Security Executive Council

RISK MANAGEMENT PORTFOLIO

Business Continuity

Playbook

Dean Correia, Contributing Editor

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Sharing is Caring: Business Continuity Playbook

At the onset of the COVID-19 pandemic, the robustness of a company's business continuity plan often decided whether it would thrive, survive, or sink. As we move forward from this crisis, executive management are uniquely motivated to continue to press for new or enhanced assurances of business continuity.

This Playbook is meant to serve as a framework to help security leaders build a business continuity program from the ground up or enhance the program that is currently in existence. The materials have been compiled using various accredited sources, international standards, and the collective knowledge of the Security Executive Council and its subject matter experts, which represents decades of experience managing business continuity programs.

The Playbook is adaptable to companies of all sizes from all industries, and its appendices include templates, job descriptions, structural diagrams, sample meeting agendas, decision matrices, and more.

Ways to use this resource:

- To guide the development of a new business continuity program
- To identify gaps and determine where your existing program may be enhanced
- To formalize or document a currently informal program
- To educate management on the direction in which you plan to take your BCP
- To assist in the hiring process for new BC roles

Send feedback about this resource to: contact@secleader.com

THE SEC PROCESS

We walk clients through eight critical steps to reach their goals

01 NEW REALITY ASSESSMENT

The first step is an assessment of your current environment. What needs improving? What are Security's fixed conditions? What recent changes have impacted Security, such as new business directions, new stakeholders, or a merger or acquisition?

02 DEFINE RISKS & DESIRED OUTCOME

An SEC team made up of former CSOs will engage with you to identify the key risks and determine the continuum of desired outcomes depending on your conditions. We map the solution to your C4R – current circumstances, conditions, culture and resources.

03 SEC RESEARCH & KNOWLEDGE BASE ANALYSIS

Once we understand the issues and potential barriers, we search our extensive security knowledge base for resources or research data that can be used as a base or to kickstart direction ideas.

04 COLLECTIVE KNOWLEDGE™ REVIEW

Next, our subject matter experts bring their varied experiences and knowledge together to create a plan to help you reach your desired outcome. We call this Collective Knowledge™.

05 EXAMINE & ALIGN FOR UNIFIED RISK

We help determine which other functions the plan should touch and align with. We use the SEC's Unified Risk Oversight™ model to help plan and communicate the value of cross-functional collaboration.

06 SPONSORSHIP ACCEPTANCE & EXECUTIVE VALIDATION

We assist in communicating the value of the project to the business leader accountable for Security's new vision. This in turn assists in communicating the strategy to senior executives from other functions.

07 DEFINE BUSINESS VALUE MEASURES

Business value metrics are developed for the client team to measure and determine project success for the organization, including key stakeholders.

08 IMPLEMENTATION ASSISTANCE

Last, clients can either take the SEC deliverables and run with them, or we can guide you through the implementation of your plan. At the end of the day, **the SEC is here to help you succeed.**

The SEC Process Outcome: Security Leader and Program Success

Business Continuity
Playbook

Edited by
Dean Correia

Vision and concept by
Bob Hayes

Collective knowledge strategy and execution by
Kathleen Kotwica

ELSEVIER
AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Security Executive Council

Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK
225 Wyman Street, Waltham, MA 02451, USA

