The SEMI Business Continuity Guideline for the Semiconductor Industry and its Supply Chain

Preface

The SEMI Business Continuity Council endorsed publication of this document as a guideline, independent of any standards on March 13, 2003. The SEMI Business Continuity Council, comprised of participants from the semiconductor device and equipment companies from the semiconductor device manufacturers, material and equipment suppliers, and consultants to the industry, has furnished the information in this document.

SEMI is publishing this document, as furnished by the Council, so that it may be referenced by the industry, as desired. **No material in this document is to be construed as an official or adopted standard.** SEMI assumes no liability for the content neither of this document, nor for any errors or inaccuracies that may appear in this document.

NOTICE: By publication of this document, SEMI takes no position respecting the validity of any patent rights or copyrights asserted in connection with any item mentioned herein. Users of this document are expressly advised that determinations of any such patent rights or copyrights, and the risk of infringement of such rights, are entirely their own responsibility.

©2003 Semiconductor Equipment and Materials International (SEMI). All rights reserved. SEMI is a registered trademark of Semiconductor Equipment and Materials International.

Document developed and edited by: Sue Howell, SEMI North America.

Acknowledgments

SEMI is grateful to the following individuals and companies for their contributions of both time and content in the development of the guideline.

Tracy Best, SK Daifuku; Giles Bumpas, STMicroelectronics, Inc.; Brett Davis, Motorola; Bob Denny, Lam Research; Indra Desai, Lam Research; Urmil Desai, Intel; Kathryn Dornfeld, Intel; Gary Euscher, AMD; Dan Lowdermilk, AMD; Sandy Mendia, Applied Materials; Xochitl Monteon, EORM; Todd Patriacca, MKS Instruments; Larry Pennington, AQS; Raul Perez, Novellus Systems; Dick Thielen, AMD.
The threat of business interruption to companies within the semiconductor industry has grown in recent years. As the complexity of devices increases, so does the universe of manufacturing, distribution, use and disposal. The opportunities for product and business issues to arise increase accordingly. Changes in technologies and materials create new dependencies. Venturing into uncharted business environments brings new risks, along with opportunities. Evolving governmental regulation and special interest agendas impose change that must be adapted to and incorporated quickly, often creating a significant burden. Today, civil unrest and disruptive political agendas are a global phenomenon. Communication dependencies have multiplied and industrial, environmental, health, safety, and human resource issues cannot be dismissed.

To overcome these and other threats to conducting business within the semiconductor industry, significant effort must be put forth to identify and prepare for issues, events or crises which could adversely affect business continuity (BC). Identifying, analyzing and quantifying risks in a systematic manner will lead to efficient and cost effective risk management. Methods to mitigate risks may be employed at all phases of an event, issue, or crisis as appropriate.

Analyzing the risks to business operations is fundamental to maintaining business continuity. As an industry we have become practiced in the identification and control of those risks inherent in our manufacturing materials and processes. Emergency response planning and preparation is often focused on controlling the failure or event and limiting the immediate consequences. Failures can be exasperated by an inappropriate response or a host of other possibilities. The level to which the consequences of extended failures are explored and mitigation comprehended and provided for, will determine a company’s likelihood to survive crises and maintain business continuity.

Business Continuity Management (BCM) requires a multidisciplinary approach. Numerous skill sets are needed to comprehend the failure potentials, appreciate the interdependencies and evaluate the consequences of failure and events - internally and externally. Strategic and operational involvement is imperative to effectively plan to avert risks and avoid business interruption. As the business environment is rarely static, a mechanism to track change, assess impact and modify planning is necessary to ensure that response to failures or events are appropriate and timely. Software tools are available that can aid this process.

The function of BCM is to safeguard your business by ensuring the continuity of a reasonable level of service for critical business functions and achieving a smooth return to normal operations when the crisis is over. Comprehensive BCM requires that roles and responsibilities are clearly defined, agreed upon and documented. The business continuity plan must contain clearly-defined instructions, advice, guidance and the processes to invoke during a BCM event.

This document explores the elements of comprehensive business continuity management. Template examples are included that may be used by businesses of various size and complexity to develop or refine their risk management programs to comprehend and address the threat of business interruption.
These guidelines and templates do not of themselves provide a BCM competency and capability; they do provide a framework that may be adopted by all in the industry.
# Table of Contents

1 Purpose ................................................................. 5

2 Scope ........................................................................ 5

3 Definitions ............................................................. 5

4 Referenced Documents .............................................. 7

5 Resources .................................................................... 7

6 Business Continuity Management Elements .................. 7
   6.1 Business Impact Analysis .....................................
   6.2 Business Continuity ............................................
   6.3 Disaster (Emergency) Recovery ............................
   6.4 Business Recovery .............................................
   6.5 Supply Chain ....................................................
   6.5 Site Readiness ..................................................

7 BCM Template .......................................................... 18
   • Business Impact Analysis Questionnaire .................... 19
   • Critical Incident Team Model .................................. 27
   • Risk Analysis and Disaster Mitigation Worksheet ....... 32
   • Disaster Recovery Plan ......................................... 40
   • Emergency Response Plan Checklist - sample .......... 43
   • Business Recovery Plan ....................................... 48
   • Drill Template - Design and testing ....................... 55
   • Drill Template – Execution .................................... 58
1 Purpose

This document is intended to advance the understanding of the threats to business continuity facing companies in the semiconductor industry and to identify methods and practices which can be employed to mitigate those threats - i.e. to manage for business continuity.

2 Scope

Business Continuity Management (BCM) is an ongoing process designed to prevent, mitigate, prepare for, respond to and recover from, disruptive failures or events that threaten a business. All business entities function uniquely in support of a company’s business plan. The role each company plays must be assessed in respect to the consequences of its incapacitation. The extent of incapacitation that can be tolerated is company dependent. This document serves as a guideline for the development or refinement of a management system to effectively address the risks of business interruption. It is intended that companies large and small with discrete or diverse products or facilities may benefit through use of the management methods presented within.

These guidelines present the BCM process in elements:

1. Business Impact Analysis
2. Business Continuity
3. Disaster (Emergency) Recovery
4. Business Recovery
5. Supply Chain
6. Site Readiness

Having an effective BCM process means that you:

- understand your core business including present and future economic conditions;
- utilize a business impact analysis to identify risks;
- develop a business continuity strategy, analyzing, prioritizing and tracking mitigation items;
- initiate BCM planning, developing emergency responses and business recovery plans;
- understand your supply chain and understand potential vulnerabilities (i.e. single source suppliers);
- embed business continuity into your organization’s culture so that BC is sustained;
- test your plans and self assess your programs and their impact.

3 Definitions

**Business Continuity Management (BCM):** a proactive management process designed to reduce the impact from disruptive failures or events so that the business can respond to a crisis and continue/resume critical business functions until full, normal operations can be restored.

**Business Disaster:** any natural, technological or human event that results in significant damage or impairment of business.

**Business Impact Analysis (BIA):** the process of analyzing critical business functions and the effects that a disaster or crisis may have upon them.

**Business Recovery Plan (BRP):** a document of the specific planned response to keep the business operational while dealing with the crisis or failure event until normal business operations can be resumed. Within a BRP there could be multiple plans within a business group, each one with increasing detail as each business unit defines their recovery strategies for the same key processes. In some business groups, the overall BRP may incorporate specific sub-plans such as application business continuity plans.

**Controls:** measures designed to reduce or deter threats.

**Crisis:** a situation or period in which things are very uncertain, difficult, or painful - especially a time when action must be taken to avoid complete disaster or breakdown.

