Business Continuity

GUIDELINE

A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery

ASIS INTERNATIONAL

Advancing Security Worldwide™

ASIS INTERNATIONAL COMMISSION ON GUIDELINES

The Commission on Guidelines was established in early 2001 by ASIS International (ASIS) in response to a concerted need for guidelines regarding security issues in the United States. As the preeminent organization for security professionals worldwide, ASIS has an important role to play in helping the private sector secure its business and critical infrastructure, whether from natural disaster, accidents, or planned actions, such as terrorist attacks, vandalism, etc. ASIS had previously chosen not to promulgate guidelines and standards, but world events have brought to the forefront the need for a professional security organization to spearhead an initiative to create security advisory provisions. By addressing specific concerns and issues inherent to the security industry, security guidelines will better serve the needs of security professionals by increasing the effectiveness and productivity of security practices and solutions, as well as enhancing the professionalism of the industry.

Mission Statement

To advance the practice of security through the development of risk mitigation guidelines within a voluntary, non-proprietary, and consensus-based process utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership and the security industry.

Goals and Objectives

- Assemble and categorize a database of existing security-related guidelines
- Develop methodology for identifying new guideline development projects
- Involve/organize ASIS Councils to support guideline development
- Identify and develop methodology for development, documentation, and acceptance of guidelines
- Develop and sustain alliances with related organizations to benchmark, participate, and support ASIS guideline development
- Produce national consensus-based guidelines in cooperation with other industries and the Security Industry Standards Council

Functions

- Establish guideline project
- Determine guidelines for development and assign scope
- Assign participating Council(s), where appropriate
- Approve membership on guideline committee
- Act as a governing body to manage and integrate guidelines from various Councils and security disciplines
- Review and monitor projects and guideline development
- Approve Final Draft Guideline and Final Guideline
- Select guidelines for submission to the Security Industry Standards Council and the American National Standards Institute (ANSI)

BUSINESS CONTINUITY GUIDELINE:

A PRACTICAL APPROACH FOR EMERGENCY PREPAREDNESS, CRISIS MANAGEMENT, AND DISASTER RECOVERY

ASIS GDL BC 01 2005

ASIS GDL BC 01 2005

Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery

This page intentionally left blank

1.0 TITLE

The title of this document is Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery.

2.0 REVISION HISTORY

Baseline Document

3.0 COMMISSION MEMBERS

Sean A. Ahrens, CPP, Schirmer Engineering
Norman D. Bates, Esq., Liability Consultants, Inc.
Regis W. Becker, CPP, PPG Industries
Jerry J. Brennan, Security Management Resources, Inc.
Chad Callaghan, CPP, Marriott International, Inc.
Pamela A. Collins, Ed.D., CFE, Eastern Kentucky University
Michael A. Crane, CPP, IPC International Corporation
Edward J. Flynn, CFE, Protiviti, Inc.
F. Mark Geraci, CPP, Bristol-Myers Squibb Co.
L. E. Mattice, Boston Scientific Corp.
Basil J. Steele, CPP, Sandia National Laboratories
Don W. Walker, CPP, Securitas Security Services USA, Inc.

4.0 COMMITTEE MEMBERS

Robert M. Baldwin, CPP, Control Risks Group LLC
Regis W. Becker, CPP, PPG Industries
Lawrence K. Berenson, CPP, L-3 Communications, Inc.
Edward G. Casey, CPP, Procter & Gamble Company
Martin Cramer, CPP, United Building Security, Inc.
Richard L. Engel, CPP, BAE Systems
Gregory Gilbert, CPP, New Covenant Church of Philadelphia
S. Ronald Hauri, CPP, Aon Corporation
Robert F. Lang, CPP, Georgia Institute of Technology
Richard E. Mainey, Marsh & McLennan Companies, Inc.
Daniel J. Muscat, Whirlpool Corporation
E. Floyd Phelps, CPP, Southern Methodist University
Thomas Smith, Comcast Corporation
Penny Turnbull, Ph.D., CBCP, Marriott International, Inc.
Kelly Jane Wilson, Deloitte Services LP

5.0 GUIDELINES DESIGNATION

This guideline is designated as ASIS GDL BC 01 2005.

6.0 SCOPE

The Business Continuity (BC) Guideline has applicability in both the private and public sector environments. The BC Guideline is a series of interrelated processes and activities that will assist in creating, testing, and maintaining an organization-wide plan for use in the event of a crisis that threatens the viability and continuity of the organization.

7.0 SUMMARY

The BC Guideline is a tool to allow organizations to consider the factors and steps necessary to prepare for a crisis (disaster or emergency) so that it can manage and survive the crisis and take all appropriate actions to help ensure the organization's continued viability. The advisory portion of the guideline is divided into two parts: (1) the planning process and (2) successful implementation and maintenance. Part One provides step-by-step Business Continuity Plan preparation and activation guidance, including readiness, prevention, response, and recovery/resumption. Part Two details those tasks required for the Business Continuity Plan to be maintained as a living document, changing and growing with the organization and remaining relevant and executable. Appendix A offers the ASIS Business Continuity Guideline Checklist.

8.0 PURPOSE

Recent world events have challenged us to prepare to manage previously unthinkable situations that may threaten an organization's future. This new challenge goes beyond the mere emergency response plan or disaster management activities that we previously employed. Organizations now must engage in a comprehensive process best described generically as *Business Continuity*. It is no longer enough to draft a response plan that anticipates naturally, accidentally, or intentionally caused disaster or emergency scenarios. Today's threats require the creation of an on-going, interactive process that serves to assure the continuation of an organization's core activities before, during, and most importantly, after a major crisis event.

In the simplest of terms, it is good business for a company to secure its assets. CEOs and shareholders must be prepared to budget for and secure the necessary resources to make this happen. It is necessary that an appropriate administrative structure be put in place to effectively deal with crisis management. This will ensure that all concerned understand who makes decisions, how the decisions are implemented, and what the roles and responsibilities of participants are. Personnel used for crisis management should be assigned to perform these roles as part of their normal duties and not be expected to perform them on a voluntary basis. Regardless of the organization—for profit, not for profit, faith-based, non-governmental—its leadership has a duty to stakeholders to plan for its survival. The vast majority of the national critical infrastructure is owned and operated by private sector organizations, and it is largely for these organizations that this guideline is intended. ASIS, the world's largest organization of security professionals, recognizes these

facts and believes the BC Guideline offers the reader a user-friendly method to enhance infrastructure protection.

9.0 KEY WORDS

Business Continuity Plan, Business Impact Analysis, Crisis Management Team, Critical Functions, Damage Assessment, Disaster, Evaluation and Maintenance, Mitigation Strategies, Mutual Aid Agreement, Prevention, Readiness, Recovery/Resumption, Resource Management, Response, Risk Assessment, Testing and Training.

10.0 TERMINOLOGY

Alternate Worksite– A work location, other than the primary location, to be used when the primary location is not accessible.

Business Continuity– A comprehensive managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis.

Business Continuity Plan (BCP)– An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the continuity of operations through personnel training, plan testing, and maintenance.

Business Impact Analysis (BIA)– A management level financial analysis that identifies the impacts of losing an organization's resources. The analysis measures the effect of resource loss and escalating losses over time in order to provide reliable data upon which to base decisions on mitigation, recovery, and business continuity strategies.

Contact List– A list of team members and key players in a crisis. The list should include home phone numbers, pager numbers, cell phone numbers, etc.

Crisis– Any global, regional, or local natural or human-caused event or business interruption that runs the risk of (1) escalating in intensity, (2) adversely impacting shareholder value or the organization's financial position, (3) causing harm to people or damage to property or the environment, (4) falling under close media or government scrutiny, (5) interfering with normal operations and wasting significant management time and/or financial resources, (6) adversely affecting employee morale, or (7) jeopardizing the organization's reputation, products, or officers, and therefore negatively impacting its future.

Crisis Management– Intervention and coordination by individuals or teams before, during, and after an event to resolve the crisis, minimize loss, and otherwise protect the organization.

Crisis Management Center– A specific room or facility staffed by personnel charged with commanding, controlling, and coordinating the use of resources and personnel in response to a crisis.

Crisis Management Planning– A properly funded ongoing process supported by senior management to ensure that the necessary steps are taken to identify and analyze the

adverse impact of crisis events, maintain viable recovery strategies, and provide overall coordination of the organization's timely and effective response to a crisis.

Crisis Management Team– A group directed by senior management or its representatives to lead incident/event response comprised of personnel from such functions as human resources, information technology facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions.

Critical Function– Business activity or process that cannot be interrupted or unavailable for several business days without having a significant negative impact on the organization.

Critical Records– Records or documents that, if damaged, destroyed, or lost, would cause considerable inconvenience to the organization and/or would require replacement or re-creation at a considerable expense to the organization.

Damage Assessment– The process used to appraise or determine the number of injuries and human loss, damage to public and private property, and the status of key facilities and services resulting from a natural or human-caused disaster or emergency.

Disaster– An unanticipated incident or event, including natural catastrophes, technological accidents, or human-caused events, causing widespread destruction, loss, or distress to an organization that may result in significant property damage, multiple injuries, or deaths.

Disaster Recovery– Immediate intervention taken by an organization to minimize further losses brought on by a disaster and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition.

Emergency– An unforeseen incident or event that happens unexpectedly and demands immediate action and intervention to minimize potential losses to people, property, or profitability.

