of the risks associated with, and current best practices for, business continuity and CMPs.

Risk Management

For BCM to be effective, it must consider the relevant prioritized risks facing an organization in the event of a crisis. Internal audit often has a detailed understanding of core business risks. Risks may be magnified and reprioritized during a crisis based on the nature and extent of events facing an organization. Internal audit may share information about key organizational risks during the establishment and evaluation of BCM.

Understanding key BCM risks can help strengthen the development of the proposed internal audit plan. Being exposed to the organization’s BCM activities helps the internal auditor identify key exposure areas including organizational tone/support, operational control activities, and core processes and potential systems/data/vendor dependencies. Weakness or failures in these areas could prompt the internal audit function to focus resources on providing assurance or advisory engagements geared toward adding value and organizational improvement. Gathering risk data helps guide internal audit’s plan and allows internal audit to perform analyses to assess risk probabilities, impacts, comprehensiveness, and credibility. Practice Aid I provides a sample risk assessment checklist.

Business Impact Analysis (BIA)

Internal audit may provide guidance on how management can perform a BIA, a key component of BCM. A BIA will support the identification of key business assets, functions, applications, partners, vendors, resources, and the eventual evaluation of potential loss to an organization in the event of a crisis. GTAG 10: Business Continuity Management provides useful direction on performing a BIA. The results of the BIA will likely drive the levels of pre-emptive actions, coverage, and risk appetite to be assumed by the organization. A BIA, if performed effectively, will outline critical operations, critical resources, and processes — facility, personnel, and technology (including logical and physical security) — and may ultimately drive investment priorities for a BCP and related CMP.

Business Continuity and Recovery Planning (BCRP)

BCRP provides a proactive method by which organizations can identify business continuity and recovery measures to manage and mitigate key organizational risks triggered by a crisis. Internal audit may provide advisory or assurance services related to BCRP.
Internal Audit Activities Before a Crisis

Internal audit’s evaluation of BCM, and specifically CMP, may help ensure that the CMP remains relevant to organizational priorities in the event of a crisis.

Included below are typical activities in which internal audit may be engaged before a crisis:

• Share knowledge of leading developments for BCM with executive management and the audit committee.
• Specifically consider BCM as a risk facing the organization and consider residual risks in the development of the annual audit plan.
• Evaluate key business partner arrangements for appropriate contractual terms, including service-level agreements, right-to-audit clauses, and requisite reporting to management regarding the partner’s control environment.
• Advise management in its performance of BCM risk assessments or evaluate the accuracy of management’s BCM risk self-assessments.
• Perform assurance engagements related to the BCP and/or CMP, as part of the annual audit plan. Assurance engagements may include evaluation of plan components, communication protocols within the plan, and the operational aspects of the plan.
• If not established by the provisions of the internal audit charter or directives from the board, clarify and establish BCM roles for internal audit and the CAE.

Internal Audit Activities During and After a Crisis

The headings below describe common activities that internal audit may perform during and after a crisis.

During the Crisis:

• Monitor and assess the organization’s response to an event and be an active participant on the crisis management team.
• Monitor outage details for subsequent audits.
• Serve on a crisis management committee to ensure that risks associated with a crisis are understood and provide recommendations on alternate courses of action to management, as appropriate.
• Participate in the wider crisis management and recovery process for the organization, as agreed upon and authorized.

The Standards allow for these types of involvement provided that the details of any potential impairment to internal audit independence are disclosed to appropriate parties (e.g., audit committee and BCM leadership). Involvement by internal audit may be greater during the initial stages of a crisis when support of the organization’s limited available resources is in high demand.

After the Crisis:

• Evaluate and report on the effectiveness of the organization’s recovery efforts.
• Continue to assess risk, provide guidance, and help develop business improvement efforts.
• Perform post-crisis reviews to identify opportunities for BCM activities and, specifically, for CMP evolution.
• Perform assurance engagements to evaluate whether management performed and appropriately considered the results of root-cause analysis to update the BCP and CMP, as needed. Participate in the organizationwide recovery process, as agreed upon and authorized per the BCP and CMP.