**Critical Point of Failure (CPOF):** any critical or single point in your business functions or processes that, if it fails, has the capability of causing significant impact and/or disruption.

**Disaster Mitigation (aka Risk Mitigation):** actions and activities to eliminate, control, or reduce the degree of impact.

**Emergency/Disaster Recovery Plan (ERP/DRP):** an approved set of arrangements and procedures that enables an organization to respond to a disaster and resume its critical business functions within a defined timeframe.

**Event:** an incident that threatens to interrupt normal business operations.

**Impact:** the consequences of an event.

**Incident:** an event with potentially serious consequences; an event that may result in a crisis.

**Risk:** the expected losses from a failure or event, expressed in terms of severity (loss) and likelihood (probability).

**Threat:** an event that may cause a risk.
Trigger: a situation, action, series of events, or process that is predefined as a stimulus or grounds for invoking BCM plans or activities.

4 Referenced Documents

4.2 SEMI S10-1296 Safety Guideline for Risk Assessment

5 Resources

Capability Assessment for Readiness (CAR) - http://www.fema.gov/rrr/car.shtm
Disaster Resources – http://www.disaster-resource.com

6 Business Continuity Management Elements

1.0 Business Impact Analysis
   1.1 Risk assessment
   1.2 Disaster mitigation analysis
   1.3 Mitigation hierarchy (priorities, ROI)

2.0 Business Continuity
   2.1 Management succession and the identification of key staff
   2.2 Emergency funding and purchasing
   2.3 Off-site storage of vital records
   2.4 Strategy for replacing specialized equipment
   2.5 Strategy for assuring the availability of key staff
   2.6 Logistics for notifying key staff and transporting to an alternate work site
   2.7 Personnel policy – human resource management

3.0 Disaster (Emergency) Recovery
   3.1 Emergency response and preliminary damage assessment
      • ensuring the safety of personnel
      • securing the environment
      • performing preliminary damage assessments
   3.2 Responsibility and process for disaster declaration
      • crisis management team
      • crisis communications
   3.3 Detailed damage assessment
4.0 Business Recovery

4.1 Restoration of minimum acceptable services
4.2 Recovery of critical business functions and ongoing operations
4.3 Primary site salvage, repair and reconstruction
4.4 Management of finances and insurance claims
4.5 Communications with key stakeholders (employees, media, shareholders, regulators, and other interested constituencies)

5.0 Supply Chain

5.1 Planning for an uninterrupted supply chain
5.2 Evaluation of the organization’s bill of materials to identify risks of supply disruption
5.3 Identification of qualified alternative suppliers that are not dependent on the same source of supply chain materials
5.4 Single source materials and/or suppliers
5.5 Consideration of continuity of materials as part of new product development plans

6.0 Site Readiness

6.1 Establish site ownership
6.2 Performance of annual drills and inspections

1.1 Risk assessment

1.1.1 Each department and operation is evaluated to identify dependencies, both internal and external
1.1.1.1 The impact from a disaster or crisis may have both tangible and intangible effects. Types of impact include:
   - people – loss of life, stranded employees, quarantine
   - financial - increased cost of working, fines and penalties, missed revenue opportunities, profit erosion, loss of market segment share
   - computing – application loss, IT infrastructure loss, security breech
   - physical – buildings, access, roadways
   - logistic – suppliers, movement of goods, access to key services
   - customer confidence - product liability, issue management
   - legal – exposure to liability
   - reputation – image, brand name
1.1.2 The network of dependencies between entities have been recorded
1.1.3 Recovery time objectives are specified for all functions and operations
1.1.4 Minimum service levels have been determined
1.1.5 Determine risk
   - expected losses X likelihood of occurrence (local or immediate) + projected impact to company’s ability to provide goods and services to customer (reduction X time)
1.1.6 Gauge risks
1.1.7 Determine risk tolerance level
1.2 **Disaster mitigation analysis**
1.2.1 Identify means to mitigate risks to tolerance level
1.2.2 Determine resources required

1.3 **Mitigation hierarchy (priorities, ROI)**
1.3.1 Match risk hierarchy with resources
1.3.2 Develop strategy to mitigate all risks to tolerable level
1.3.3 Allocate resources to achieve and maintain tolerable risk levels

2.1 **Management succession and identification of key staff**
2.1.1 Key staff (by function) have been identified, documented, reviewed, and regularly updated for all business locations. These functions and associated key staff, if disabled, would affect the normal day-to-day business operations.
2.1.2 The plan clearly identifies key members of staff (skills, knowledge, IP, organizational role and experience) to ensure business continuity management
2.1.3 The plan provides for the non-availability of key personnel. In other words, you have designated back-ups and alternates who are familiar with the role and associated responsibilities
2.1.3.1 In addition, a succession plan has been developed, documented, reviewed, and regularly updated to establish the successors of key staff who may be disabled as defined above
2.1.4 Key individuals have appropriate sign-off authority for approving emergency purchases and capital purchases
2.1.5 Chain of command is established with key contact information identified and documented
2.1.6 All key functions have been identified. Primary and secondary process owners are identified and trained
2.1.7 Employee contact data is updated regularly
2.1.8 All key individuals have been identified and at least one individual per critical function is trained as back-up

2.2 **Emergency funding and purchasing**
2.2.1 There is an established and documented means for emergency purchasing, sign-off and expediting procedures
2.2.2 There is an established and documented means for capital purchasing, sign-off and expediting procedures
2.2.3 Strategies have been identified to ensure you have access to “cash” during times of a crisis for unanticipated emergency supplies. (Credit card purchases, banks and automated tellers may not be available).

2.3 **Off-site storage of vital records**
2.3.1 Records vital to the day-to-day operations of all business locations have been identified, documented, and listings are regularly reviewed and updated by management
2.3.2 Determination of acceptable off-site storage site(s) have been made and documented
2.3.3 Determination of back-up storage site(s) have been made and documented and regularly reviewed and updated
2.3.4 Frequency of delivery of vital records to off-site storage have been determined, documented, reviewed, and updated regularly by management
2.3.5 Frequency of inspection/audit of off-site storage site(s) has been determined, documented, reviewed, and updated regularly by management
2.3.6 Actions resulting from inspection/audit of off-site storage site(s) are documented, reviewed and updated. Disqualification strategy is defined and documented when necessary
2.3.7 Security requirements of the off-site storage site have been determined, documented, reviewed and updated regularly by management
2.3.8 Access privilege to off-site storage site is determined, documented, reviewed, and is updated regularly by management
2.3.9 The business continuity plan is stored in a location that is immediately accessible in case of disaster or business interruption
2.3.9.1 Key individuals involved with the response have easy access to this documentation during a crisis

2.4 Strategy for replacing specialized equipment
2.4.1 There is a company-wide strategy in place to identify specialized equipment, to determine critical need, and effectively manage loss or impact due to loss
2.4.2 Specialized equipment responsibility and equipment ownership is identified
2.4.3 Replacement strategies have been developed for all specialized equipment identified in the corporate impact analysis
2.4.4 Functional work-arounds or temporary operations have been identified and documented for specialized equipment based on criticality and impact to the function or organization
2.4.5 Backup sources for specialized equipment functionality have been identified and procedures are in place to obtain or transfer services
2.4.6 Plans exist to secure all required reference materials and operating procedures
2.4.7 Cross training exists for all specialized equipment
2.4.8 Critical spares have been identified and strategies developed to ensure they are available when needed during a crisis

2.5 Strategy for assuring availability of key staff
2.5.1 An organization-wide plan is in place which identifies key staff, responsibilities and includes back-up, alternatives and cross-trained personnel
2.5.2 Key staff have been identified for all business and mission-critical functions
2.5.3 Organizational chain of command is identified, documented, and communicated
2.5.4 Responsibilities have been clearly documented and staff have been trained
2.5.5 HR and business policies have been established which provide key staff and alternative crisis coverage
2.5.6 Processes are in place to regularly review staff assignments and availability
2.5.7 Cross-training plans and training programs are in place to permit uninterrupted key staff requirements in crisis situations
2.5.8 A company-wide critical response communications methodology is in place which comprehends the chain of command and key staff structure requirements.