Evacuation– Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas.

Evaluation and Maintenance– Process by which a business continuity plan is reviewed in accordance with a predetermined schedule and modified in light of such factors as new legal or regulatory requirements, changes to external environments, technological changes, test/exercise results, personnel changes, etc.

Exercise– An activity performed for the purpose of training and conditioning team members and personnel in appropriate crisis responses with the goal of achieving maximum performance.

Maintenance– See Evaluation and Maintenance.

Mitigation Strategies– Implementation of measures to lessen or eliminate the occurrence or impact of a crisis.

Mutual Aid Agreement– A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.

Prevention– Plans and processes that will allow an organization to avoid, preclude, or limit the impact of a crisis occurring. The tasks included in prevention should include compliance with corporate policy, mitigation strategies, and behavior and programs to support avoidance and deterrence and detection.

Readiness– The first step of a business continuity plan that addresses assigning accountability for the plan, conducting a risk assessment and a business impact analysis, agreeing on strategies to meet the needs identified in the risk assessment and business impact analysis, and forming Crisis Management and any other appropriate response teams.

Recovery/Resumption– Plans and processes to bring an organization out of a crisis that resulted in an interruption. Recovery/resumption steps should include damage and impact assessments, prioritization of critical processes to be resumed, and the return to normal operations or to reconstitute operations to a new condition.

Response– Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population. Response steps should include potential crisis recognition, notification, situation assessment, and crisis declaration, plan execution, communications, and resource management.

Risk Assessment– Process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.

Shelter-in-Place– The process of securing and protecting people and assets in the general area in which a crisis occurs.

Simulation Exercise– A test in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises are performed under conditions as close as practicable to ''real world'' conditions.

Tabletop Exercise– A test method that presents a limited simulation of a crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation.

Testing– Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties and to reveal weaknesses in the Business Continuity Plan.

Training– An educational process by which teams and employees are made qualified and proficient about their roles and responsibilities in implementing a Business Continuity Plan.

Vital Records– Records or documents, for legal, regulatory, or operational purposes, that if irretrievably damaged, destroyed, or lost, would materially impair the organization's ability to continue business operations.
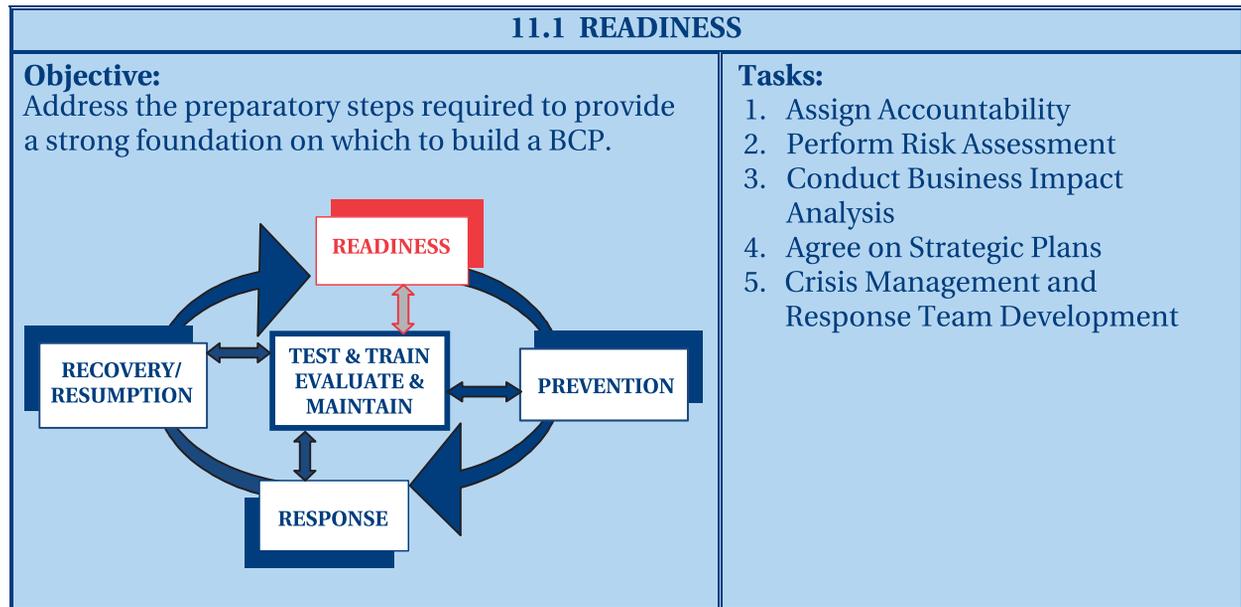
11.0 PRACTICE ADVISORY—PART ONE

The Business Continuity Guideline is comprised of two sections: (1) the planning process and (2) successful implementation and maintenance.

Note: Business continuity planning is cyclical. Rigorous plan administration and maintenance, as well as any events experienced, will necessitate revisions and/or plan additions.

DEVELOPING THE PLAN

This section addresses the process of preparing a Business Continuity Plan (BCP), including readiness, prevention, response, and recovery/resumption. It details the specific BCP elements and provides step-by-step plan preparation and activation guidance. The specifics of this guideline are appropriate for a mid- to large-sized organization. By understanding the concepts and procedures described, it will be possible to effectively adapt the guideline to smaller-sized organizations. The level of effort may vary widely, but the basic approach of preparedness and response should be constant.

11.1 READINESS	
Objective: Address the preparatory steps required to provide a strong foundation on which to build a BCP. 	**Tasks:** 1. Assign Accountability 2. Perform Risk Assessment 3. Conduct Business Impact Analysis 4. Agree on Strategic Plans 5. Crisis Management and Response Team Development

11.1.1 Assign Accountability

It is essential that senior leadership of the organization sponsors and takes responsibility for creating, maintaining, testing, and implementing a comprehensive Business Continuity Plan (BCP). This will insure that management and staff at all levels within the organization understand that the BCP is a critical top management priority. It is equally essential that senior leadership engage a ''top down'' approach to the BCP so that management at all levels of the organization understand accountability for effective and efficient plan maintenance as part of the overall governance priorities.

11.1.1.a Corporate Policy
In the event of a crisis, an organization-wide BCP Policy committed to undertaking all reasonable and appropriate steps to protect people, property, and business interests is essential. Corporate policy should include a definition of a ''crisis.''

11.1.1.b Ownership of Systems, Processes, and Resources
Responsibility for systems and resource availability and key business processes should be clearly identified in advance.

11.1.1.c Planning Team
A Business Continuity Planning Team with responsibility for BCP development that includes senior leaders from all major organizational functions and support groups should be appointed to ensure wide-spread acceptance of the BCP.

11.1.1.d Communicate BCP
The BCP should be communicated throughout the organization, to ensure employees are aware of the BCP structure and their roles within the plan.

11.1.2 Perform Risk Assessment

Step two in the creation of a comprehensive BCP is completion of a Risk Assessment, designed to identify and analyze the types of risk that may impact the organization. Assessment should be performed by a group representing various organizational functions and support groups. More detailed information on Risk Assessments can be found in the ASIS General Security Risk Assessment Guideline, available at www.asisonline.org/ guidelines/guidelines.htm.

11.1.2.a Review Types of Risks That Could Impact the Business
Using available information about known or anticipated risks, the organization should identify and review risks that could possibly impact the business, and rate the likelihood of each. A Risk Assessment matrix can aid identification of risks and prioritization of mitigation/planning strategies.

The sample matrix below illustrates threat examples and demonstrates how risks can be categorized and quantified. Note: this list is not exhaustive and should be tailored to reflect the organization's operating environment. *Additional variables such as onset speed (1=slow, 2=fast), forewarning (1=sufficient, 2=insufficient), duration (1=short, 2=long) and intensity (1=low, 2=high) can also be added as additional columns and entered in the formula: e.g., likelihood x (onset speed + forewarning + duration + intensity) x impact = relative weight.*

Threat or Trigger	Likelihood (Rate 1-5)	X	Impact (Rate 1-5)	=	Relative Weight
	1=Very Low *2=Low* *3=Medium* *4=High* *5= Very High*		*1=Negligible* *2=Some* *3=Moderate* *4=Significant* *5= Severe*		
Earthquake		x		=	
Power Failure		x		=	
Fire		x		=	
Hurricane		x		=	
Flood		x		=	
Bombing		x		=	
NBC* Attack at Site		x		=	
NBC* Attack within 50 miles		x		=	
Cyber Attack		x		=	
Kidnapping		x		=	
Sabotage		x		=	
Hazmat Accident		x		=	
Product Recall		x		=	
Public Health		x		=	
Work Stoppage		x		=	

*Nuclear, Biological, and Chemical

11.1.3 Conduct Business Impact Analysis (BIA)

Once risks have been identified, any organizational impacts that could result from an interruption of normal operations should be examined in a Business Impact Analysis (BIA).

11.1.3.a Identify Critical Processes
Business critical processes should be identified and documented. They could include purchasing, manufacturing, supply chain, sales, distribution, accounts receivable, accounts payable, payroll, IT, and research and development. Once the critical processes are identified, an analysis of each can be made using the evaluation criteria described below. Processes should be ranked as a High, Medium, or Low.