Originally published by the Security Executive Council, 2007

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

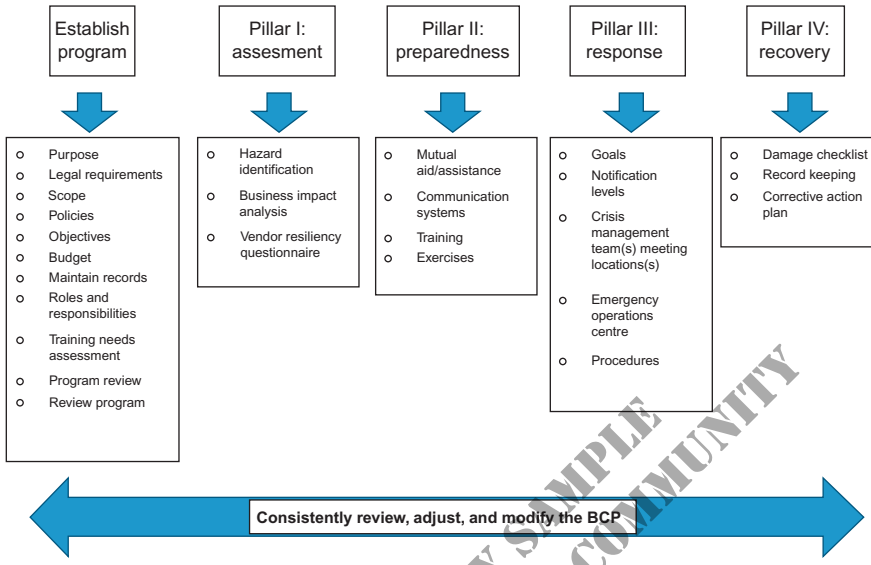
British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-411648-1

CONTENTS

How Do I Implement the Four Pillars of a Business Continuity Program?



The four pillars of a successful business continuity program (BCP).

The figure above highlights the four interdependent risk-based functions of a BCP: **assessment** of business needs and risks, and **preparedness** for, **response** to, and **recovery** from emergencies. These functions can be undertaken sequentially or concurrently, and they are not independent of each other. This diagram can be used as a quick checklist for security leaders to compare what's currently in place in their organization and components of the plan that are missing. It will also benefit the security leader by its flexibility for customization specific to the current company personnel structure by illustrating who in the company should be involved, which components security exclusively runs, and when security should partner with other internal/external stakeholders.

PILLAR I: ASSESSMENT

Business disruptions can take many forms. Before a BCP can be developed to address these disruptions, one must understand what the risks to the organization are and how these risks might affect the business. This is the goal of the first core element of the BCP, known as the risk assessment.

Risk assessments should be conducted by a team of individuals who represent various business functions and support groups. As business plans change, risks and their possible effects on the business may change. Therefore, risk assessments need to be reviewed on a regular basis to ensure they remain relevant and effective. The assessment process should include hazard identification and risk evaluation. This information becomes the needs or requirements that the remainder of the BCP must address.

Hazard Identification

Hazards are typically grouped into three categories: natural (fire, flood, pandemic), human-caused (hazardous material spill or release, terrorism, fraud), and technological (software/hardware malfunction). Risk information should be gathered from all local, regional, and national industry, association, and governmental sources. During this process, keep in mind that threats and vulnerabilities can be internal or external to the business. For example, disruption to the business can be indirectly caused by crises suffered by suppliers, customers, the local community, or government.

Risk Evaluation

Not all risks are equal. Risks that are extremely improbable or that have little impact on the organization may need to be treated differently than high-cost events. Therefore, after identifying the hazards to the organization the next step is to determine the likelihood and possible impact of the events.

In order to effectively analyze and communicate the results of the assessments, they usually result in the construction of a threat matrix and heat map which show the relationship of risks to their probability and amount of damage to the organization. (*Note: Examples of a threat matrix and heat map can be found in Appendix 4.*)

Risk assessments should be conducted by a team of individuals who represent various company functions and support groups. The ASIS Business Continuity Guideline[6] recommends that when companies are performing a risk assessment, the company should keep the following four objectives in mind:

1. Identify internal and external threats and vulnerabilities
2. Identify the likelihood of an event arising from such threats or vulnerabilities
3. Define the critical functions necessary to continue an organization's operations
4. Define the controls in place or necessary to reduce exposure and evaluate the cost for such controls