2.6 Logistics for notifying key staff and transporting to an alternate site
2.6.1 An organization-wide plan is in place, which identifies alternative sites for critical functions and the process of staff notification and transportation.
2.6.2 Alternative sites have been identified to include all mission critical operations as defined in the business impact analysis.
2.6.3 Alternative sites have been tested to ensure the availability of adequate functionality and resources to sustain designated operations.
2.6.4 Communications procedures and a contact structure have been established for employees and alternative sites.
2.6.5 All key staff have been identified and trained in the process and relocation requirements.
2.6.6 Responsibilities have been clearly documented and staff have been trained.
2.6.7 Employee data required to take action is maintained and reflects current contact information to include:
   • the ability to contact key staff at any time;
   • off hours contact information to include data that have a geographical impact; and might impede the individual(s) from coming to the work site and/or communicating with work;
   • transportation methods and alternatives have been established and tested for all key staff.

2.7 Personnel policy – human resource management
2.7.1 An organization-wide human resource management plan is in place.
2.7.2 A contingency plan is in place and the workforce is trained.
2.7.3 Responsibilities for contingency management are defined with designated owners identified.
2.7.4 Employee screening processes and background checks are in place to ensure reliability of newly-hired personnel.
2.7.5 A system is in place to maintain critical HR management information system data, including employee data, company information and necessary forms.
2.7.6 Employees with obligations to organizations such as the National Guard, medical/rescue squads and other emergency service organizations are identified. Redundancy plans are in place for these individuals.
2.7.7 Cross-training plans and training programs are in place to enable an employee to accomplish another person’s duties in a crisis situation.
2.7.8 Key functions have been identified – designated personnel and alternates are identified to staff these positions.
2.7.9 A company-wide communications plan and methodology to communicate with and account for personnel during crisis and after emergency situations have been developed. (i.e. company hotline or 800#)
2.7.9.1 All employees know where to report and/or call during a crisis.

3.1 Emergency response and preliminary damage assessment
3.1.1 The plan addresses emergency disaster and includes the following assumptions:
- an emergency action plan is in place
- the emergency response plan for Emergency Response Team (ERT) leader and ERT staff to implement during the actual event have been developed
- all relevant statutory, regulatory, and official agreements have been identified and have been considered in the BCM planning

3.1.2 The safety of personnel is considered first before all other responses

3.1.3 Prevention of any negative environmental impact and securing the environment from further negative impact is considered

3.1.4 A clearly defined coordination and contact procedure for local authorities and service utilities is established

3.1.5 The emergency response and preliminary damage assessment considers:
- response system configuration. (e.g. incident command system and members)
- corporate emergency coordinator leadership assignments
- functional response team duties
- types of expected disasters and responses. (e.g. evacuation, medical, power failure, earthquake/severe weather, violence, terrorist threat)
- available resources internal to the company to mitigate the disaster and implement preliminary damage assessments
- mutual aid agreements with other local businesses

3.2 Responsibility and process for disaster declaration

3.2.1 A corporate communications plan connecting executive management, employees, outside response agencies, outside service providers, customers, and the media is established

3.2.2 A recovery management team whose responsibility is the control, coordination, communication and leadership is defined, trained. Trigger events and recovery functions are defined and documented

3.2.3 A corporate communications plan includes both processes, targets, and messages - examples:
- toll-free numbers (ensure staff and stakeholders are kept informed)
- alternative help line and customer inquiry lines with tested roll-over
- structured call tree or cascade process
- approved preformatted messages for employees, media etc.

3.2.4 A predefined process for dealing with the media and public relations is established and specific individuals have been identified and trained to work with the media

3.2.5 The BCP clearly identifies and unambiguously describes all stakeholders and interest groups

3.2.6 Procedures for communicating both during and after an event concerning the business interruption to employees, suppliers, and customers have been established

3.2.7 Managers are aware of their responsibilities to ensure compliance with legal, regulatory and policy requirements for crisis management

3.3 Detailed damage assessment
3.3.1 The process, documentation, reporting criteria and staffing is in place to provide a timely accurate assessment of damage and impact

3.3.2 A coordinated approach is established which enables detailed damage assessment

3.3.3 Documentation and check lists have been developed to evaluate and record all forms of impact such as:
- personnel
- structural and facilities infrastructure
- IT – information technology
- machinery and tools
- IP - intellectual property
- office equipment
- inventory

3.3.4 Plan elements consider:
- pre-disaster service agreements with outside providers to assist with damage assessments (e.g. fire and water damage, building seismic evaluations, infrastructure damage, chemical releases, etc.)
- damage assessment mitigation agreements with outside service providers prior to the disaster occurrence (e.g. service contracts, purchase orders, priority of response agreements, etc.)
- resource availability from property insurance brokers or carriers to assist with damage assessments

3.3.5 Emergency response teams are coordinated and have documented training

3.3.6 Contacts and notification procedures have been established for all local, city and state disaster response centers

3.3.7 Contacts and notification procedures have been established for all emergency services, and include critical services such as water, gas, electrical, and telecom

3.3.8 Contacts and communication procedures have been established for customers and suppliers

4.1 Procedures to restore minimum acceptable service levels under disaster conditions

4.1.1 An organization-wide plan is in place, which assesses disaster conditions and minimum acceptable service levels

4.1.2 Disaster conditions have been identified and categorized by functional impact

4.1.3 Minimum service levels and maximum interruption times have been established for all functions

4.1.4 Preventative measures have been identified and documented

4.1.5 Procedures are in place to routinely check effectiveness

4.1.6 A coordinated approach is established and documented to restore service levels

4.1.7 Alternative production and operation sites have been identified and procedures to transfer service have been documented and tested

4.1.8 Responsibilities have been clearly documented and staff are trained
4.2 **Recovery of critical business functions and ongoing operations**
4.2.1 There is a company-wide strategy in place which has identified critical business functions, the dependencies and impact to operations
4.2.2 Critical data (both electronic and paper) necessary to support the mission-critical activities and their dependencies can be recovered simultaneously at more than one work area or recovery site if required
4.2.3 The organization has a clearly defined process for storing critical papers and other work in progress and unique documents

4.3 **Primary site salvage, repair and reconstruction**
4.3.1 There is a company-wide strategy in place, which assesses damage and prioritizes repair and reconstruction
4.3.2 All recovery/repair assumptions are documented such as:
   - the disaster recovery plan is current
   - an alternative facility is available
   - staff can be notified and can report to backup sites
   - off-site storage and materials survive
4.3.3 A process is established to determine what equipment/facilities have been destroyed or damaged
4.3.4 A process is established to determine what records, files and materials were protected from destruction or damage
4.3.5 A process is established to determine the available resources following the disaster or damage
4.3.6 A coordinated plan exists to manage all damage assessments and insurance claims activities
4.3.7 A coordinated plan exists to manage facilities clean up and reconstruction
4.3.8 A coordinated plan exists to manage replacement of equipment and tools

4.4 **Management of finances and insurance claims**
4.4.1 There is a company-wide strategy in place which includes a financial impact analysis
4.4.2 There is a financial policy in effect which covers displaced workers
4.4.3 All insurance policies are current and accessible
4.4.4 Back up access to all insurance coverage data is established
4.4.5 Insurance policies have been reviewed to insure adequate loss coverage
4.4.6 Business impact analysis has included insurance providers to potentially lower premiums and expand coverage

4.5 **Communication with key stakeholders**
4.5.1 Communication methods are identified and established with key stakeholders before a crisis occurs
   - key stakeholders to consider are employees, on-site contractors, media, shareholders, regulators, customers, neighbors and other interested constituencies
4.5.2 A crisis communications policy is established for communicating to all key stakeholders
4.5.3 Resources and a chain of command have been established for all company communications
- note: all external media communications are done by a trained individual.