11.1.3.b Assess Impact if Crisis Were to Happen

- Human cost: physical and psychological harm to employees, customers, suppliers, other stakeholders, etc.
- Financial cost: equipment and property replacement, downtime, overtime pay, stock devaluation, lost sales/business, lawsuits, regulatory fines/penalties, etc.
- Corporate image cost: reputation, standing in the community, negative press, loss of customers, etc.

11.1.3.c Determine Maximum Allowable Outage and Recovery Time Objectives

- Determine how long process can be nonfunctional before impacts become unacceptable
- Determine how soon process should be restored (shortest allowable outage restored first)
- Determine different recovery time objectives according to time of year (year-end, tax filing, etc.)
- Identify and document alternate procedures to a process (manual workarounds or processes, blueprints, notification/calling trees, etc.)
- Evaluate costs of alternate procedures versus waiting for system to be restored.

11.1.3.d Identify Resources Required for Resumption and Recovery
Such resources can include personnel, technology hardware and software (including telecommunications), specialized equipment, general office supplies, facility/office space and critical and vital business records. Identifying, backing-up, and storing critical and vital business records in a safe and accessible location are essential prerequisites for an effective BCP.

> The Risk Assessment and BIA provide the foundation on which the organization's BCP will rest, as strategies will be formulated and plans will be developed to meet the needs identified in them. These analyses should be repeated on a regular basis and/or in response to significant changes to the organization's operating environment.

11.1.4 Agree on Strategic Plans

Strategic planning addresses the identification and implementation of:

- Methods to mitigate the risks and exposures identified in the BIA and Risk Assessment (see 11.2 Prevention)
- Plans and procedures to respond to any crisis that does occur.

A BCP may include multiple strategies that address a variety of probable situations, including the duration of the business interruption (short versus long term), the period in

which it occurs (peak versus low), and the extent of the interruption (partial versus complete). It is important that the strategies selected are:

- Attainable
- Highly probable to be successful
- Verifiable through tests and exercises
- Cost effective
- Appropriate for the size and scope of the organization.

## 11.1.5 Crisis Management and Response Team Development

It is necessary that an appropriate administrative structure be put in place to effectively deal with crisis management. Clear definitions must exist for a management structure, authority for decisions, and responsibility for implementation. An organization should have a Crisis Management Team to lead incident/event response. The Team should be comprised of such functions as human resources, information technology, facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions, with all under the clear direction of senior management or its representatives.

The Crisis Management Team may be supported by as many Response Teams as appropriate taking into account such factors as organization size and type, number of employees, location, etc. Response Teams should develop Response Plans to address various aspects of potential crises, such as damage assessment, site restoration, payroll, human resources, information technology, and administrative support. Response Plans should be consistent with and included within the overall BCP. Individuals should be recruited for membership on Response Teams based upon their skills, level of commitment, and vested interest.

11.1.5.a Contact Information
Contact information for personnel assigned to crisis management and response teams should be included in the plans. Personal information such as unlisted phone numbers and home addresses should be protected. The organization should establish procedures to ensure that the information is kept up to date. Consideration should be given to a BCP software tool that supports effective change management. (See also 12.2 Evaluation and Maintenance.)

11.2 PREVENTION	
Objective: Address those areas where good planning will allow an organization to avoid, prevent, or limit the impact of a crisis occurring. READINESS RECOVERY/ RESUMPTION — TEST & TRAIN EVALUATE & MAINTAIN — PREVENTION RESPONSE	**Tasks:** 1. Compliance with Corporate Policy 2. Mitigation Strategies 3. Avoidance, Deterrence and Detection
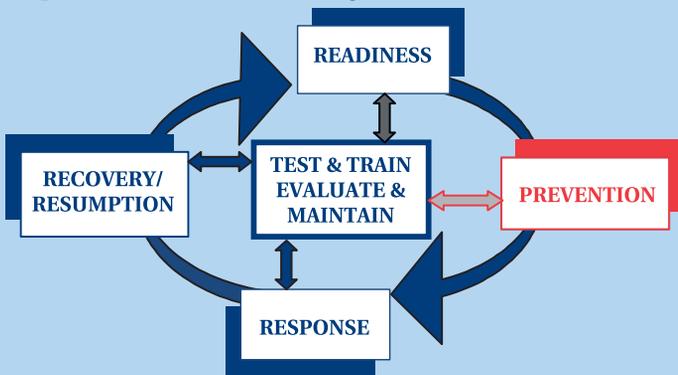
11.2.1 Compliance with Corporate Policy

Compliance audits should be conducted to enforce BCP policies and procedures. Policy and procedures violations should be highlighted and accountability for corrective action assigned in accordance with organizational governance regimes.

11.2.2 Mitigation Strategies

11.2.2.a Devise Mitigation Strategies
Cost effective mitigation strategies should be employed to prevent or lessen the impact of potential crises. For example, securing equipment to walls or desks with strapping can mitigate damage from an earthquake; sprinkler systems can lessen the risk of a fire; a strong records management and technology disaster recovery program can mitigate the loss of key documents and data.

11.2.2.b Resources Needed for Mitigation
The various resources that would contribute to the mitigation process should be identified. These resources, including essential personnel and their roles and responsibilities, facilities, technology, and equipment should be documented in the plan and become part of ''business as usual.''

11.2.2.c Monitoring Systems and Resources
Systems and resources should be monitored continually as part of mitigation strategies. Such monitoring can be likened to simple inventory management.

The resources that will support the organization to mitigate the crisis should also be monitored continually to ensure that they will be available and able to perform as planned during the crisis. Examples of such systems and resources include, but are not limited to:

- Emergency equipment

- Fire alarms and suppression systems

- Local resources and vendors

- Alternate worksites

- Maps and floor plans updated/changed due to construction and internal moves

- System backups and offsite storage.
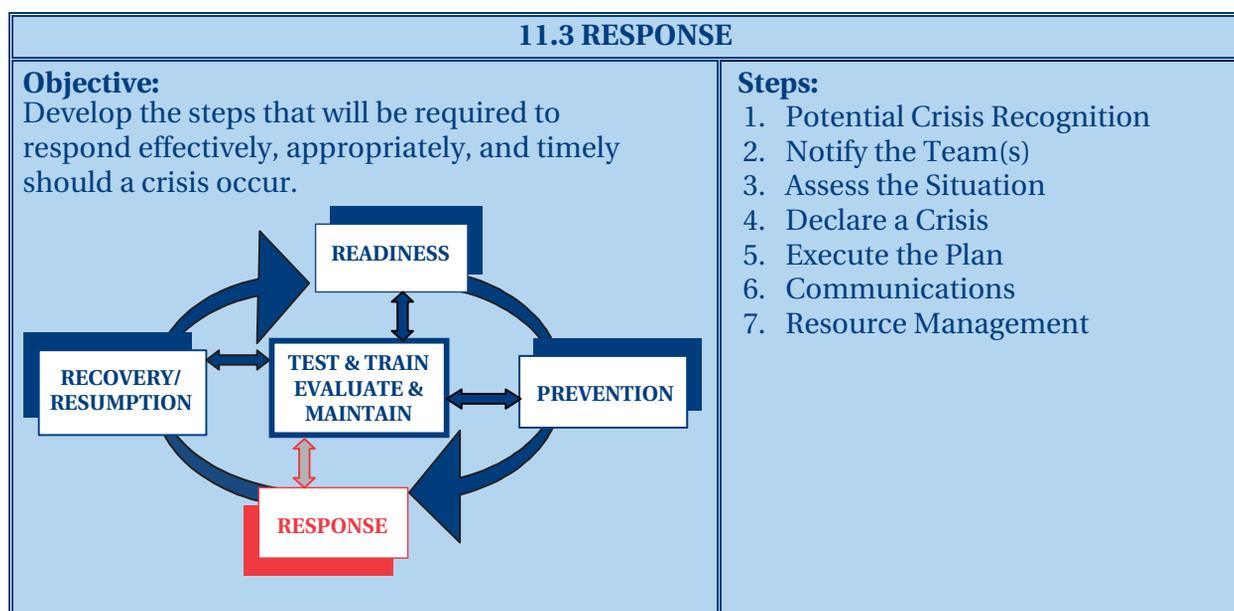
11.2.3 Avoidance, Deterrence and Detection

Avoidance	Deterrence and Detection
Avoidance has the goal of preventing a crisis from happening. The potential crisis should be identified, understood, and addressed and, in doing so, avoided. The Risk Assessment can be used to identify the specifics of potential crises, including any precursors and warning signs.	The purpose of deterrence and detection is to make a hostile act (or activity) more difficult to carry out against the organization or significantly limit, if not negate, its impact. The BCP should address and include overall deterrence and detection measures.

Examples of crises that can have warning signs include, but are not limited to:
- *Workplace violence (erratic or threatening employee behavior)*
- *Natural disasters (hurricanes, wild-fires, etc.)*
- *Activism, protests, riots*
- *Product or manufacturing failure*
- *Hostile takeover*
- *Terrorism*
- *Lawsuits.*

11.2.3.a. Employee Behavior to Support Avoidance and Deterrence and Detection
Employees should be appropriately motivated to feel personally responsible for avoidance and deterrence and detection. Through the proper corporate climate, operational plans, and management objectives, employees should support avoidance and deterrence and detection policies and procedures.

11.2.3.b Facility Security Programs to Support and Enhance Avoidance and Deterrence and Detection

- Architectural: natural or manmade barriers.

- Operational: security officers' post orders; employee security awareness programs; counter surveillance and counter intelligence as avoidance, detection and deterrence measures; and Protective Security Operations for the protection of the leadership and their families.