These activities are discussed in greater detail in the following pages.
Conduct Audits of the Recovery Processes and Plan Effectiveness

The disaster recovery plan, as a component of the BCM, may include requirements for internal audit to conduct an audit of the recovery process. Where this is the case, this additional work will need to be included in the initial draft plan and may lead to changes to those priorities.

Additionally, where such a role has not been specifically assigned, the CAE should consider whether, following a risk-based assessment, he or she should recommend to the BCP leadership team that particular aspects of data recovery and/or CMP should be audited.

The types of audit work that might be undertaken include:

- An end-to-end review of the recovery process (i.e., whether it complied with the planned process and whether the plan proved to be detailed enough to deal with the issues that emerged).
- An audit of the effectiveness of the recovery process, including performance against defined metrics or plan components as well as effective and timely internal and external stakeholder/business partner communication.
- A review of controls and special processes introduced outside the normal control framework and potential impact on operational or financial risks for the organization.
- An audit of management’s data recovery processes, which may include examining key data reconciliations performed by management to ensure data completeness and accuracy.
- A review of actual BCP and CMP variations following activation of the plans, including recommendations that will allow for effective plan evolution. This also should apply to the internal audit activity’s own plans.

Participate in the Broader Recovery Process

Internal auditors may be requested by organizational leadership to lend additional support to operational staff who are either:

- Working on recovery processes.
- Working on revisions to normal business processes as a result of the unavailability of IT systems.
- Using alternate defined procedures to carry out activities for which normal processes have been disrupted.

It will be important for the CAE to consider requests authorized by the audit committee in advance of determining internal audit’s BCP/CMP role. Additionally, when internal audit staff is released to assist with CM or recovery efforts, assigned duties should be carried out under the direction of operational management. To protect objectivity, the CAE should consider the operational duties performed by internal auditors and avoid assigning them to future internal audit assurance activities in the same area.
Appendix

Practice Aid I: Sample Work Programs for BCM Assurance or Advisory Engagements

The internal audit activity plays an important role in providing an independent review of the adequacy of the overall BCM. The depth and frequency of audit activities and reporting should be scaled to the criticality of the operation. While the scope of the audit activities and deliverables may vary, in all cases they must encompass an independent and objective evaluation of the effectiveness of the testing program. The internal audit activity should determine the reasonableness of the underlying assumptions that were made in developing the testing program. The reasonableness of underlying assumptions, as well as the adequacy of the test plan, scenarios, schedules, and reports, should be evaluated relative to the size and complexity of the organization, the criticality of the business line, and the risk and impact of possible business disruption. Internal audit also should observe test exercises to assess the control environment of alternative locations, verify the results, assess that appropriate reporting and escalation mechanisms are established and used, and evaluate whether test plans are updated to reflect prior test results. An audit considers five common aspects of the BCM:

1. **Business environment and strategy.**
2. **BCP methodology and strategy.**
3. **Business impact analysis (risk evaluation and controls).**
4. **Recovery plan.**
5. **Awareness, testing, and training.**

Example 1:

<table>
<thead>
<tr>
<th>BCM SAMPLE WORK PROGRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SUB AREA</strong></td>
</tr>
<tr>
<td>1. Business environment and strategy</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### BCM SAMPLE WORK PROGRAM

<table>
<thead>
<tr>
<th>SUB AREA</th>
<th>ITEMS</th>
<th>POSSIBLE CONSIDERATIONS</th>
</tr>
</thead>
</table>
| **2. BCP methodology linkage to business, operational, and financial strategy** | Business strategy | 1. BCP is based on the company’s business strategy.  
2. All relevant entities and critical functions are considered within this BCP. |
| | Operational/technical strategy | 1. Both operational and IT are integrated.  
2. BCM planning is considered in every relevant business decision.  
3. BCP/CMP responsibilities, including maintenance, are incorporated in applicable employee job descriptions and personnel evaluations.  
4. BCP is updated, reviewed, and tested at a frequency appropriate for risks, vulnerabilities, and value of business functions. |
| | Financial strategy | 1. Adequate financial resources are made available for the preparation and maintenance of a BCP. |
| **3. Impact Analysis (includes business impact analysis [BIA], risk evaluation, and controls)** | Tone at the top | 1. Board of directors and senior management is supporting the BCM initiative.  
2. Senior executive is responsible for ensuring successful implementation, maintenance, and update of plans supporting BCM.  
3. BCM policy/charter exists and is updated periodically.  
4. BCM-related plans, including BCP and CMP, are approved by board of directors and each appropriate level of management. |
# BCM SAMPLE WORK PROGRAM

