

Business Continuity

G U I D E L I N E

**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)

Copyright ASIS International
Provided by IHS
No reproduction or networking permitted without license from IHS



Documents
Document Sharing Hub



BUSINESS CONTINUITY GUIDELINE:

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

ASIS GDL BC 01 2005

Copyright © 2005 by ASIS International

ISBN 1-887056-56-4

ASIS International (ASIS) disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. In issuing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is ASIS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstance.

All rights reserved. Permission is hereby granted to individual users to download this document for their own personal use, with acknowledgment of ASIS International as the source. However, this document may not be downloaded for further copying or reproduction nor may it be sold, offered for sale, or otherwise used commercially.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1



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

1.0	Title	5
2.0	Revision History	5
3.0	Commission Members	5
4.0	Committee Members	5
5.0	Guidelines Designation	6
6.0	Scope	6
7.0	Summary	6
8.0	Purpose	6
9.0	Key Words	7
10.0	Terminology	7
11.0	Practice Advisory – Part One	10
11.1	Readiness	10
11.2	Prevention	15
11.3	Response	17
11.4	Recovery/Resumption	24
12.0	Practice Advisory – Part Two	26
12.1	Testing & Training	26
12.2	Evaluation & Maintenance	31
13.0	References/Bibliography	33
14.0	Appendix A – BC Guideline Checklist	38

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.

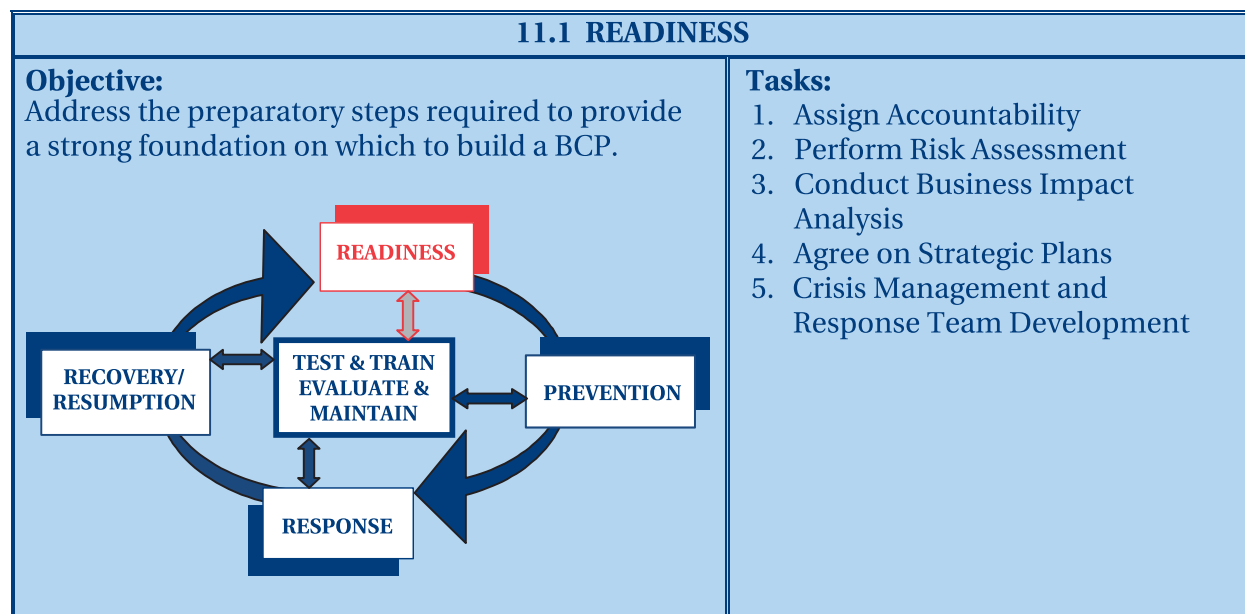
11.0 PRACTICE ADVISORY—PART ONE

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.



11.1.1 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