- Technological: intrusion detection, access control, recorded video surveillance, package and baggage screening, when appropriate.

11.3 RESPONSE

Objective:
Develop the steps that will be required to respond effectively, appropriately, and timely should a crisis occur.

READINESS

RECOVERY/
RESUMPTION

TEST & TRAIN
EVALUATE &
MAINTAIN

PREVENTION

RESPONSE

Steps:
1. Potential Crisis Recognition
2. Notify the Team(s)
3. Assess the Situation
4. Declare a Crisis
5. Execute the Plan
6. Communications
7. Resource Management

11.3.1 Potential Crisis Recognition

The first element in a response program is to determine if a potential crisis exists. The organization should know and be able to easily recognize when specific dangers occur that necessitate the need for some level of response. A strong program of avoidance and deterrence and detection policies and procedures as outlined above will support this process.

11.3.1.a Identification and Recognition of Danger Signals
Identification of danger signals coupled with the likelihood of an event is often indicative of an imminent crisis. Warning signs may include, but are not limited to:

- Unusual or unexplained changes in sales volume
- Legislative changes
- Corporate policy changes
- Changes to competitive environment
- Changes to supply based environment
- Warnings of natural disasters
- Imminent or actual changes in Homeland Security Advisory System threat level
- Cash flow changes
- Potential for civil or political instability
- Impending strike or likely protests
- Hostile labor negotiations.

11.3.1.b Responsibility to Recognize and Report Potential Crises
Certain departments or functions are uniquely situated to observe warning signs of an imminent crisis. Personnel assigned to these departments or functions should be trained

appropriately. The responsibility to report a potential crisis (including the notification mechanism) should be communicated to all employees. The general employee population may also be an excellent source of predictive information when there is a documented reporting structure and where attention is paid to what the employee reports.

11.3.2 Notify the Team(s)

A potential crisis, once recognized, should be immediately reported to a supervisor, a member of management, or another individual tasked with the responsibility of crisis notification and management.

11.3.2.a Parameters for Notification
Specific notification criteria should be established, documented, and adhered to by all employees (with the timing and sequence of notification calls clearly documented). The actual activation of a response process should require very specific qualifications being met.

11.3.2.b Custody and Updates to Contact Information
Qualified personnel should have ready access to the updated, confidential listings of persons and organizations to be contacted when certain conditions or parameters of a potential crisis are met.

11.3.2.c Types of Notification
Notifications in a crisis situation should be timely and clear and should use a variety of procedures and technologies, with recognition that devices used have advantages and limitations.

> Remember: In some types of crises, the notification systems are themselves impacted by the disaster, whether through capacity issues or infrastructure damage. Thus, it is important to have redundancies built into the notification system and several different ways to contact the listed individuals and organizations.

11.3.3 Assess the Situation

Problem assessment (an evaluative process of decision making that will determine the nature of the issue to be addressed) and severity assessment (the process of determining the severity of the crisis and what any associated costs may be in the long run) should be made at the outset of a crisis. Factors to be considered include the size of the problem, its potential for escalation, and the possible impact of the situation.

11.3.4 Declare a Crisis

The point at which a situation is declared to be a crisis should be clearly defined, documented, and fit very specific and controlled parameters. Responsibility for declaring a crisis should also be clearly defined and assigned. First and second alternates to the responsible individual should be identified.

The activities that declaring a crisis will trigger include, but are not limited to:

- Additional call notification
- Evacuation, shelter, or relocation
- Safety protocol
- Response site and alternate site activation
- Team deployment
- Personnel assignments and accessibility
- Emergency contract activation
- Operational changes.

In certain situations, there may be steps that can and should be implemented, even without officially declaring a crisis.

11.3.5 Execute the Plan

BCPs should be developed around a ''worst case scenario,'' with the understanding that the response can be scaled appropriately to match the actual crisis. When initiating a response, it is important to insure that the goals protect the following interests listed in order of their priority:

- Save lives and reduce chances of further injuries/deaths
- Protect assets
- Restore critical business processes and systems
- Reduce the length of the interruption of business
- Protect reputation damage
- Control media coverage (e.g. local, regional, national or global)
- Maintain customer relations.

Prioritized classifications can be set up as relative indicators of the magnitude, severity, or potential impact of the situation:

Level 1	Level 2	Level 3	Level 4
Routine emergency incidents	Minor business interruptions • No casualties • Minimal damage • Limited impact on customer service • No community impact • Local media only	Moderate business interruptions • Several injuries or deaths • Moderate damage • Some impact on customer service • Moderate community impact • National media	Major business interruptions • Major impact in all areas

These levels may aid organizations that are developing response plans and implementation ''triggers'' for use during a crisis. Determining the initial level of the crisis and the progression from one level to the next will normally be the responsibility of the Crisis Management Team.

11.3.6 Communications

Remember: Effective communication is one of the most important ingredients in crisis management.

11.3.6.a Identify the Audiences
Internal and external audiences should be identified in order to convey crisis and organizational response information. In order to provide the best communications and suitable messages for various groups, it is often appropriate to segment the audiences. In this way, messages tailored specifically for a group can be released.

Internal	External
• Employees and their families • Business Owners/Partners • Boards of Directors • Onsite Contractors/Vendors	• Customers/Clients, present and potential • Contractors/Vendors • Media • Government and Regulatory Agencies • Local law enforcement • Emergency responders • Investors/Shareholders • Surrounding communities

11.3.6.b Communicating With Audiences
The following items should be taken into account in the crisis communications strategy:

- Communications should be timely and honest.

- To the extent possible, an audience should hear news from the organization first.

- Communications should provide objective and subjective assessments.

- All employees should be informed at approximately the same time.

- Give bad news all at once – do not sugarcoat it.

- Provide opportunity for audiences to ask questions, if possible.

- Provide regular updates and let audiences know when the next update will be issued.

- Treat audiences as you would like to be treated.

- Communicate in a manner appropriate to circumstances:
    - Face-to-face meetings (individual and group)
    - News conferences
    - Voice mail/email

- ◦ Company Intranet and Internet sites
- ◦ Toll-free hotline
- ◦ Special newsletter
- ◦ Announcements using local/national media.

> Preplanning for communications is critical. Drafts of message templates, scripts, and statements can be crafted in advance for threats identified in the Risk Assessment. Procedures to ensure that communications can be distributed at short notice should also be established, particularly when using resources such as Intranet and Internet sites and toll-free hotlines.

11.3.6.c Official Spokesperson

The organization should designate a single primary spokesperson, with back-ups identified, who will manage/disseminate crisis communications to the media and others. This individual should be trained in media relations prior to a crisis. All information should be funneled through a single source to assure that the messages being delivered are consistent. It should be stressed that personnel should be informed quickly regarding where to refer calls from the media and that only authorized company spokespeople are authorized to speak to the media. In some situations, an appropriately trained site spokesperson may also be necessary.

11.3.7 Resource Management

11.3.7.1 The Human Element

People are the most important aspect of any BCP. How an organization's human resources are managed will impact the success or failure of crisis management.

11.3.7.1.a Accounting for All Individuals

A system should be devised by which all personnel can be accounted for quickly after the onset of a crisis. This system could range from a simple telephone tree to an elaborate external vendor's call-in site. Current and accurate contact information should be maintained for all personnel. Consideration should be given to engaging the company's travel agency to assist in locating employees on business travel.

11.3.7.1.b Notification of Next-of-Kin

Arrangements should be made for notification of any next-of-kin in case of injuries or fatalities. If at all possible, notification should take place in person by a member of senior management. Appropriate training should be provided.

11.3.7.1.c Family Representatives

The organization should implement a Family Representative program in case of severe injury or fatality. The Family Representative should be someone other than the person who performed the notification. This Representative should act as the primary point of contact between the family and the organization. Comprehensive training for the Representative is a necessity.

11.3.7.1.d Crisis Counseling

Crisis counseling should be arranged as necessary. In many cases, such counseling goes beyond the qualifications and experience of an organization's Employee Assistance Program (where available). Other reliable sources of counseling should be identified prior to a crisis situation.

11.3.7.1.e Financial Support

A crisis may have far reaching financial implications for the organization, its employees and their families, and other stakeholders; these implications should be considered an important part of a BCP. Implications may include financial support to families of victims. Additionally, there may be tax implications that should be referenced and clarified in advance.

11.3.7.1.f Payroll

The payroll system should remain functional throughout the crisis.

11.3.7.2 Logistics

Logistical decisions made in advance will impact the success or failure of a good BCP. Among them are the following:

11.3.7.2.a Crisis Management Center

A primary Crisis Management Center should be identified in advance. This is the initial site used by the Crisis Management Team and Response Teams for directing and overseeing crisis management activities. The site should have an uninterruptible power supply, essential computer, telecommunications, heating/ventilating/air conditioning systems, and other support systems. Additionally, emergency supplies should be identified and kept in the Center.

Where a dedicated Center is not possible, a designated place where the Teams may direct and oversee crisis management activities should be guaranteed. Access control measures should be implemented, with the members of all Teams given 24x7 access.

A secondary Crisis Management Center should also be identified in the event that the primary Center is impacted by the crisis event.

11.3.7.2.b Alternate Worksites

The organization should have alternate worksites identified for business resumption and recovery. In the absence of other company facilities being available and/or suitable, access to alternate worksites can be arranged through appropriate vendors. Planning concerning the identification and availability of alternate worksites should take place early in the BCP process. Alternate worksites should provide adequate access to the resources required for business resumption identified in the BIA.