Business Impact Analysis

To complete the risk assessment process, the probable impact of a threat or vulnerability on the organization must be determined. The process of determining and recording the extent and potential costs of business disruption is called a business impact analysis (BIA). The BIA will be used to develop recovery strategies and therefore needs to include enough information to support this task. (*Note: An example of a BIA template can be found in Appendix 5.)* According to the ASIS Business Continuity Guideline, the four major functions of the BIA are:

1. To identify critical processes
2. To assess impact if crisis were to happen
3. To determine maximum allowable outage and recovery time objectives
4. To identify the resources required for resumption and recovery

The identification and documentation of critical business processes should consider not only all business functions but also how they interrelate to each other. Allowable outage and recovery times should take into consideration seasonality. For example, longer outage recovery times may be acceptable during a time of the year where slower sales are expected. The resources required for recovery may include people, technology, data records, and third parties such as vendors or public sector personnel. When possible, the BIA should quantify the operational impacts in terms such as lost sales, increased expenses, regulatory fines, penalties, or other financial terms.

Vendor Resiliency Questionnaire

Most companies rely on outsourced vendors to support their operations in one or more areas. As these outsourced vendors are key members of a company's BCP, it is as important to assess their crisis readiness as it is the company's. This will provide the organization's leaders with a comfort level that the vendor is performing its diligence within the four pillars of the BCP to an acceptable minimum standard.

The company should establish a standard minimum score that the vendor must achieve in order to be deemed in compliance with the company's crisis readiness guidelines. If the vendor receives a failing score, it should be required to take remedial action within a designated timeframe in order to achieve the acceptable passing score and continue as an approved company vendor.

PILLAR II: PREPAREDNESS

The "Emergency Management Planning Guide 2010–2011,"[7] issued by Public Safety Canada, is an excellent resource for a discussion of preparedness and the purpose of preparatory training exercises. The guide states that "the objective of planning activities associated with preparedness is to have an effective and coordinated approach to BCP and operational readiness." The goals of planning activities related to preparedness, according to the guide, should include:

- Maintain a level of sustainable capacity, supplies, and resources to meet the goals outlined in departmental BCP plans that are based on priorities, needs analysis, and capability requirements
- Incorporate lessons learned and best practices into the BCP process for continuous improvement

As with other continuous improvement methodologies, the BCP will benefit from a continuous cycle of planning, implementation, testing, and improvement. Each iteration of the cycle provides learning opportunities that can be used to identify gaps or issues with the BCP. The opportunity for ongoing training this cycle provides ensures that all BCP team members, management, and employees are aware of and capable of carrying out their responsibilities in the BCP process.

Mutual Aid/Mutual Assistance

A mutual aid/mutual assistance agreement is any formal agreement between entities to share or provide resources, facilities, services, and other required support to one another during an incident. Examples include cooperative assistance agreements, service level agreements, and intergovernmental compacts. Such agreements may include neighboring or nearby private sector entities, as well as relevant government, private sector, and nongovernmental organizations. Mutual aid/mutual assistance agreements should be:

- developed in consultation with the parties involved,
- in writing,
- reviewed by legal counsel, and
- signed by responsible individuals.

At a minimum, a mutual aid/mutual assistance agreement should include the following elements or provisions:

- Definitions of key terms used in the agreement
- Roles and responsibilities of individual parties
- Procedures for requesting and providing assistance
- Procedures, authorities, and rules for payment, reimbursement, and allocation of costs
- Notification procedures
- Protocols for interoperable communications
- Relationships with other agreements among entities
- Employment standards/occupational health and safety/workers' compensation coverage
- Treatment of liability and immunity
- Recognition of qualifications and certifications

Communication Systems

Telecommunication and other communication systems should support all components of the program in order to notify and update key internal and external stakeholders regarding the incident. These systems can include the following:

- Traditional phone, wireless, and satellite telephones
- Pagers
- Fax machines
- Computer systems and networks, including personal digital assistants (PDAs), company intranet, external web sites

- Automated, purchased, or hosted systems and services that can simultaneously send and/or verify receipt of messages to telephone and computer devices
- Two-way radios operating on public, private, or amateur radio frequencies
- Public radio and television systems, including provision for interrupting broadcasts with emergency messages or superimposing messages on current programming
- Sirens and other outside warning devices
- Computerized incident management systems for sharing operational communications

Training

Individuals who perform tasks related to any aspect of the company's BCP are expected to be competent as a result of appropriate education, training, and experience. Training or instruction should be conducted at all levels of the organization, including C-level, and be specific to emergency management and business continuity duties and responsibilities as determined by a training needs assessment.