<table>
<thead>
<tr>
<th>SUB AREA</th>
<th>ITEMS</th>
<th>POSSIBLE CONSIDERATIONS</th>
</tr>
</thead>
</table>
| **Risk Assessment** | | 1. A comprehensive impact analysis/BIA exists and is prepared with the line of business input.  
2. Various types of events that could prompt the formal declaration of a crisis or disaster and the process for invoking the BCP and CMP are clearly described.  
3. Work flow analysis was performed and results are documented, if deemed necessary by the organizational leadership.  
4. Prioritization of business functions is adequate.  
5. Risk assessment includes impact and probability of disruptions of all business, operational, and IT areas, and considers acceptable downtime.  
6. Procedures exist to execute the plan’s priorities for critical versus noncritical functions, services, and processes.  
7. Financial impact in case of emergency reflects accurately the cost in case of emergency.  
8. Reputation risks are considered and all relevant stakeholders are considered in the BIA. |
| **Mitigation** | | 1. Adequate risk mitigation, including preparedness and prevention strategies, have been considered, such as:  
   a) Alternative locations and capacity (ensure geographic diversity).  
   b) Back-up of data, applications, telecommunications, and other relevant data is ensured and procedures exist.  
   c) Communication channels in case of emergency are clearly defined (communication tree).  
2. All critical personnel are identified and the contact list is updated.  
3. Employees understand their role in case of emergency.  
4. Redundant vendor support is established. |
| **4. Recovery plan** | **Recovery point objective (RPO)** | 1. RPOs are clearly defined and communicated.  
2. RPOs consider the organization’s recovery needs. |
| | **Recovery time objective (RTO)** | 1. RTOs are clearly defined and communicated.  
2. Recovery time adequately reflects how much downtime the organization is willing to tolerate.  
3. BIA results are considered in defining RPO and RTO. |
## BCM SAMPLE WORK PROGRAM

<table>
<thead>
<tr>
<th>SUB AREA</th>
<th>ITEMS</th>
<th>POSSIBLE CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Awareness, testing, and training</td>
<td>Testing policy</td>
<td>1. Within the BCP, the organization has set testing requirements for the organizationwide continuity functions, business lines, support functions, and CM.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Key roles and responsibilities are defined in the testing policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Testing cycles with increasing levels of test scope and complexity are defined.</td>
</tr>
<tr>
<td></td>
<td>Testing strategy</td>
<td>1. Testing strategy includes documented test plans and related testing scenarios, methods, and schedules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expectations for testing internal and external independencies are defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Testing strategy is in line with management’s assumptions and expectations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. BCP is validated through annual or more frequent testing cycles.</td>
</tr>
<tr>
<td></td>
<td>Testing observations</td>
<td>1. Tests are done without prior notice to employees. Internal audit activity may observe management’s execution of test exercises with focus on the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a) All relevant employees were available and received timely communication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b) Back-up facilities and resources satisfied the needs of the business units.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>c) Relevant back-up procedures worked as intended.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>d) Key business partners were included in the testing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e) Business processes were re-established in the expected time frame.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Internal audit documents audit findings.</td>
</tr>
<tr>
<td></td>
<td>Post-testing</td>
<td>1. Gap analysis is performed by BCM leadership team.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Internal audit independently documents and communicates audit findings, if any.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. BCM findings or areas for improvement are addressed and corrected; BCM leadership team discusses corrective actions and communicates findings to appropriate stakeholders. Such data may support the need for BCM evolution or plan updates.</td>
</tr>
</tbody>
</table>
### BCM Sample Work Program