11.3.7.2.c Offsite Storage

Offsite storage is a valuable mitigation strategy allowing rapid crisis response and business recovery/resumption. The off-site storage location should be a sufficient distance from the primary facility so that it is not likely to be similarly affected by the same event. Items to be considered for off-site storage include critical and vital records (paper and other media) necessary to the operations of the business. Procedures should be included in the plan to ensure the timely deliver of any necessary items from offsite storage to the Crisis Management Center or the alternate worksites.

11.3.7.3 Financial Issues and Insurance

If appropriate, existing funding and insurance policies should be examined, and additional funding and insurance coverage should be identified and obtained. Policy parameters should be established in advance, including pre-approval by the insurance provider of any response related vendors. Where possible, the amount of funds to help ensure continuity of operations should be determined in the planning process. Additionally, any cash should be stored in an easily accessible location to assure its availability during a crisis, and some cash and credit should be available for weekend and after-hours requirements.

All crisis related expenses should be recorded throughout the response and recovery/ resumption periods.

Insurance providers should be contacted as early as possible in the crisis period, particularly in instances of a wide-reaching crisis, where competition for such resources could be vigorous. All insurance policy and contact information should be readily available to the Crisis Management Team and backed up or stored offsite as appropriate.

11.3.7.4 Transportation

Transportation in a time of crisis can be a challenge. Provisions should be arranged ahead of time, if possible. Areas where transportation is critical include, but are not limited to:

- Evacuation of personnel (e.g., from a demolished work-site or from a satellite facility in another country)
- Transportation to an alternate worksite
- Supplies into the site or to an alternate site
- Transportation of critical data to worksite
- Transportation for staff with special needs.

11.3.7.5 Suppliers/Service Providers

Critical vendor or service provider agreements should be established as appropriate and their contact information maintained as part of the BCP. Such information could include phone numbers, contact names, account numbers, pass-codes (appropriately protected), and other information in the event that someone unfamiliar with the process would need to make contact.

In some instances, it may be appropriate to request and review the BCP, or a summary of such, of the critical vendors, in order to evaluate their ability to continue to provide necessary supplies and services in the case of a far-reaching crisis. At a minimum, the vendor's or service provider's roles and service level agreements should be discussed in advance of the crisis.

11.3.7.6 Mutual Aid Agreements

Mutual aid agreements identify resources that may be borrowed from other organizations during a crisis, as well as mutual support that may be shared with other organizations. Such agreements should be legally sound and properly documented, clearly understood by all parties involved, and representative of dependable resources as well as a commitment to cooperation.

11.4 RECOVERY AND RESUMPTION

Objective:
Develop policies, procedures and plans to bring the organization out of the crisis, recover/resume critical processes, and finally return to normal operations.

Steps:
1. Damage and Impact Assessment
2. Resumption of Critical and Remaining Processes
3. Return to Normal Operations
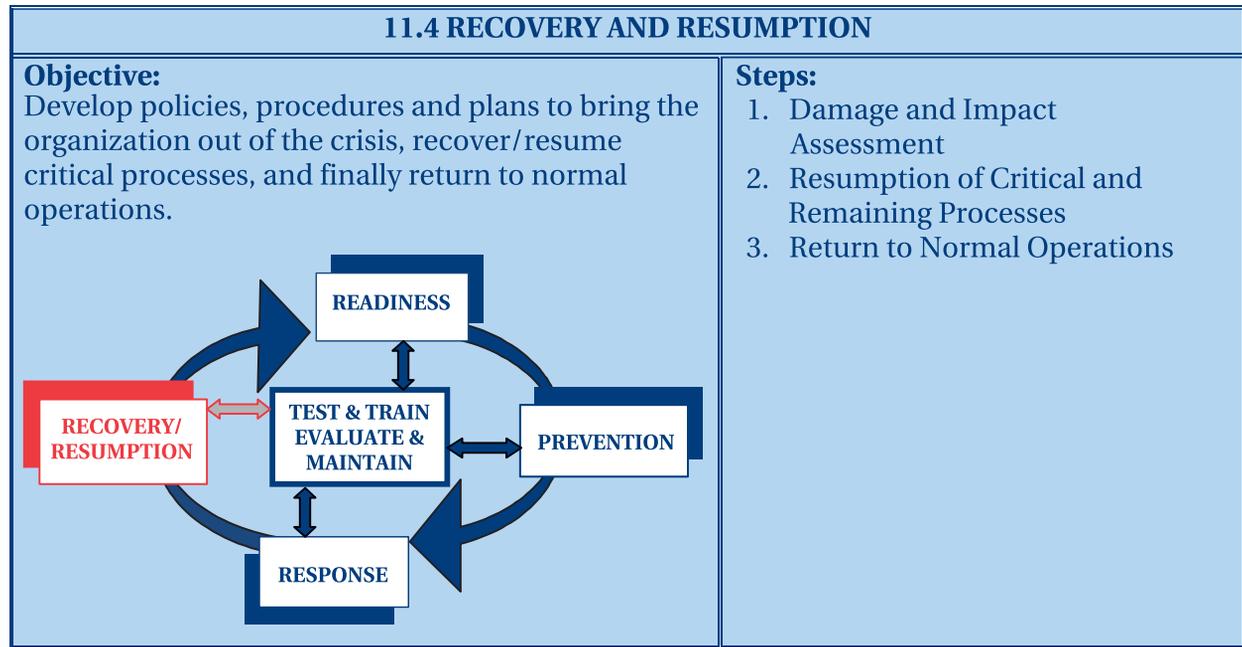
11.4.1 Damage and Impact Assessment

Once the Crisis Management Team has been activated, the damage should be assessed. The damage assessment may be performed by the Crisis Management Team itself or a designated Damage Assessment Team. Responsibility should be assigned for the documentation of all incident related facts and response actions, including financial expenditures.

11.4.1.a Crises Involving Physical Damage
For situations involving physical damage to company property, the Crisis Management Team or its designated Damage Assessment Team should be mobilized to the site. The Team will gain entry, if permission from the public safety authorities is granted, and make a preliminary assessment of the extent of damage and the likely length of time that the facility will be unusable.

11.4.1.b Crises Not Involving Physical Damage
Certain types of crises do not involve immediate physical damage to a company worksite or facility. These would include the business, human, information technology, and societal types of crises. In these crises, the Team will likely assess the damage or impact as the crisis unfolds.

11.4.2. Resumption of Critical and Remaining Processes

11.4.2.a Process Resumption Prioritization
Once the extent of damage is known, the process recovery needs should be prioritized and a schedule for resumption 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.

11.4.2.b Resumption of Critical Processes
Once the processes to be restored have been prioritized, the resumption work can begin with processes restored according to the prioritization schedule. The resumption of these processes may occur at either the current worksite or an alternate worksite, depending on the circumstances of the crisis. Documentation should be kept of when the processes were resumed.

11.4.2.c Resumption of Remaining Processes
Once the critical processes have been resumed, 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.

11.4.3. Return to Normal Operations

The organization should seek to bring the company ''back to normal.'' If it is not possible to return to the pre-crisis ''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.

12.0 PRACTICE ADVISORY – PART TWO

IMPLEMENTING AND MAINTAINING THE PLAN

This section of the Guideline contains those functions and tasks required for the Business Continuity Plan to remain a living document: one that grows and changes with the organization and remains relevant and actionable.

12.1 TESTING AND TRAINING	
Objective: Train and educate team members, as well as general employee population, and validate and enhance the BCP.	**Steps:** 1. Educate and Train 2. Test the BCP
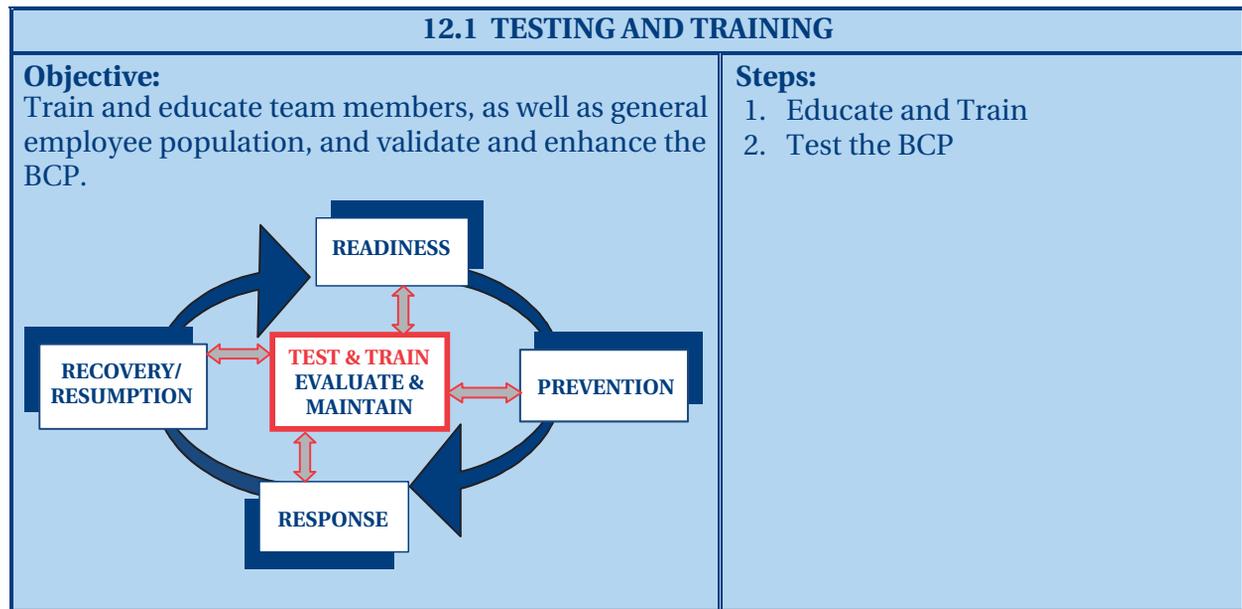
12.1.1 Educate and Train

The BCP is only as valuable as the knowledge that others have of it. Education and training are necessary components of the BCP process. They require a time commitment from the Crisis Management Team, the Response Teams, and the general employee population.