Training may be conducted through workshops, webinars, conference calls, internal or external courses, and industry-specific seminars. In the "Emergency Management Planning Guide 2010–2011," Public Safety Canada recommends that the training plan should address the following questions:

- What are the objectives of the training and what will it consist of?
- Who will be trained?
- Who will do the training?
- What training activities will be used?
- When and where will each session take place?
- How will the session(s) be evaluated and documented?

Exercises

An exercise provides the chance to simulate a real-world crisis. It promotes preparedness while offering the best opportunity to test the BCP and identify weaknesses. A simulation is a valuable way to improve the coordination and communication between various teams as well as judge the effectiveness of the training. It is crucial to involve all

key stakeholders with involvement in the organization's crisis response plan.

Exercises can be designed to test certain portions of a plan or the entire plan(s). Some common exercise formats include:

- **Tabletop exercise:** A facilitator, who is not a member of the company's current crisis management, provides the group of attendees with details of a mock crisis scenario. Participants review and discuss the actions they would take in response to the scenario details presented by the facilitator. Specific response actions are not performed.
- **Functional exercise:** A facilitator, who is not a member of the company's current crisis management, provides the group of attendees with details of a mock crisis scenario. Participants perform some or all of the actions they would take in the event of plan activation to respond to the scenario. Specific response actions are taken.
- **Full operational exercise:** A facilitator, who is not a member of the company's current crisis management, provides the group of attendees with details of a mock crisis scenario. Participants suspend normal operation and activate the plans as if the event were real.

It is important to consider any applicable legislative requirements when determining exercise frequency and format. Exercises should be conducted when there have been significant changes to the business' key personnel responsible for implementing the plan or a new risk to the organization with a high probability of impact has emerged.

In order for an organization to realize a high degree of benefit from an exercise, the following best practices should be considered:

- The scenario should be as real as possible and be based on the risk assessment. This means that key stakeholders and resources, inside and outside the company, should be involved.
- Debriefing sessions should be included at the end of the exercise, with lessons learned documented.

PILLAR III: RESPONSE

A critical incident is a sudden, unplanned event that affects or potentially affects the company's ability to execute critical business functions and results in great damage or loss. A critical incident is characterized by:

- an interruption of normal business operations;
- the need for an immediate, coordinated response by numerous resources;
- and the potential to draw extensive news media and public attention on the organization.

The goals of critical incident response are to:

- protect human life,
- protect company assets and the surrounding community,
- contain the incident,
- communicate to all stakeholders and media,
- assess the effects of the critical incident, and
- decide on and implement optimal response plans.

Key principles in the management of all incidents include:

- initial assessment of the incident's impact,
- communication to involve stakeholders as deemed by initial assessment,
- continuous assessment, response, and communication updates to all internal and external stakeholders.

Important Crisis Management Skills

- Be calm—Crisis management requires clear thinking, emotional control, and balance.
- Be open-minded—Take in large quantities of information without tunnel vision and focus on listening.
- Be decisive—Decisiveness needs to be balanced with a willingness to consider ideas and input from others. Be willing to prioritize and make decisions with only partial knowledge.
- Be flexible—Adapt to rapidly changing situations. Remember that some information relayed about critical incidents is incorrect or incomplete.
- Be persuasive—Crisis management requires the ability to convince others to follow directions.

Response Teams and Expectations

Three interrelated teams may manage incident response at different levels within the organization.