<table>
<thead>
<tr>
<th>Sub Area</th>
<th>Items</th>
<th>Possible Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>4. Conclusions regarding the testing program and whether it is appropriate for the size, complexity, and risk profile of the organization are documented pursuant to plan content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Board of directors and/or executive management is informed of testing results.</td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td>1. All staff is trained and aware of their responsibilities.</td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td>2. Training details, such as content, participants, and timing are documented.</td>
</tr>
</tbody>
</table>
Example 2:
Selected portions of the assessment below are completed to provide examples of potential content.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>STATUS</th>
<th>ASSESSMENT NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PURPOSE, SCOPE, AND OBJECTIVES</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Define program | Is the BCM program documented to define?  
• BCM purpose, scope, and objectives.  
• BCM procedures.  
• BCM resources, roles, and responsibilities.  
• BCM measurement and verification.  
• BCM continual improvement. | Yes | Yes — overall program scope established and documented. |
| | Does the BCM scope cover the entire operation, including all business processes and operations, as well as related facilities and workforce that are the responsibility of the company? | No | All facilities not addressed. |
| **PROCEDURES** | | |
| Risk assessment  
Designed to identify threat scenarios (credible events) that could disrupt business. To successfully complete this BCM risk assessment, those who are knowledgeable of threats to the organization, environment, and region should participate. Participation may include those from security staff, facilities staff, etc. | Has a BCM risk assessment been conducted for the organization?  
NI (Needs improvement) | Greater formalization and documentation needed. |
| | Did the risk assessment consider these categories of risks:  
• Natural hazards.  
• Militant/people.  
• Human factors/IT.  
• Operational. | NI | Consider regional events. |
<table>
<thead>
<tr>
<th>ITEM</th>
<th>Status</th>
<th>Assessment Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A site-based BCM risk assessment should be completed and shared with applicable facility/location tenants.</td>
<td>Were risk mitigation strategies identified?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Were risks mitigated?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Did you align your BCM risk assessment (e.g., disaster scenarios) with other organizations at your site?</td>
<td></td>
</tr>
<tr>
<td>Business impact analysis (BIA)</td>
<td>Has a BIA been conducted for the organization (including all business teams)?</td>
<td></td>
</tr>
<tr>
<td>Identifies critical business processes that need to be recovered following a disaster event. After completing the BIA, identify recovery solutions needed to resume the critical business processes.</td>
<td>Were critical business processes identified?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Has your leadership team approved the list of critical business processes identified during the BIA and the associated proposed recovery solutions?</td>
<td></td>
</tr>
<tr>
<td>Recovery solutions</td>
<td>Have the recovery solutions and resource requirements been identified for each critical process?</td>
<td></td>
</tr>
<tr>
<td>Recovery solutions are developed and a list of the resources needed to support the CM (recovery) efforts of the organization and/or team are created.</td>
<td>Have all teams documented the resources required to recover critical business processes?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Have the IT requirements been assessed?</td>
<td></td>
</tr>
<tr>
<td>Written plans</td>
<td>Has a written BCP been prepared that includes all business teams, critical business processes, and organizational CMP?</td>
<td></td>
</tr>
</tbody>
</table>
### BCM Risk or Self-Assessment

<table>
<thead>
<tr>
<th>ITEM</th>
<th>STATUS</th>
<th>ASSESSMENT NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service-level agreements (SLAs), memorandum of understanding (MOU), and contracts</td>
<td>Have SLAs and/or an MOU been established for:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Office space (with facilities management)?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IT/communications (with IT provider)?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data restoration (with IT provider)?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Other third-party contracts?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Has action been taken to protect company interests when third-party contracts include a “force majeure” clause?</td>
<td></td>
</tr>
<tr>
<td>Alignment</td>
<td>Do you participate in multitenant, multisite coordinated planning?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Has your organization established an emergency communications plan, including accounting for all staff?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Have you aligned the BCP with CM and emergency response?</td>
<td></td>
</tr>
</tbody>
</table>
### BCM RISK OR SELF-ASSESSMENT

<table>
<thead>
<tr>
<th>ITEM</th>
<th>STATUS</th>
<th>ASSESSMENT NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training and exercise</td>
<td>Have the BCM executive and BCM manager received training?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Has the BC coordinator been trained?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Have all members of the BCM team received training pertaining to their roles and responsibilities?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are key BCM activities exercised on an annual basis or more frequently?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Notification drill.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Table top exercise.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Functional exercise.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full scale exercise.</td>
<td></td>
</tr>
</tbody>
</table>