12.1.1.a Educate and Train Teams
The Crisis Management and Response Teams should be educated about their responsibilities and duties. Check lists of critical actions and information to be gathered are valuable tools in the education and response processes. Teams should be trained at least annually and new members should be trained when they join. These Teams should also be trained with respect to prevention of crises, as described in the next section.

12.1.1.b Educate and Train All Personnel
All personnel should be trained to perform their individual responsibilities in case of a crisis. They should also be briefed on the key components of the BCP, as well as the Response Plans that affect them directly. Such training could include procedures for evacuation, shelter-in-place, check-in processes to account for employees, arrangements at alternate worksites, and the handling of media inquiries by the company.

> It is recommended that any external resources that may be involved in a response – such as Fire, Police, Public Health, and third party vendors – should be familiar with relevant parts of the BCP.

12.1.2 Test the BCP

12.1.2.a Benefits of Testing
The benefits and necessity for testing, which involves training and exercises, cannot be overemphasized. Testing can keep Teams and employees effective in their duties, clarify their roles, and reveal weaknesses in the BCP that should be corrected. A commitment to testing lends credibility and authority to the BCP.

12.1.2.b Goals and Expectations
The first step in testing should be the setting of goals and expectations. An obvious goal is to determine whether a certain crisis response process works and how it can be improved. Other less obvious goals can be to test capacity (as in the case of a call-in or call-out phone system, for instance), to reduce the time necessary for accomplishment of a process (for example, using repeated drills to shorten response times), and to bring awareness and knowledge to the general employee population about the BCP.

Lessons learned from previous tests, as well as actual incidents experienced, should be built into the testing cycle for the BCP.

12.1.2.c Planning and Development
The responsibility for testing the BCP should be assigned. Larger organizations may consider establishing a Test Team. Where appropriate, the expertise of external resources (consultants, local emergency organizations, etc.) can be leveraged.

12.1.2.d Timeline
A test schedule and timeline as to how often the plan and its components will be tested should be established.

12.1.2.e Scope of Testing
The scope of testing should be planned to develop over time. In their infancy, tests should start out relatively simple, becoming increasingly complex as the test process evolves. Early tests could include checklists, simple exercises, and small components of the BCP. As the test schedules evolve, tests should become increasingly complex, up to a full-scale activation of the entire BCP, including external participation by public safety and emergency responders.

12.1.2.f Test Monitoring
When feasible, assign observers to take notes during the test. If possible, arrange to videotape and/or use audiotape devices for further appraisal at the conclusion of the exercise. If videotape and/or audiotape devices are not available, then a person should be assigned to document the chronological list of events during the testing.

12.1.2.g Test and Exercise Scenarios
Testing scenarios should be designed using the events identified in the Risk Assessment.

Type	Orientation (Introductory, Overview or Education Sessions)	Tabletop (Practical or Simulated Exercise)
Goal	Provides overview of plan to motivate and familiarize participants with team roles, responsibilities, expectations, and procedures. Useful when implementing new plan or adding new staff/leadership.	Presents limited simulation of a scenario (presented in narrative format) to evaluate plans, procedures, coordination, and assignment of resources. Addresses one issue at a time and allows breaks for discussion. Familiarizes participants with specific roles.
Benefits	Informal, easy to conduct and low stress.	Practices team building and problem solving.
Issues		Somewhat detailed with a medium stress level.
Needs	30 days planning cycle 1 hour duration.	2-3 months planning cycle, 2-4 hours duration and 30-60 minutes debriefing.

Type	Functional (Walk-Through or Specialized Exercise)	Full Scale (Live or real-life exercise)
Goal	Simulates a scenario as realistically as possible in a controlled environment (short of moving personnel, equipment, and resources to an actual site), requiring the actual performance of response functions. Tests communications, preparedness, and availability of resources.	Deploys personnel, equipment, and resources to a specific location for the real time, real-life simulation of a scenario. Incorporates as many BCP functions as possible to test the entire BCP.
Benefits	Decisions and actions occur in real time and generate real responses and consequences. Involves more participants, simulators, and evaluators such as local emergency services and media.	Evaluates operational capabilities in an interactive manner; facilitates communication and coordination across organization and public-private sector.
Issues	Typically detailed and high stress level.	Detailed, expensive and highly stressful.
Needs	3-4 months planning cycle, 4-6 hours duration plus 30-60 minutes debriefing.	6-8 months planning cycle, 6-8 hours duration plus 60-90 minutes debriefing.

12.1.2.h Test and Exercise Roles
There are several roles that test participants can fill. All participants should understand their roles in the exercise, and the exercise should involve all participants. As part of the exercise, participants should be allowed to interact and discuss issues and lessons.

Facilitator (Lead Controller)	Controller	Simulator
Possesses overall knowledge of the scenario. Supervises the exercise. Monitors sequence of events, adjusts pace, and controls timeline. Introduces action messages. Provides exercise oversight.	Introduces artificial stimuli at the direction of the facilitator. Acts as an extension of the facilitator. Makes decisions in the event of unanticipated actions or resource requirements. Helps eliminate safety and property damage issues by maintaining order as well as tracking and aiding actions of participants.	Adds realism to the scenario. Portrays private citizens, companies, agencies, and organizations as they would normally interact with participants. Acts as victim, adversary, media member, and any other extra role that needs to be filled. Uses groups such as local college students, community theater troupes, and volunteer organizations.
Observer Strategically positioned to observe and document performance. Should be knowledgeable about the subject matter or function being evaluated. Evaluates the actions of participants and the effectiveness of the BCP.	**Participants** Assume crisis roles and perform actual or simulated activities commensurate with the type of exercise and scenario being used.	

12.1.2.i Test and Exercise Participation
Various groups from the organization itself, as well as from the public sector, can participate in the tests:

Departments	Public Sector
Security and Safety Operations Facilities Human Resources Public Relations Medical Legal Finance Information Systems	Police, Fire, Emergency Medical Services Emergency Services and Disaster Agencies Hospitals Public Health Volunteer Organizations Hazardous Materials Response Teams

12.1.2.j Test and Exercise Evaluation

After completion, the test should be critically evaluated. The evaluation should include, among other things, an assessment of how well the goals and objectives of the test were achieved, the effectiveness of participation, and whether the BCP itself will function as anticipated in the case of a real crisis. Future testing, as well as the BCP itself, should then be modified as necessary based on the test results.

12.1.2.k Ongoing Development of Test Schedules

Design of tests should be evaluated and modified as necessary. They should be dynamic, taking into account changes to the BCP, personnel turnover, actual incidents, and results from previous exercises.

12.2 EVALUATION AND MAINTENANCE	
Objective: Keep the BCP relevant to the organization using a rigorous maintenance and evaluation program. 	**Steps:** 1. Develop BCP Review Schedule 2. Develop BCP Maintenance Schedule

12.2.1 Develop BCP Review Schedule

The BCP should be regularly reviewed and evaluated. Reviews should occur according to a pre-determined schedule, and documentation of the review should be maintained as necessary. The following factors can trigger a review and should otherwise be examined once a review is scheduled:

- **Risk Assessment:** The BCP should be reviewed every time a Risk Assessment is completed for the organization. The results of the Risk Assessment can be used to determine whether the BCP continues to adequately address the risks facing the organization.

- **Sector/Industry Trends:** Major sector/industry initiatives should initiate a BCP review. General trends in the sector/industry and in business continuity planning techniques can be used for benchmarking purposes.

- **Regulatory Requirements:** New regulatory requirements may require a review of the BCP.

- **Event Experience:** A review should be performed following a response to an event, whether the BCP was activated or not. If the plan was activated, the review should take into account the history of the plan itself, how it worked, why it was activated, etc. If the plan was not activated, the review should examine why and whether this was an appropriate decision.

- **Test/Exercise Results:** Based on test/exercise results, the BCP should be modified as necessary.

12.2.2 Develop BCP Maintenance Schedule

Regular maintenance of the BCP cannot be overemphasized. Clear responsibility for BCP maintenance should be assigned. Maintenance can be either planned or unplanned and should reflect changes in the operation of the organization that will affect the BCP. The following are examples of procedures, systems, or processes that may affect the plan:

- Systems and application software changes
- Changes to the organization and its business processes
- Personnel changes (employees and contractors)
- Supplier changes
- Critical lessons learned from testing
- Issues discovered during actual implementation of the plan in a crisis
- Changes to external environment (new businesses in area, new roads or changes to existing traffic patterns, etc.)
- Other items noted during review of the plan and identified during the Risk Assessment.