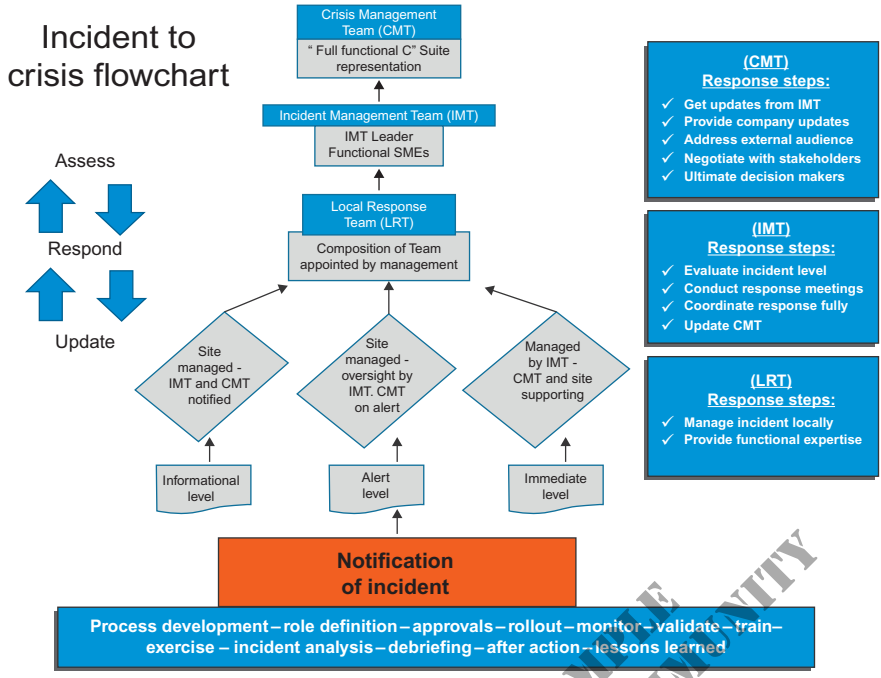
1. **Crisis Management Team (CMT)**—The CMT manages the uppermost level of incident response, providing senior executive guidance and making decisions regarding policy, procedure, and finances as they relate to the management of critical incidents. The CMT may be led by the functional leader of a company's security department and should include executive-level representation. Other relevant external stakeholders may be brought in to support the CMT as required.
2. **Incident Management Team (IMT)**—The IMT actively manages critical incidents that extensively threaten employees, assets, and brand reputation from the corporate office. This group consists of subject-matter experts (SMEs) from each critical business function and may be led by a leader within the company's security department. Other relevant external stakeholders may be brought in to support the IMT as required.
3. **Local Response Team (LRT)**—The LRT responds to local critical incidents that extensively threaten employees, assets, and brand reputation. This group consists of local SMEs from each critical business function and may be led by the local leader of a company's security department. Other relevant external stakeholders may be brought in to support the LRT as required.

Members of the CMT, IMT, and LRT must:

- Attend training, exercises, and meetings as required (or send backups when necessary).
- Be knowledgeable in the four pillars of the company's BCP and review it at least quarterly.
- Keep the BCP with them at all times.
- Ensure that their designated backups are aware of their roles.
- Provide functional expertise as required during crisis management meetings.

(Note: A template to capture the names, functions, and contact numbers for CMT, IMT, and LRT primary and backup members can be found in Appendix 6. CMT, IMT, and LRT members and lead roles and responsibilities can be found in Appendix 7.)

Incident Notification and Escalation



Incident to crisis flowchart, including the roles of each response team.

The diagram above illustrates the typical framework of incident management along with the interdependencies of all stakeholders. Regardless of the level of the incident, the IMT lead notifies the CMT lead of an emerging critical incident. Based on the incident's severity, the CMT lead determines when it is appropriate to communicate to respective CMT members at one of the three levels, which each include steps that should be followed.