5.1 Planning for an uninterrupted supply chain
5.1.1 Plan for assuring an uninterrupted supply of all materials down the entire supply chain regardless of disasters, embargoes, labor disputes, etc.
5.1.2 Ensure there is a company-wide strategy in place which assesses key suppliers and the processes they have established to mitigate disruption to the supply chain
5.1.3 All bill of materials (BOM) have been identified by supplier
5.1.4 Single (sole) source materials have been identified
5.1.5 Second source suppliers have been identified for all single source materials
5.1.6 Source or critical materials used by suppliers have been identified and risk to supply has been established
5.1.7 Requirements, specifications, and qualification procedures for all materials are regularly maintained and updated
5.1.8 Local requirements which could potentially impact supply have been reviewed at the supplier level and plans exist to mitigate exposures
5.1.9 Suppliers have business continuity plans in place and have been assessed to ensure the uninterrupted delivery of materials to the required facility or customer

5.2 Evaluation of the organization’s bill of materials to identify risks of supply disruption
5.2.1 The process and documentation has been developed to assess and assure key suppliers capabilities for continuity of supply for all tools, equipment and services
5.2.2 A process is in place for the review of all BOM
5.2.3 The levels of criticality, risk and impact have been established for products and services
5.2.4 A process is in place to review and evaluate a supplier’s risk to business
5.2.5 Second source and alternatives have been identified

5.3 Identification of qualified alternative suppliers that are not dependent on the same source of supply chain materials
5.3.1 A process is in place for the identification of long lead-time or single source materials
5.3.2 Qualified alternative suppliers that are not dependent on the same source of supply chain materials (stand alone) have been identified
5.3.3 Suppliers that are dependent on same source materials have been identified
  • all source supply and sole source providers of material are identified
  • a list is maintained of suppliers using sole source supply
  • inventory and disaster recovery plans are in place for suppliers using sole source materials

5.4 Single source materials and/or suppliers
5.4.1 A process is in place for the identification of single source needs
5.4.2 A list is maintained of single source materials and/or suppliers of services
5.4.3 Inventory plans or other disaster recovery plans are in place for single source materials and/or suppliers of services
5.4.4 A process is in place, which establishes alternative supply for both single source and long lead-time materials
5.4.5 Business continuity plans incorporate different levels of disaster recovery events
5.4.6 Material history and forecast of demand are available for single source materials
5.4.7 Single source material capacity is tracked and source of supply is understood
5.4.8 Emergency flexibility in supplier capacities, short and long-term, are tracked
   • suppliers of single source materials maintain multiple inventory locations
   • alternate sources of supply have been identified for single source material
   • qualification time for alternate sourcing is understood, qualification plans are in place, and qualification of alternate sources is ongoing

5.5 Consideration of continuity of materials as part of new product development plans
5.5.1 The process and documentation have been developed to assess supplier capabilities for continuity of supply in the new product development phase for all tools, equipment and services
5.5.2 A coordinated approach has been developed and is followed as part of the new product development cycle based on the BOM which identifies potential suppliers and sourcing capabilities
5.5.3 Company-wide, engineers and product developers have been instructed on the requirements for supplier continuity capabilities
5.5.4 Suppliers of materials, parts and services have been notified of the business continuity requirements and are assessed prior to purchasing or design commitment
5.5.5 A systematic approach is in place to identify potential continuity of materials issues and solutions or their alternatives

6.1 Establish site ownership
6.1.1 There is a company-wide strategy and documentation is in place which assures resource allocation and responsibility
6.1.2 All sites have owners assigned and succession plans
6.1.3 All owners have comprehensive and up-to-date call lists
6.1.4 All owners have comprehensive and up-to-date contacts for all emergency response teams, departments and functions
6.1.5 Site owner is responsible for maintaining currency, coordinating activities, and ensuring accuracy

6.2 Performance of annual drills and inspections
6.2.1 BCM recovery solutions and their plans are reviewed on an ongoing basis
   • the frequency and triggers that determine when such a plan is reviewed or audited is dependent upon the nature and scale of the business
6.2.2 There is a company-wide plan in place, which assures that the schedule for drills and exercises is executed. A process for tracking and recording the completion of the BCP tasks is established
- up-to-date (internal and external) contact schedules
- incident management and decision log template
- recovery status report
- relocation recovery profile
- relevant contracts, service level agreements, MOU’s letters of agreement

6.2.3 All sites have programs in place which test assumptions

6.2.4 All sites regularly exercise the plan with drills and inspections

6.2.5 Local response teams, fire, HAZMAT, etc., participate in scenario tests

6.2.6 Employees are regularly tested against the plan

6.2.7 Performance against plan is regularly evaluated and changes incorporated as identified

6.2.8 Exposure and avoidance techniques are regularly reviewed
7 BCM Templates

Note: The templates are provided as potential tools, not requirements.

Business Impact Analysis Questionnaire

Business Impact Analysis Overview

The Business Impact Analysis (BIA) is a process to determine the mission critical business functions and associated critical resources for “A Company.” This is done by identifying all of the “A Company” business functions and their processes, identifying all computer system applications that support all processes, determining the critical point in the business cycle of each process, determining if the process is critical to the business, estimating the potential loss and recovery time frame, and then ranking the vital business processes.

This questionnaire is designed to assist you when identifying the following types of key sources of information and other resources for your function, and for “A Company” overall. The intent is to identify:

- the financial impact resulting from the loss of your business function;
- the tangible and intangible causes of the financial impact;
- critical processes and resources required by your business function;
- computer system applications identification and ranking;
- recovery concerns and issues.

Scenario

When answering the questions within this document, please use the following scenario as the basis for your response.

- A major disruption of the “A Company” technology that supports your location has occurred. The technology or business function will be inaccessible for an undetermined period of time (for this exercise estimate at least 30 days).

- Over time, outside services, travel, and lodging expenses, etc. are authorized to assist in reestablishing business critical operations.
## Documentation Section

<table>
<thead>
<tr>
<th>Name:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Function:</td>
<td></td>
</tr>
<tr>
<td>Department:</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Title:</td>
<td>Phone:</td>
</tr>
<tr>
<td>Signature:</td>
<td>Date:</td>
</tr>
</tbody>
</table>

## Business Function Interview List

<table>
<thead>
<tr>
<th><strong>Information Technology</strong></th>
<th>Contact</th>
<th>Title</th>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer Service</strong></td>
<td>Contact</td>
<td>Title</td>
<td>Telephone</td>
<td>Email</td>
</tr>
<tr>
<td><strong>Finance</strong></td>
<td>Contact</td>
<td>Title</td>
<td>Telephone</td>
<td>Email</td>
</tr>
<tr>
<td><strong>Human Resources</strong></td>
<td>Contact</td>
<td>Title</td>
<td>Telephone</td>
<td>Email</td>
</tr>
<tr>
<td><strong>Manufacturing</strong></td>
<td>Contact</td>
<td>Title</td>
<td>Telephone</td>
<td>Email</td>
</tr>
<tr>
<td><strong>Purchasing</strong></td>
<td>Contact</td>
<td>Title</td>
<td>Telephone</td>
<td>Email</td>
</tr>
<tr>
<td><strong>Materials Management</strong></td>
<td>Contact</td>
<td>Title</td>
<td>Telephone</td>
<td>Email</td>
</tr>
<tr>
<td><strong>Payroll</strong></td>
<td>Contact</td>
<td>Title</td>
<td>Telephone</td>
<td>Email</td>
</tr>
</tbody>
</table>
Business Functions and Processes of “A Company”

Please provide a high-level overview of the business function by identifying the 3 to 5 major business processes within the function you are representing. Also needed is your prioritization (1 is highest priority) of those processes based on the scenario. The following is an example of how “xxxxx” might be documented.