### RESOURCES, ROLES, AND RESPONSIBILITIES

<table>
<thead>
<tr>
<th>Staff supporting BCM</th>
<th>Have you verified that alternative staff who will perform critical work have the capabilities (knowledge, access, etc.) to perform these functions?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM executive</td>
<td>Has the organization’s leadership team identified a BCM executive?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Does the BCM executive have access to the leadership team?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are funding, personnel, and resources adequate?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Has BCM been coordinated with other organizational processes and linked to the organization’s business plan?</td>
<td></td>
</tr>
</tbody>
</table>
## BCM Risk or Self-Assessment

<table>
<thead>
<tr>
<th>ITEM</th>
<th>STATUS</th>
<th>ASSESSMENT NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BCM manager</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has an organizationwide BCM manager been identified?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the BCM manager coordinate and lead the implementation of BCM?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the BCM manager ensure cross-functional resources are available and appropriately engaged when needed?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the BCM manager ensure the effectiveness and efficiency of CM is measured, verified, and periodically reviewed for improvement opportunities?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BCM coordinator</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has an organizationwide BCM coordinator been identified?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the BCM coordinator manage business continuity planning at the organization, business unit (BU), regional BU, or other sub-level?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the BCM coordinator participate in multitenant, multisite coordination activities, as appropriate?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Measurement and Verification

<table>
<thead>
<tr>
<th>ITEM</th>
<th>STATUS</th>
<th>ASSESSMENT NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are measurement and verification processes in place to verify annually that requirements of BCM have been addressed in a way that is aligned with current business needs?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**BCM RISK OR SELF-ASSESSMENT**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>STATUS</th>
<th>ASSESSMENT NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTINUAL IMPROVEMENT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have the IT requirements been validated, including IT requirements needed to support relocation planning, network or remote access, local or central data, etc.?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are measurement and verification processes linked with continual improvement processes?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you track actions required to resolve BCM gaps identified during the BCM exercise to ensure timely completion?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a process in place to reassess the effectiveness of your BCM program?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Practice Aid II: Glossary of Key Terms

Business Continuity Plan (BCP) – the ability to plan for the continuity of critical business processes; protect critical assets; and provide service and support to customers in the face of a crisis, disaster, incident, or emergency. Such a plan allows an organization to recover effectively from, and manage risks associated with, a crisis. This is often included in a crisis management program.

Business Continuity and Recovery Planning (BCRP) – a proactive method by which organizations can identify business continuity and recovery measures to manage and mitigate key organizational risks triggered by a crisis.

Crisis – an event that, if not handled appropriately, may significantly impact an organization’s ability to operate, remain profitable, and manage reputational risk. Commonly, these are natural or physical disasters, failures of critical operations and/or connectivity, disruptions to key business partner relationships, and technology exposures.

Crisis Management Program (CMP) – a consolidated portfolio of activities consisting of preventive and reactive measures executable by an organization to effectively mitigate and manage risks implied by a crisis or event. A CMP often will include a business continuity plan and a disaster recovery plan.

Disaster – a sudden, unplanned catastrophic event causing unacceptable damage or loss. This may include events that compromise an organization's ability to provide critical functions, processes, or services. This is an example of an event in which business continuity and/or disaster recovery plans often are activated as part of an overall CMP.

Emergency – an unplanned, impending incident or situation that may cause injury; loss of life; destruction of property; or interference, loss, or disruption of normal business operations. Such events may escalate into a crisis if not controlled or managed.

Incident – an event that is not part of operational standards, which may temporarily impact a business and in some cases could lead to an emergency or disaster.

Impact Analysis – a process to analyze key operational functions or critical data with a view to understand potential internal or external impact of potential loss/disruption. Impact analysis includes Business Impact Analysis (BIA), which involves the identification of critical business assets, functions, and resources, as well as an evaluation of the potential damage or loss that may be caused to the organization resulting from a disruption or a change in the business or operating environment. A BIA should identify: a) sources of damage, interruption, or loss; b) the extent to which time passage will magnify the potential damage, interruption, or loss; c) the level of services or resources required to sustain core business activities; and d) the time line during which all critical business assets, functions, and resources should be restored to avoid permanent significant loss for the organization.

Recovery Point Objective (RPO) – the point in time to which systems and data must be recovered after an outage (e.g., end of previous day’s processing). RPOs often are used as the basis for developing backup strategies and to determine the amount of data that may need to be recreated after the systems or functions have been recovered.