Information Level

1. The CMT lead is contacted by the IMT lead regarding the incident. The CMT lead then contacts the remaining CMT members regarding the critical incident on a convenient basis, usually during working hours. The incident does not require a call to action.
2. The IMT meets in order to manage the incident. The IMT lead is responsible for tracking the incident status and updating the CMT

lead as necessary, who in turn updates the other CMT members accordingly.
3. If the incident is at a local level impacting people, assets, or brand, the LRT lead is responsible for alerting the IMT lead.

Alert Level

1. The CMT lead is contacted by the IMT lead regarding the incident. The CMT lead contacts the remaining CMT members regarding the critical incident regardless of the time of day.
2. The CMT lead contacts the other CMT members to establish representation and availability in the event that the situation escalates and a meeting is required.
3. Additional key internal and external stakeholders are identified and placed on call if the situation escalates.
4. The IMT meets in order to manage the incident from the corporate office level. The IMT lead is responsible for tracking the incident status and updating the CMT lead as necessary, who in turn updates the other CMT members accordingly.
5. If the incident is at a local level impacting people, assets, or brand, the LRT lead is responsible for alerting the IMT lead. The LRT meets.

Immediate Level

1. The CMT lead is contacted by the IMT lead regarding the incident. The CMT lead then contacts the remaining CMT members regarding the critical incident regardless of the time of day.
2. The CMT lead contacts the other CMT members to establish representation and availability.
3. Upon activation, respective CMT members will meet at one of these predesignated sites described below.
4. The IMT meets in order to manage the incident from the corporate office level. The IMT lead is responsible for tracking the incident status and updating the CMT lead as necessary, who in turn updates the other CMT members accordingly.
5. If the incident is at a local level impacting people, assets, or brand, the LRT lead is responsible for alerting the IMT lead. The LRT meets.

Crisis Management Meeting Locations

The CMT, IMT, and LRT should have clearly defined locations at which to meet and manage an incident. Some basic requirements of a primary and secondary meeting locations are the following:

- They are equidistant in opposite directions of the corporate office/key facility.
- There are sufficient tables, chairs, and meeting supplies for the team members.
- An extra copy of the company's BCP is secured there.
- There is ample parking.
- The site has redundant power, Internet, television, and telephone capability.
- The site is accessible 24/7.

(Note: A form for documenting the locations of crisis management meetings as well as critical phone numbers and contact information is provided in Appendix 8.)

Emergency Operations Center

An emergency operations center (EOC) is a room or facility staffed by personnel charged with commanding, controlling, and coordinating the use of resources and personnel in response to a crisis. This room may be located at the corporate office. The EOC must be available to use 24/7 to monitor emerging risks to the company and may also be used to support the management of a crisis. The EOC should have similar features to the CMT meeting locations mentioned above.

Response Procedures

When an incident occurs at the local level, the IMT lead will need to initiate an update from the LRT lead to determine the following:

- What information is confirmed and what is unconfirmed?
- What decisions have already been made?
- Does a decision on any portion of the emergency need to be made immediately?
- What are timelines for pending items?
- Who is impacted?
- Are any employees, customers, vendors, or members of the community still in danger?
- Are any employee emergency contacts arriving on site? Who will meet the emergency contacts and where will they be taken?

- Is the incident area now secure?
- If needed, can ingress and egress be controlled?
- Is additional security needed?
- What confirmed damage has occurred?
- Has anyone spoken to the media? What was said and to whom?
- Has a site spokesperson been established?
- Is there a need for an immediate media statement?