<table>
<thead>
<tr>
<th>Business Function: XXXXX</th>
<th>Process</th>
<th>Description</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Function: XXXXX</th>
<th>Process</th>
<th>Description</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Function: XXXXX</th>
<th>Process</th>
<th>Description</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Function: XXXXX</th>
<th>Process</th>
<th>Description</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Financial Impact

The financial impact is usually comprised of impact to the revenue stream, as well as expenses incurred during, or due to, the outage.

Please identify the impact to “A Company” in terms of revenue loss and expenses incurred due to the loss of technology support to your business function.

<table>
<thead>
<tr>
<th></th>
<th>1 Hour</th>
<th>8 Hours</th>
<th>24 Hours</th>
<th>48 Hours</th>
<th>72 Hours</th>
<th>1 Week</th>
<th>1 Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue Impact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expense Impact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Areas of Impact

The revenue impact and expense impact can usually be associated with a particular tangible or intangible area. The table below provides a list of areas of revenue impact and areas of expense impact. Please identify the top two or three areas of impact in each column.

<table>
<thead>
<tr>
<th>Revenue Impact Areas</th>
<th>Expense Impact Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tangible Revenue Impact Areas</strong></td>
<td><strong>Tangible Expense Impacts</strong></td>
</tr>
<tr>
<td>Permanently lost sales</td>
<td>Emergency recovery expenses:</td>
</tr>
<tr>
<td>Deferred sales</td>
<td>Overtime</td>
</tr>
<tr>
<td>Loss of trade discount</td>
<td>Services</td>
</tr>
<tr>
<td>Loss of contracts</td>
<td>Temporary help</td>
</tr>
<tr>
<td>Interest or cash float</td>
<td>Equipment rental</td>
</tr>
<tr>
<td>Cash postings</td>
<td>Office space rental</td>
</tr>
<tr>
<td>A/R- delays in receivables</td>
<td>Fines and penalties</td>
</tr>
<tr>
<td>Supply chain</td>
<td>Charges or fees</td>
</tr>
<tr>
<td>Others: (please identify)</td>
<td>Others: (please identify)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Revenue Impact Areas</th>
<th>Expense Impact Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intangible Revenue Impact Areas</strong></td>
<td><strong>Intangible Expense Impacts</strong></td>
</tr>
<tr>
<td>Organization image</td>
<td>Morale</td>
</tr>
<tr>
<td>Community image</td>
<td>Productivity</td>
</tr>
<tr>
<td>Loss of market share</td>
<td>Regulatory compliance</td>
</tr>
<tr>
<td>Customer service</td>
<td>Labor relations</td>
</tr>
<tr>
<td>Vendor relations</td>
<td>Legal liability</td>
</tr>
<tr>
<td>Competitive advantage</td>
<td></td>
</tr>
<tr>
<td>Quality / accuracy</td>
<td></td>
</tr>
<tr>
<td>Others: (please identify)</td>
<td>Others: (please identify)</td>
</tr>
</tbody>
</table>
Business Function Detail

Review and discuss the questions on this page.

What are the *vital records* essential to support and reestablish the business function? Are the *vital records* protected?

Do your business processes have documented manual procedures for conducting its business functions without access to critical application systems?

What are the department interdependencies? *(Which department do you depend on for input to perform your business function? Which departments depend on you to perform their business function)?*

Are there any peak load or stress considerations (*e.g. special monthly/annual processing, biweekly work, etc.*)?
“A Company” Application Systems

Definitions:

Recovery Time Objective (RTO): the time when an application must be available to the user following the computer outage, usually measured in hours or days.

Recovery Point Objective (RPO): the point to which the data "will be recovered to." This point is the state of the data as of the last backup.

Using the chart on the following pages, please identify the computer application system(s) that support your business function. Indicate their priority to your business function, as well as the recovery time objective (RTO) and the recovery point objective (RPO). Business functions are encouraged to work with their company IT/IS organizations in completing this section.

The following chart is an example:

<table>
<thead>
<tr>
<th>Software-Application Core (examples)</th>
<th>Recovery Time Objective (RTO)</th>
<th>Recovery Point Objective (RPO)</th>
<th>Number Of Users</th>
<th>Business Function &amp; Priority</th>
<th>Executive Sponsor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Tracking</td>
<td>2 days</td>
<td>1 day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDX</td>
<td>2 days</td>
<td>1 day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medacom</td>
<td>4 days</td>
<td>2 days</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GMIS</td>
<td>7 days</td>
<td>3 days</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

“A Company” Application Systems Chart

<table>
<thead>
<tr>
<th>Software-Application Core (examples)</th>
<th>Recovery Time Objective (RTO)</th>
<th>Recovery Point Objective (RPO)</th>
<th>Number Of Users</th>
<th>Business Function &amp; Priority</th>
<th>Executive Sponsor</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label printing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product data management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchanges (eHITEX)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchanges (e2open)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partner-to-partner integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;What if&quot; / supply chain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replenishment - VMI / RLT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business partner extranet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global SBM escalation process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workflow (generic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERP - QMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RF applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time/attendance (DL)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indirect labor tracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fax server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warehouse management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e-logistics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Freight pay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financials</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image capture &amp; doc. storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financials</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web procurement (WebPro)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MRO procurement (e-Pro)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quotation system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measurements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDI (out)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDI (In)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Materials management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ad hoc reports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Data warehousing |  |  |

<table>
<thead>
<tr>
<th>Software-Application Core (examples)</th>
<th>Recovery Time Objective (RTO)</th>
<th>Recovery Point Objective (RPO)</th>
<th>Number Of Users</th>
<th>Business Function</th>
<th>Executive Sponsor</th>
</tr>
</thead>
<tbody>
<tr>
<td>AR/AP/GL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expense statement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product data management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturing execution (SFDM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturing execution (STATIS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**GLOBAL SERVICE**

| ERP - service |  |  |  |  |  |
| Service execution |  |  |  |  |  |
| Customer interfacing |  |  |  |  |  |

**Applications that should be listed:**

|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
Section A:

Business Unit: _______________________

Contact Name: ________________________

Approved: __________________ Date: __________________

BCP Confidence Rating as of _____ (1-Low; 5-High) ______

Section B: Customers & Suppliers

<table>
<thead>
<tr>
<th>Business unit customers - name, key contact, alternate contact, contact information, address</th>
<th>Business unit suppliers - name, key contact, alternate contact, contact information, address</th>
</tr>
</thead>
</table>

Key processes: ranked in order of importance (1-Low; 5-High)

Primary and secondary critical resources: applications, tools, servers, power sources, people (insert description of resource, processes and alternate method to use if the primary is unavailable)

Vital records storage and retrieval: insert document type, media type, and procedure to retrieve and restore information
### Section C: Business continuity procedures - action plan

**Business process impacted**

<table>
<thead>
<tr>
<th>Automated and manual procedures:</th>
<th>Responsible person:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name:</td>
</tr>
<tr>
<td></td>
<td>Title:</td>
</tr>
</tbody>
</table>

**Duration**: denote duration these alternate processes can be utilized

### Section D: Key contacts and resources

**Implementation**: describe when the BCP is implemented

**Responsible person:**

<table>
<thead>
<tr>
<th>Activates plan: the process for activating the plan</th>
<th>Team contacts: primary and alternates with contact information</th>
</tr>
</thead>
</table>
Return to normal operation:

| Resource requirements: | office space, phones, fax, PC, laptops, etc. |

### Critical Incident Team Model

A critical incident management model begins with development of a Critical Incident Team. The model consists of the following six steps:

- organizational structural design;
- selecting the team;
- developing the team;
- designing and conducting a critical incident audit;
- developing a contingency plan;
- managing the incident.