13.0 REFERENCES/BIBLIOGRAPHY

American Red Cross. *Preparing Your Business for the Unthinkable*. Washington, DC: American Red Cross, [no date available].
www.redcross.org

ASIS International. *ASIS Emergency Planning Handbook, Second edition*. Alexandria, VA: ASIS International, 2003.

ASIS International. *ASIS Disaster Preparation Guide*. Alexandria, VA: ASIS International, 2003.

ASIS International. *General Security Risk Assessment Guideline*. Alexandria, VA: ASIS International, 2003.

Baker Engineering & Energy. *Emergency Management Program Services: Business Continuity,* [Online]. Available: http://www.mbakercorp.com/emps/business_continuity.htm [2004]

''Business Continuity: Are you Prepared? Strategies, Products & Services for Today's World.'' *Fortune*, vol.144, no. 6 March 18, 2002, Special Advertising Section. s1-s6.

''Business Continuity: A Dearth of Shared Experiences.'' *Business Survival Newsletter* 6.1 (2002). [Online]. Available: www.Rothstein.com/nletter.shtml [2004].

Business Continuity Institute. [Website]. www.thebci.org [2004]

Business Operations Seismic Recovery Committee & the Human Resources Subcommittee. *Business Resumption Plan*. Berkeley, CA: University of California, Berkeley, 2001. Available: http://obr.berkeley.edu/pdfs/UCBBusinessResumptionPlanFinal12-31-01.pdf [2004].

Childs, Donna R. and Dietrich, Stefan. *Contingency Planning and Disaster Recovery: A Small Business Guide*. New York: John Wiley & Sons, 2002.

Continuity Insights.Com [Website]. www.continuityinsights.com [2004]

DavisLogic & All Hands Consulting. *Business Continuity Planning*. PowerPoint Presentation, [Online]. Available: www.allhandsconsulting.com [no date available].

DavisLogic, Inc. *Business Continuity Planning Basics*. (2002-2003). [Online]. Available: www.all-hands.net/pn/
modules.php?op=modload&name=Sections&file=index&req=viewarticle&artid=3 [2004].

Doughty, Ken, ed. Business Continuity Planning, Protecting Your Organization's Life. Boston: Auerbach Publications, 2000.

Downtown Dallas Emergency Response Resource Manual. (December 2002) [Online]. Available: http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/Top20/1%20—%20Management%20and%20Accountability/3A%20—%20Integrated%20System/Additional/Downtown_Dallas_Emergency_Response_Resource_Manual.pdf#page=35 [2004].

Disaster Recovery Institute International (DRII). *Glossary of Terms.* (no date available). [Online]. Available: http://www.drii.org/displaycommon.cfm?an=3 [2004].

Disaster Recovery Institute International (DRII). *Professional Practices for Business Continuity Professionals.* (2004). [Online]. Available: http://www.drii.org/displaycommon.cfm?an=2 [2004].

Disaster Recovery Institute International (DRII). *Seven Step Business Continuity Planning Model.* (2003) [Online]. Available: http://www.drii.org/associations/1311/files/planningmodel.pdf [2004].

Disaster Recovery Journal. *DRJ's Sample DR Plans and Outlines.* (no date available). [Online]. Available: www.drj.com/new2dr/samples.htm

Disaster Recovery Planning Group. [Website]. www.disaster-recovery-plan.com

Deloitte & Touche. Disaster Recovery and Business Continuity Planning. PowerPoint Presentation. Presented by Kelly Jane Wilson, Office of Firm Security [no date available].

EMC White Paper. *Business Continuity and Ethics: Minimizing Future Risks.* EMC Corp. July, 2003.

The Emergency Email & Wireless Network® [Website]. www.emergencyemail.org

Emergency Management Guide for Business & Industry: A Step-By-Step Approach to Emergency Planning, Response and Recovery for Companies of All Sizes. (2002). Sponsored by a Public-Private Partnership with the Federal Emergency Management Agency (FEMA). [Online]. Available: http://www.fema.gov/pdf/library/bizindst.pdf [2004].

Expecting the Unexpected: Business Continuity in an Uncertain World. London, UK: London First, 2003. [Online]. Available: www.thebci.org/London%20Firsts.pdf [2004].

Federal Emergency Management Agency (FEMA). *Are You Ready? A Guide to Citizen Preparedness.* FEMA Publication H-34. Washington, DC: Federal Emergency Management Agency, revised September 2002. www.fema.gov/areyouready/

Federal Emergency Management Agency (FEMA). *State and Local Guide (SLG) 101: Guide for All-Hazard Emergency Operations Planning.* Washington, DC: Federal Emergency Management Agency, September, 1996

Federal Emergency Management Agency (FEMA). *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings.* FEMA 426; Risk Management Series.

Washington, DC: Federal Emergency Management Agency, December 2003. www.fema.gov/library/prepandprev.shtm

Federal Emergency Management Agency (FEMA). *Standard Checklist Criteria for Business Recovery*. Washington, DC: Federal Emergency Management Agency, February 2003. www.fema.gov/ofm/bc.shtm

Griffith, Carl and Vulpitta, Rick. *Effective Emergency Response Plans: Anticipate the Worst, Prepare for the Best Results*. Itasca, IL: National Safety Council, 2001. [Online]. Available: http://www.nsc.org/issues/emerg/99esc.htm [2004].

Homeland Security State Contact List [Website] www.whitehouse.gov/homeland/contactmap.htm

Jolly, Adam, consultant ed. *Managing Business Risk: A Practical Guide to Protecting Your Business*. London, UK: Kogan Page Ltd., 2003.

Knox, Donald E. *Crisis Management: Exercising Plans Using Scenario Based Training*. Powerpoint presentation. ASIS International Annual Seminar and Exhibits, 2002, 2003; ASIS International Emerging Trends In Security Technology and Practice, 2003; ASIS Crisis Management Council Workshop, 2002, 2003; ASIS International Central Illinois Chapter Seminar, 2002, 2003; ASIS International Greater Milwaukee Chapter Seminar, 2003; Association of Threat Assessment Professionals (ATAP) Annual Threat Management Conference, 2004.

Los Angeles City Fire Department. *The Earthquake Preparedness Handbook*, (1997). [Online]. Available: www.lafd.org/eqindex.htm#menutop [2004].

Massachusetts Institute of Technology (MIT). *MIT Business Continuity Plan*. Boston, MA: Massachusetts Institute of Technology, 1995. [Online]. Available: http://web.mit.edu/security/www/pubplan.htm [2004].

Michigan Department of State Police, Emergency Management Division (EMD). *Local Emergency Management Standards*. EMD Pub 206, (November 1998). [Online]. Available: http://www.michigan.gov/msp/0,1607,7-123-1593_3507-25233—,00.html [2004].

Michigan Department of State Police, Emergency Management Division (EMD). *Guidance for Community Hazmat Response Plans*. EMD Pub 308,(July 2003). [Online]. Available: http://www.michigan.gov/documents/msp-pub308haz_plans_8748_7.pdf [2004].

Michigan Department of State Police, Emergency Management Division (EMD). *Site Emergency Planning Workbook*. EMD Pub 602, (April 2000). [Online]. Available: http://www.michigan.gov/documents/msp-pub602_site_planning_8707_7.pdf [2004]. EMD Pub 308, July 2000.

Michigan Department of State Police, Emergency Management Division (EMD).

Emergency Information Procedures Workbook, A Workbook for Developing Emergency Public Information Standard Operations Procedures. EMD Pub 401, (June 2001). [Online]. Available: http://www.michigan.gov/documents/msp-pub401_pio_workbook_8733_7.pdf [2004].

Michigan Department of State Police, Emergency Management Division (EMD). *Disaster Exercise Manual: Guidelines for Exercising Emergency Operations Plans for Local Government.* EMD Pub 702, (January 2004). [Online]. Available: http://www.michigan.gov/documents/pub702-Disaster_Exercise_Manual1-14-04_83182_7.pdf [2004].

Michigan Department of State Police, Emergency Management Division (EMD). *Local Hazard Mitigation Planning Workbook,* EMD Pub 207, revised February 2003. [Online]. Available: http://www.michigan.gov/msp/0,1607,7-123-1593_3507-14743—,00.html [2004].

Michigan Hazardous Materials Training Center, *Hazardous Materials Operations-Level Training for the First Responder, Second Edition.* Lansing, MI: Michigan Hazardous Materials Training Center, 2000. www.hazmatems.com

Michigan Hazardous Materials Training Center, *First Responder Awareness Training for Hazardous Materials.* Lansing, MI: Michigan Hazardous Materials Training Center, 1997. www.hazmatems.com

National Fire Protection Association. *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs.* Quincy, MA: National Fire Protection Association, 2004.

National Incident Management System Coordination Draft, Working Draft v7.1, December 3, 2003.

National Organization on Disability. *Emergency Preparedness Initiative: Guide on the Special Needs of People with Disabilities for Emergency Managers, Planners, & Responders.* Washington, DC: National Organization on Disability, 2002. [Online]. Available: http://www.nod.org/pdffiles/epiguide2004.pdf [2004]

Reference List for Business Resumption Planning. (no date available). [Online]. Available: www.occ.cccd.edu/~pcmgrs/BRP.html [2004].

Sikich, Geary W. *Integrated Business Continuity, Maintaining Resilience in Uncertain Times.* 2003.