Recovery Time Objective (RTO) – the period of time within which systems, applications, or functions must be recovered after an outage (usually one business day). RTOs often are used as the basis for developing recovery strategies and to determine whether to implement those strategies during a disaster situation. Maximum allowable downtime is a commonly associated term.

Risk Assessment/Analysis – the process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organizational exposure, and evaluating the cost for such
controls. Risk analysis often involves an evaluation of the probabilities and likelihood of a particular event. A crisis is an example of an event.

**Practice Aid III: BCM Standards and Guidance Resources**

Numerous resources provide standards and guidance related to BCM. Resources include frameworks and maturity models to benchmark the internal auditor’s role in supporting the business continuity plan (BCP) and crisis management plan (CMP) development life cycles. Many resources may serve to educate internal audit staff and provide an opportunity for knowledge sharing with organization management that are seeking to build, adjust, or validate BCM efforts. Resources as of April 2013 include:

- The Institute of Internal Auditors’ *International Standards for the Professional Practice of Internal Auditing (Standards)* and related guidance (www.theiia.org), including:
  - Global Technology Audit Guide 10: Business Continuity Management. This guidance includes: 1) common disaster scenarios, 2) management roles during business interruption, 3) disaster recovery solutions, 4) risk assessment and mitigation, 5) business recovery and continuity strategy, and 6) CM plan testing.
  - 2010 GAIN Survey and Results–Crisis Management.
  - Audit Executive Center’s 2011 Knowledge Alert–Three Crisis Management Imperatives for CAEs.
- Disaster Recovery Institute (www.drii.org), *Professional Practices for Business Continuity Planners* (2008). A widely used framework that includes information on: 1) program initiation and management, 2) risk evaluation and control, 3) business impact analysis, 4) business continuity strategies, 5) emergency response and operations, 6) business continuity plans, 7) awareness and training programs, 8) audit and maintenance, 9) communications, and 10) coordination with external agencies.
- The Business Continuity Institute’s (www.thebci.org) *Good Practice Guidelines* (2010). The guidelines include six elements: 1) policy and program management, 2) embedding CM in the organization’s culture, 3) understanding the organization, 4) determining CM strategy, 5) developing and implementing a CM response, and 6) exercising, maintaining, and reviewing.
- International Organization for Standardization (ISO) (www.iso.org) guidelines:
  - ISO/IEC 24762, *Guidelines for Information and*
Communications Technology Disaster Recovery Services (2008). “Provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services as part of BCM, applicable to both “in-house” and “outsourced” ICT DR service providers of physical facilities and services.”


- ISO 22301, Societal Security–Business Continuity Management Systems–Requirements, which superseded BS 25999. Specifies generic BCM system requirements applicable to all organizations or parts thereof.

- British Standards Institute (www.bsigroup.com).

- PAS 200 (2011) advises organizations regarding the types of activities and resources they need to develop and maintain to allow for effective crisis detection, preparedness, and response. This specification is sponsored by the U.K. Cabinet Office, and the crisis management specification has been developed through consultation with several leading U.K. businesses and public organizations. This specification addresses the requirements for CM, in addition to the guidance provided by BS 25999: Business Continuity Management and ISO 27001.

- BS 25777: Information and Communications Technology Continuity Management–Code of Practice (2008). “Provides recommendations for information and communication technology continuity management within the framework of business continuity management provided by BS 25999-1.”

Several organizations mentioned above also provide BCP education and certifications. Other organizations that offer such training and certifications include:

Authors:

David Bentley, CIA
Brian Foster, CIA
Brian Peterson
Brian Reed, CIA
Erich Schumann, CIA, CRMA
Rita Thakkar, CIA
Benito Ybarra, CIA

Reviewer:

Steven E. Jameson, CIA, CCSA, CFSA, CRMA
About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession’s global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA’s IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes. For other authoritative guidance materials provided by The IIA, please visit our website at https://globaliia.org/standards-guidance.

Disclaimer

The IIA publishes this document for informational and educational purposes. This guidance material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

Copyright

Copyright © 2014 The Institute of Internal Auditors. For permission to reproduce, please contact The IIA at guidance@theiia.org.