### Organizational Structure Design

The critical incident management matrix is composed of a lean, permanent staff, augmented by experts from various functional divisions as needed. It should be inherently flexible and structured to adapt quickly to changing conditions. In general, the Team is assembled in situations where a serious threat requiring swift intervention is critical. The Team is not intended to handle disaster recovery or emergency situations best left to ERT protocols.
Once a critical incident or threat has been identified, the Team can select from the various functional divisions, those personnel with the most appropriate skills and abilities to handle the incident. Once the organizational structure has been designed, the Team of individuals who will participate can be selected.

**Selecting the Team**

The policies used to select a critical incident team is similar to those used for assigning people to new jobs. The permanent critical incident team should decide what additional skills or input are needed to handle an impending threat successfully, identify the divisions where individuals with these skills are currently assigned, and decide from what level of management the representative should be selected. How long the task will take and whether it will require full time or part time assignment should also be considered. Clarifying these points will help determine which key individuals are best suited to managing an incident.

Often, the selected Team Manager is the Director of Human Resources or his designee. Other permanent members might be comprised as follows:

- director of operations or facilities;
- director of security;
- general counsel or legal representative.

Depending on the nature of a specific situation, members from other groups can be temporarily added, such as:

- finance;
- MIS/IT;
- purchasing;
- manager of the employee making the threat;
- outside resources (consultant(s), psychologist, forensic examiner, public or private agencies, etc.).

**Developing the Team**

After selecting the critical incident team members, the team manager becomes responsible for developing the group into a cohesive, effective unit. The manager must clearly understand his purpose which is to develop a proficient team to handle the crisis while others in the organization continue to perform their daily routines. It is important for each member to select and develop an alternate to represent the function in the absence of the primary team member. The designated alternates should be provided with minutes of all meetings and drills.

Team development is accomplished by analyzing goals (where the team is going), roles (who will be doing what) and processes (how members will function as a team). Once the members understand these principles this allows development of a dedicated team. Drills using realistic scenarios should be done and the post-drill briefings should point out what worked well and what
did not work well. To keep the drills as realistic as possible, regular members should periodically be “unavailable”, allowing the alternate designee have the opportunity to participate. It is generally not realistic to have a drill where both the primary and alternate member are both participants. It would be OK, however to have the alternate or “unavailable” member participate strictly as an observer, and to participate in the debriefing afterwards.

**Designing and Conducting a Critical Incident Audit**

The critical incident audit is the foundation of the team management cycle. For planning purposes, the audit assists managers in analyzing their environment, identifying potential threats, assessing the effects of each threat, determining each threat’s probability, and setting threat priorities.

The audit should weigh the probability of a threat occurring against the impact or loss the act would have if it did occur. For example, a crisis audit in a multi-national company might conclude that the likelihood of a key executive being kidnapped is low. However, the impact on the company might be quite high. Therefore the Team might conclude the threat of an executive kidnapping should be given a high priority on a list of possible threats even though the chance is low that such an attack might occur.

Based on these assessments, specific threats can be divided into various levels that reflect the seriousness of the consequences.

A level-one incident, for example, would seriously affect a company’s ability to stay in business, while a level-two threat might cause disruption but would not completely shut down operations.

Formulating crisis objectives follows setting of priorities among possible crisis threats. Managing critical incident objectives are not distinct from corporate objectives. In fact, the very purpose of the Team is to deal with a situation that might impede the accomplishment of the company mission. The Team role should be approved by the chief executive officer (CEO) or other high-level executive. The final objectives should reflect the thinking of those at the highest levels in the organization.

Specific crisis objectives should be set for each threat. For example, the crisis objectives developed to counter the threat of an executive kidnapping might include a plan for protecting those at risk at home, as well as in the office.

**Developing a Contingency Plan**

A contingency plan, written by members of the Team, should consist of five components: the introduction, the objectives, the assumptions, triggers, and the action steps. For example, a contingency plan designed to deal with a terrorist threat would begin with an overview of the crisis, identifying the group or groups presenting the threat, the target locations, and the individuals and issues that might be affected. This introduction should be followed by a specific, yet succinct, outline of the plan’s objectives. One objective, in another example, might be to implement security measures designed to protect employees from a person making threats of violence. These measures should be spelled out in to the contingency plan along with the ways to achieve them.
Another part of the plan should be the selection and advance preparation of a suitable command center where the Team and expanded resources can properly conduct planning and implementation.

The next component of the contingency plan is the assumptions. Assumptions are those factors the Team planners cannot control, but would cause concern if they did occur. Assumptions should be thought of as a guideline that adds both focus and depth to the objectives. In other words, the Team should, “plan for the worst and hope for the best.”

In certain geographic areas, for example, it may be suspected that law enforcement officials are sympathetic to specific terrorist organizations or not particularly supportive of the U.S. The assumptions laid out in the contingency plan must consider these factors and alternate plans should be made to deal with the various possible scenarios.

The triggers are the fourth part of the contingency plan and act as alarms that activate the crisis plan. The trigger must be carefully constructed to prevent premature or delayed implementation. The trigger can be designed so it escalates the response by degrees. Although this response will vary from organization to organization, such a system activates the Team and only those resources needed to cope with the emergency at hand. Without controls, each incident might cause a full response, potentially causing severe disruption of the organization’s day-to-day operations.

The final component, the action plan, develops a systematic sequence of events designed to accomplish the objectives. These steps clearly delineate the activities required to accomplish each objective. The role of every person, division, department, or agency is outlined, designating primary players, as well as backup or support players.

For example, in a terrorist threat scenario, the security director might assume a primary role by providing expert guidance on the tactics that should be used and for coordinating with the appropriate public agencies and private resources.

**Managing the Incident**

At this point, the organization has ideally implemented its crisis structure, selected and developed its Team, conducted a crisis audit, delineated and prioritized team objectives, and developed a contingency plan. The CEO or other senior management should develop guidelines that will establish how the specific crisis will be managed and who will manage it. Depending on the circumstances and management structure, the CEO or other senior management might want to be directly involved, while in another instance, may prefer to have the Team Manager handle the incident.

Another management approach might tie the decision concerning who will handle the incident to various crisis levels. For example, a level-one situation (such as an executive kidnapping) would have a potentially significant effect on the organization as a whole.
On the other hand, a **level-two** situation (such as a bombing that causes only property damage) might not affect the entire organization as widely, or threaten its survival. Certainly (depending on the circumstances) a level-two incident could escalate into a level-one crisis. The bombing of one building accompanied by a threat to bomb additional locations is an example.

An example of a **level-three** situation might be an employee (or other person) who exhibits dangerous behavior, such as threatening or assaulting a fellow worker or supervisor.