Subsequent to the primary collection of information, CMT, IMT, and LRT meetings may be held to assess, update, and respond accordingly to the incident during the response and recovery. In order to maximize the efficiency and effectiveness of the meeting, an agenda outline should be used when managing the crisis. (*Note: Examples of a CMT/IMT and an LRT meeting agenda are shown in Appendix 9.)* Meetings also serve to collect and disseminate information and to support the determination and prioritization of action steps. (*Note: Examples of a critical incident decision matrix and a critical incident individual decision matrix are shown in Appendices 10 and 11.)*

PILLAR IV: RECOVERY

Once the extent of damage is known, the process recovery needs should be prioritized and a schedule for resumption needs to be determined and documented. The prioritization should take into account the fundamental criticality of the process and other factors, including relationships to other processes, critical schedules, and regulatory requirements, as identified in the BIA. Decisions regarding prioritization of processes should be documented and recorded, including the date, time, and justification for the decisions.

Once the processes to be restored have been prioritized, the recovery work can begin. The resumption of these processes may occur at either the current worksite or an alternate worksite, depending on the circumstances of the crisis. A facility property damage checklist is an effective tool to provide documentation of the damage suffered and how recovery should be prioritized. (*Note: An example of a facility property damage checklist is shown in Appendix 12.)* As the critical processes resume, the resumption of the remaining processes can be addressed. Where possible, decisions about the prioritization of these processes should be thoroughly documented in advance, as should the timing of actual resumption.

Postincident Recovery and Record Keeping

The company's employees are encouraged to follow the instructions below once authorities have reported that the area is safe and has been cleared for reentry. If possible, obtain written evidence of this authorization.

- Attempt to secure the site. If you are not able to complete this task alone, contact your manager and use your best judgment.
- If the site cannot be secured, consult with management regarding the removal of high-value items from the site. Complete the facility property damage checklist (*Appendix 12*). Take detailed notes on all damage and take photographs, if possible.
- Take detailed notes on all damaged assets. Record the item description, item number, and quantity. Be realistic when estimating quantities.
- Test all equipment before use. If equipment needs repair, contact company-approved vendors for the specific equipment.
- Keep accurate records for hours spent by employees and outside vendors for clean-up or emergency repairs.
- Keep receipts for any expenses incurred for emergency repairs or replacement or for expedient replenishment of equipment, inventory, etc.
- Keep accurate records as to when sites are closed, by day and number of business hours, including financial information on lost revenues and any continued expenses during the shutdown period.
- Coordinate with the appropriate company management representatives prior to reopening the impacted facility(ies). Note date and time that the site reopened, together with the site's normal business hours.
- Report any public or governmental order affecting site operation.
- Report on activity of other businesses in the vicinity or any unusual activity or extraordinary conditions occurring in the vicinity.
- Fill out the company incident report form (*Appendix 13*). Attach additional pages of documentation with the incident report if necessary.
- Send the completed incident report form along with all documentation to the appropriate company department.

Return to Normal Operations

The main objective of a BCP is to bring the company back to normal operations. If it is not possible to return to the precrisis normal, a new normal should be established. This new normal creates the expectation that, while there may be changes and restructuring in the workplace, the organization will phase back into productive work. Each step of the process and all decisions should be carefully documented.

As a rule, it is at this point that the crisis may be officially declared over. Again, it is important to document this decision. Press conferences and mass media communications may be undertaken to bolster employee and client confidence.

Corrective Action Plan

Any time a simulation exercise or an actual crises occurs a postmortem should be performed. If any failures, deficiencies, or weaknesses in the BCP are identified during the postmortem, a corrective action plan should be created. This documentation is then used to guide changes to the BCP in order to improve the process and avoid future problems.

When evaluating the response to an event, simulated or otherwise, notes should be gathered about what went well and what could be improved upon. This evaluation should include people, processes, and resources. It may be helpful to note that the NFPA 1600 Standard[8] categorizes corrective actions as follows:

1. Plan or standard operating procedures (SOP) revisions
2. Training
3. Equipment additions or modifications and facilities

Once the corrective action plan is completed, the results should be used to guide the necessary modifications to the existing BCP. As with any changes to the BCP, the BCP team should plan for and perform the appropriate training and exercise(s) to ensure the changes are communicated and prepared for.