Strohl Systems. [Website]. www.strohlsystems.com

U. S. Department of Justice. Office of Justice Programs. *Crisis Information Management Software (CIMS) Feature Comparison Report.* National Institute of Justice Special Report. NCJ 197065. Washington, DC, 2002. www.ojp.usdoj.govv www.ojp.usdoj.gov/nij

U.S. Department of Labor. Occupational Safety and Health Administration. *Emergency Preparedness and Response.* (no date available). [Online]. Available: http://www.osha.gov/ SLTC/smallbusiness/sec10.html [2004].

U.S. Department of Labor. Occupational Safety and Health Administration. *Evacuation Plans and Procedures: eTool.* (no date available). [Online]. Available: http://www.osha.gov/ SLTC/etools/evacuation/ [2004].

14.0 APPENDIX A

ASIS Business Continuity Guideline Checklist

	Considerations	Y/N	Notes
	DEVELOPING THE PLAN Overview		
1	If a major disaster occurred today, has your organization planned for survival?		
2	Does your organization have a Business Continuity Plan (BCP), and is it up to date?		
3	Has senior management approved the BCP?		
4	Does senior management support the BCP?		
5	Has the cost of the BCP been determined, including development and maintenance?		
6	Have the initial audit, security, and insurance departments reviewed the BCP?		
7	Has the BCP been tested, including a surprise test?		
	DEVELOPING THE PLAN Accountability		
1	Does your organization's policy include a definition of crisis?		
2	Has the person responsible for critical systems and business processes been identified?		
3	Has a BCP Team been appointed, and does it include senior business function leaders?		
4	Has the BCP been communicated throughout the organization?		
5	Has a person been assigned with the responsibility to update the BCP?		
	DEVELOPING THE PLAN Risk Assessment		
1	Has your organization conducted a Risk Assessment? (See ASIS International's General Security Risk Assessment Guideline at www.asisonline.org/guidelines/guidelines.htm)		
2	Have the types of risks that may impact your organization been identified and analyzed?		
3	Has the likelihood for each type of risk been rated?		

	DEVELOPING THE PLAN Business Impact Analysis		
1	Have the critical business processes been identified?		
2	Have the business processes been ranked (low, medium, high)?		
3	If a crisis were to happen, has the impact, in terms of human and financial costs, been assessed?		
4	Have the maximum allowable outage and recovery time objectives been determined?		
5	Has the length of time your organization's business processes could be non-functional been determined?		
6	Have the recovery time objectives been identified?		
7	Have the resources required for resumption and recovery been identified?		
	DEVELOPING THE PLAN Strategic Plans		
1	Have methods to mitigate the risks identified in the Business Impact Analysis and Risk Assessment been identified?		
2	Have plans and procedures to respond to any incident been developed?		
3	Have strategies that address short and long term business interruptions been selected?		
4	Are the strategies attainable, tested, and cost effective?		
	DEVELOPING THE PLAN Crisis Management and Response Team Development		
1	Is the Crisis Management Team comprised of members from human resources?		
2	Have Response Teams to support the Crisis Management Team been organized?		
3	Have response plans to address the various aspects of the crisis been developed and incorporated into the organization's overall BCP?		
4	Do the response plans address damage assessment, site restoration, payroll, human resources, information technology, and administrative support?		
5	Has contact information been included in the plan for the Crisis Management and the Response Teams?		

	PREVENTION Compliance w/Corporate Policy & Mitigation Strategies		
1	Have compliance audits been conducted to enforce BCP policy and procedures?		
2	Have the systems and resources that will contribute to the mitigation process been identified, including personnel, facilities, technology, and equipment?		
3	Have the systems and resources been monitored to ensure they will be available when needed?		
	PREVENTION Avoidance, Deterrence, and Detection		
1	Are employees motivated to be responsible for avoidance and deterrence and detection?		
2	Have facility security programs to support avoidance and deterrence and detection been established?		
3	Have operational policy and procedures to protect the facilities been developed?		
4	Is it ensured that sufficient physical security systems and planning are in place to protect the facility?		
	RESPONSE Potential Crisis Recognition and Team Notification		
1	Will the response program recognize when a crisis occurs and provide some level of response?		
2	Have the danger signals been identified that indicate a crisis is imminent?		
3	Have personnel been trained to observe warning signs of an imminent crisis?		
4	Has a notification system been put in place, including redundant systems?		
5	Is the notification contact list complete and up to date?		
	RESPONSE Assess the Situation		
1	Has an assessment process to address the severity and impact of the crisis been developed?		
2	Has the responsibility for declaring a crisis, with first and second alternates, been assigned?		

		RESPONSE Declare a Crisis		
1		Have the criteria been established for when a crisis should be declared?		
2		Has the responsibility for declaring a crisis been clearly defined and assigned?		
3		Has an alert network for BCP Team members and employees been established?		
4		Is it ensured that there is an alternate means of warning if the alert network fails?		
5		Have the activities that will be implemented in event of a crisis been identified, including notification, evacuation, relocation, alternate site activation, team deployment, operational changes, etc?		
		RESPONSE Execute the Plan		
1		Has consideration been given to developing the BCP around a "worst case scenario?"		
2		Has the BCP been prioritized to save lives, protect assets, restore critical business processes and systems, reduce the length of the interruption, protect reputation, control media coverage, and maintain customer relations?		
3		Have the severity of the crisis and the appropriate response been determined?		
		RESPONSE Communications		
1		Has a crisis communications strategy been developed?		
2		Are communications timely, honest, and objective?		
3		Are communications with all employees occurring at approximately the same time?		
4		Are regular updates provided, including notification of when the next update will be issued?		
5		Has a primary spokesperson and back-up spokespersons been designated who will manage and disseminate crisis communications to the media and others?		

	RESPONSE Resource Management – Human Element		
1	Has a system been devised by which all personnel can be accounted for quickly?		
2	Is there a system to ensure current and accurate contact information is maintained?		
3	Have arrangements been made for next-of-kin notifications?		
4	Can crisis counseling be arranged as necessary?		
5	Will the financial systems for payroll and support of facilities and employees remain functional?		
	RESPONSE Resource Management—Logistics		
1	Has a designated Crisis Management Center been identified, and does it have necessary life support functions, including uninterruptible power supply and communications equipment?		
2	Have alternate worksites for business resumption and recovery been identified?		
3	Have critical and vital records been stored at an offsite storage facility?		
4	How long can each business function operate effectively without normal data input storage processes?		
5	What must be done to restore data to the same previous point in time within the recovery time objective?		
6	Can any alternate data storage processes be used, after the initial data recovery, to speed the forward recovery to the present time?		
	RESPONSE Resource Management – Financial Issues and Insurance, Transportation, Suppliers/Service Providers, and Mutual Aid		
1	Has the appropriate insurance coverage been identified and obtained?		
2	Are cash and credit available to the BCP Team?		
3	Have transportation alternatives been arranged in advance?		
4	Have critical vendor and service provider agreements been established?		

5	Have mutual aid agreements been established?		
6	If so, are they legally sound, properly documented, and understood by all parties?		
	RECOVERY AND RESUMPTION Damage and Impact Assessment, Process Resumption, and Return to Normal Operations		
1	Has a damage assessment been performed as soon as possible?		
2	Has the Damage Assessment Team been mobilized to the site?		
3	Has business process recovery been prioritized to recover the most critical business processes first?		
4	Is the schedule of the processes to be restored in accordance with the prioritization schedule?		
5	Is there documentation of when the processes were resumed?		
6	Has the organization returned to normal operations?		
7	Has the decision to return to normal operations been documented and communicated?		
	IMPLEMENTING AND MAINTAINING THE PLAN Education and Training		
1	Are the Crisis Management and Response Teams educated about their responsibilities and duties?		
2	Has a checklist of critical actions and responsibilities and duties been developed?		
3	Do Teams receive annual training?		
	IMPLEMENTING AND MAINTAINING THE PLAN Testing		
1	Are the Business Continuity Plan and appropriate Teams tested to reveal any weaknesses that require correction?		
2	Have goals and expectations of testing and drills been established?		
3	Are drills and tabletop exercises conducted on an annual basis?		
4	Has responsibility for testing the BCP been assigned with consideration for establishing a test team?		

5	Does test participation include various groups from the organization and the public sector?		
6	Have observers been assigned who will take notes during the test and critique the test at the conclusion of the exercise?		
7	Have tests and drills been evaluated, including assessing how well the goals and objectives of the tests and drills were met?		
	IMPLEMENTING AND MAINTAINING THE PLAN BCP Review and Maintenance Schedules		
1	Is the BCP regularly reviewed and evaluated on a pre-determined schedule?		
2	Is the BCP reviewed every time a Risk Assessment is completed for the organization?		
3	Is the BCP modified as needed based on test/exercise results?		
4	Has responsibility for on-going BCP maintenance been assigned?		
5	Does BCP maintenance reflect changes in the operation of the organization?		

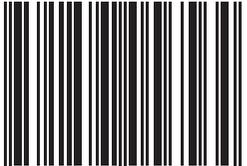**ASIS**
INTERNATIONAL
Advancing Security Worldwide™

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 33,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine — *Security Management* — ASIS leads the way for advanced and improved security performance.

ASIS
INTERNATIONAL
Advancing Security Worldwide™

1625 Prince Street
Alexandria, VA 22314-2818 USA
703-519-6200
Fax: 703-519-6299
www.asisonline.org