Prompt response of the Team might prevent a lower level threat, emergency, or other event from turning into a level-two or level-one situation.

There are many different types of situations or events that might trigger the activation of the Team. Examples include, but are not limited to:

- disruptive or threatening behavior by employee(s) or outsiders;
- events or situations that have the potential for damaging the reputation of the company or causing a major disruption to business.

Ordinarily, the CEO or other senior management may become involved in a level-one incident, either managing it directly or delegating authority. For the most part, a level-two situation will be managed by the Team Leader. While the Team Leader may be responsible for keeping the CEO informed, he or she should have overall authority to manage the event. This allows the best chance to deal with the situation in a swift, cost-effective, and coordinated manner. Roles, responsibilities, and authority must be made clear to avoid interruptions in the process by other well intentioned, but uninformed persons. A crisis is no time for “too many cooks in the kitchen.” The authority and mission of the Team must be vigorously supported by the CEO and others in senior management.

Crime, terrorist activity, violence, threats from a number of sources from both outside and within a company - are not only a reality but have become a rather common situation, particularly for multi-site companies with a growing global presence. An efficient and cost-effective method of addressing an array of potential critical situations is through management and thoughtful preparation **before** a situation occurs.
# Risk Analysis and Disaster Mitigation Worksheet

<table>
<thead>
<tr>
<th>Purpose</th>
<th>A process to perform a risk analysis of your organization and develop a disaster mitigation plan that mitigates risk and impact prior to occurrence. The goal is to reduce or eliminate the business impact from a variety of threats.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective</td>
<td>To determine the effect of defined impact on the core business functions. To maximize the recovery of return to normal operating conditions.</td>
</tr>
</tbody>
</table>
| In Scope | • business functions and associated business processes  
• key impacts and related failures  
• disaster mitigation strategies/controls  
• disaster mitigation options |
| Out of Scope | • development of business recovery and emergency response plans/ site emergency plans. These plans are the actual procedures for dealing with failure events and steps to recover from the failure  
• product plans or product build plans |
| Identify Business Impacts | Identify the potential impacts to normal business operations your organization might sustain, such as:  
• extended building closures;  
• the inability to transport products-parts/equipment;  
• supply disruption;  
• outages of the internet and other forms of communications;  
• etc. |
| Process | Fill in the shaded areas of the Risk Analysis Worksheet.  
Fill in the shaded areas of the Disaster Mitigation Worksheet.  
Fill in the shaded areas of the Disaster Mitigation Plan.  
Develop a Risk Plotting Worksheet. |
## Risk Analysis Process

### Getting Started
List the primary mission/objective of the organization or business unit.

### Step 1
- List the organization’s key business functions.
- Select the top 3 to 5 business functions.
- For each business function identified, list the business processes that support the functions.
- For each business process, identify the key resources needed for these business processes to operate - consider the following areas:
  - people;
  - computer applications;
  - building infrastructure;
  - other infrastructure needs (i.e. communication);
  - internal groups (IT, security, HR, safety);
  - suppliers/vendors.

### Step 2
Brainstorm any additional unique risks and impacts associated with your business functions and the supporting processes that could cause a failure.
- What's the worst thing that could happen?
- What's the worst thing that has happened to this organization?
- What are the critical interfaces with other business groups that give you the most concern, and why?
- What are your expectations of service level agreements and internal groups such as IT, human resources, etc.?

### Step 3
For each of the business processes and the supporting processes, perform a risk and impact analysis using the definitions:
- Severity of the impact -  H = High, M = Medium, L = Low
- Likelihood of the impact and failure occurring -  H = High, M = Medium, L = Low
  - note - don’t forget to consider geographic differences when determining impact severity & likelihood
**Next Steps**

- Finish performing all analysis of the business functions. Additional sessions may be required depending upon the complexity of the business processes. Ensure that you assess all critical points of failure.

- Summarize the information from steps 1 through 3 on the Risk Analysis Worksheet.

- Determine the plans of organizations and external groups and develop your plans accordingly. List all expectations and the services external groups will provide in an emergency. Determine how prepared they are themselves to sustain business disruption both short-term and long-term.

- Ensure your organizations management and key stakeholders ratify the risk / impact analysis.

- Prepare the disaster mitigation worksheet prior to the disaster mitigation session. Include all the information from the Risk Analysis Worksheet, the supporting business processes, and identified impacts.

- Prepare electronic and hard copies of the two completed documents (Risk Analysis Worksheet and Disaster Mitigation Worksheet) for the Disaster Mitigation Session.
## Disaster Mitigation Session

### Getting Started
Review the information in the Risk Analysis Worksheet developed from the risk analysis session(s).

### Step 1
For each process, create a severity impact and likelihood of a failure analysis.
- Plot the information on the risk plotting worksheet to help identify the items to mitigate or control.
- Identify critical points of failure.

### Step 2
Identify disaster mitigation strategy options for business failures identified.
- Develop a prioritized list of risks to eliminate.
- Develop controls and/or disaster mitigation strategies based on those items that are in the high severity and high likelihood of occurrence quadrant.
- Work through the quadrants assessing and categorizing each impact identified.

### Step 3
Identify your control and mitigation options
- Using ‘do nothing and do everything’ options may help establish boundary conditions.
- Define the options, the estimated cost, the time period, and the percent of risk mitigated for each issue.
- Identify the advantages or disadvantages of each option.
- Define the timeline and phases if appropriate.

Document the information on the Disaster Mitigation Worksheet in the appropriate column.

### Step 4
Repeat step 1 through 3 for all business functions and supporting business processes.

### Next Steps
Determine which options are feasible, appropriate, and have high ROI.
- Develop a proposal based on your control and mitigation prioritized options list.
- Review the results internally to ensure that they are complete and within the established acceptable levels of corporate risk.
- Obtain management support for the disaster mitigation plan.
- Present the final options and recommendation for ratification to management for ratification and support.
- Develop the disaster mitigation plan by documenting the disaster mitigation strategies, controls and options selected, plus the risk analysis information for the organization.
- Maintain this document with your organization’s other key operating and strategic plans.
## Develop and Implement the Disaster Mitigation Plan

- Include all mitigation plan items.
- Ensure annual risk analysis and review of the disaster mitigation plan.
- Keep the process healthy and alive from year to year.
- Identify risk reduction activities from the disaster mitigation worksheet options.
- Determine the priority and timing of each activity and clearly identify the expected deliverable and outcome.
- Obtain management ratification on the final disaster mitigation plan.

<table>
<thead>
<tr>
<th>Definitions Category</th>
<th>Impact Severity</th>
<th>Likelihood</th>
</tr>
</thead>
</table>
| **High**             | Significant and lasting disruption to business operations -  
                        - any risk of injury to employees, customers, suppliers or consumers  
                        - extremely serious financial loss  
                        - significant time to return to normal business operations  
                        - permanent or long-term damage to brand image  
                        - loss of market segment share in key segments  
                        - breach of legal requirements, customs and excise  
|                      | The likely chance of occurrence -  
                        - has happened at this site before  
                        - has happened at other company sites before  
                        - will likely occur  
                        - the likelihood of occurrence is so high an insurance company won’t insure |
| **Medium**           | The potential to cause temporary disruption to business operations -  
                        - no risk of injury  
                        - serious financial loss  
                        - takes some time to return to normal business  
                        - some loss of sales  
                        - medium-term damage to brand image  
|                      | The possible chance of occurrence -  
                        - has happened at our other company sites, with different risk factors  
                        - has happened at another company’s site  
                        - it is possible it will occur  
                        - insurable event with high/medium likelihood |
| **Low**              | Minor disruptions, irritants -  
                        - minor or insignificant financial loss  
                        - no risk of injury  
                        - return to normal business operations is less than a few days.  
                        - minor damage to reputation of company, easily protected by action such as letter of apology  
                        - any loss of sales would be temporary and easily made up  
                        - damage to brand image easily and quickly corrected  
|                      | The unlikely chance of occurrence -  
                        - has not happened at our company or at other companies at this site  
                        - it is not likely to occur  
                        - insurable event – low likelihood/low probability  
                        - easily insurable |
### Risk Analysis Worksheet

<table>
<thead>
<tr>
<th>Business Function #1</th>
<th>Description of process and key resources</th>
<th>Critical links (Organizations you rely upon)</th>
<th>Impacts/Failure(s)</th>
<th>Impact Severity (H/M/L)</th>
<th>Likelihood of failure (H/M/L)</th>
<th>Disaster mitigation required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Function #2</th>
<th>Description of process and key resources</th>
<th>Critical links (Organizations you rely upon)</th>
<th>Impacts/Failure(s)</th>
<th>Impact Severity (H/M/L)</th>
<th>Likelihood of failure (H/M/L)</th>
<th>Disaster mitigation required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Disaster Mitigation Worksheet

Examples of events or incidents: unauthorized access to facilities; breach of physical perimeters or facilities; computing infrastructure dependencies; loss of key workers; external threats; natural disasters; malicious attacks; supplier failure; customer failure.

### Business Function #1

#### Business Process

<table>
<thead>
<tr>
<th>Process step Ref. #</th>
<th>Impact/Failure Description</th>
<th>Disaster Mitigation for Impacts/Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>List failures that require a risk mitigation plan</td>
<td>Options</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Option 1 – do nothing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Option 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Option 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Option 4 – do everything</td>
</tr>
<tr>
<td>Process step Ref. #</td>
<td>Impact/Failure Description</td>
<td>Disaster Mitigation for Impacts/Failures</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>List failures that require a risk mitigation plan</td>
<td>Options</td>
</tr>
<tr>
<td>2.1</td>
<td>Option 1 – do nothing</td>
<td>Option 1 – do nothing</td>
</tr>
<tr>
<td></td>
<td>Option 2</td>
<td>Option 2</td>
</tr>
<tr>
<td></td>
<td>Option 3</td>
<td>Option 3</td>
</tr>
<tr>
<td></td>
<td>Option 4 – do everything</td>
<td>Option 4 – do everything</td>
</tr>
<tr>
<td>2.2</td>
<td>Option 1 – do nothing</td>
<td>Option 1 – do nothing</td>
</tr>
<tr>
<td></td>
<td>Option 2</td>
<td>Option 2</td>
</tr>
<tr>
<td></td>
<td>Option 3</td>
<td>Option 3</td>
</tr>
<tr>
<td></td>
<td>Option 4 – do everything</td>
<td>Option 4 – do everything</td>
</tr>
</tbody>
</table>

**Sample Disaster Mitigation Plan**

**Format example**

<table>
<thead>
<tr>
<th>Risk Reduction Activities</th>
<th>Q2 200x</th>
<th>Q3 200x</th>
<th>Q4 200x</th>
</tr>
</thead>
<tbody>
<tr>
<td>activity 1</td>
<td></td>
<td></td>
<td>activity 7</td>
</tr>
<tr>
<td>activity 2</td>
<td></td>
<td></td>
<td>activity 8</td>
</tr>
<tr>
<td>activity 3</td>
<td></td>
<td></td>
<td>activity 9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Reduction Deliverables</th>
<th>Q2 200x</th>
<th>Q3 200x</th>
<th>Q4 200x</th>
</tr>
</thead>
<tbody>
<tr>
<td>deliverable 1</td>
<td></td>
<td></td>
<td>deliverable 7</td>
</tr>
<tr>
<td>deliverable 2</td>
<td></td>
<td></td>
<td>deliverable 8</td>
</tr>
<tr>
<td>deliverable 3</td>
<td></td>
<td></td>
<td>deliverable 9</td>
</tr>
</tbody>
</table>
Risk Plotting Worksheet Example

![Image of a risk plot diagram](image)

The SEMI Business Continuity Guideline for the Semiconductor Industry and its Supply Chain
Disaster Recovery Plan

The Disaster Recovery Plan should include a concise table of contents.

Overview

Plan Author(s) and Preparing Organization
Identify the author(s) of the plan and organization/application of the plan.

Emergency Response Plan Scope
Identify the services or systems being addressed within this document. You may have numerous Emergency Response Plans, one for each system or service supported by your group. In general, a business group will have more than one emergency response plan (ERP) to address different aspects of your response. A high-level plan may be used to define the crisis management team, while more detailed plans will provide systematic instructions on how to fix problems impacting the business. The template may be used for all of your emergency response plans — you can remove the sections that do not apply.

This document can be used to establish the basic crisis management framework for a variety of crises regardless of whether emergency response or business recovery plans (BRP’s) are activated. For example, a crisis team could be convened to deal with a serious workplace violence issue, even if there is no need to execute the other ERP’s and BRP’s.

You will not need plans for emergency response activities that are done by other groups — these should be referenced in the business group’s business recovery plan. If the group has key facility equipment, software, or data that is not supported by the software applications team or IT department, procedures to rebuild should be covered in an emergency response plan.

Emergency response procedures should begin at the point where you have control over the executed response. For example, in a fire situation, the emergency response teams may not be permitted to re-enter the building until authorized by the fire department or chain of command. An emergency response plan would begin at that point.

Plan Objectives
This section contains the clearly defined objectives for the emergency response plan.

Emergency Response Priorities
Define the response priorities for all services and applications within the scope of the plan. Emergency Response procedures and decisions should be guided by the agreed-upon priorities.
Emergency Response Team Contact list
List the members of the team who will address the crisis and fix the problem. Determine who will maintain the team locator list and where it will be kept. Include names, addresses, phone numbers and alternate contacts as well.

<table>
<thead>
<tr>
<th>Position</th>
<th>Primary</th>
<th>Alternate 1</th>
<th>Alternate 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name &amp; address</td>
<td>Name &amp; address</td>
<td>Name &amp; address</td>
<td></td>
</tr>
<tr>
<td>Work phone</td>
<td>Work phone</td>
<td>Work phone</td>
<td></td>
</tr>
<tr>
<td>Cell phone</td>
<td>Cell phone</td>
<td>Cell phone</td>
<td></td>
</tr>
<tr>
<td>Home phone</td>
<td>Home phone</td>
<td>Home phone</td>
<td></td>
</tr>
</tbody>
</table>

Crisis Team Roles and Responsibilities
Define expectations of all members on the Team. Clearly define the scope of the roles of senior management. Establish the composition of the teams well in advance. Your senior management may actively participate in the emergency response or business recovery teams, or it may be that the Team has different roles for senior managers. However you organize it, determine how to let the emergency response teams and business recovery teams make decisions appropriate to their areas of responsibility. You may need to provide a pre-established communications method to provide communication updates to senior management.

The table below includes sample positions and responsibilities. Specific roles and responsibilities may vary. Positions may be customized and the team-specific details added.

<table>
<thead>
<tr>
<th>Position</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crisis Team Director</td>
<td>Manages all crisis team activities. Communicates with organization’s executive staff, and senior management. Creates sub teams and other groups necessary to assess the situation and develop appropriate strategies.</td>
</tr>
<tr>
<td>Crisis Team Coordinator</td>
<td>Keeps the team, processes and meetings focused</td>
</tr>
<tr>
<td>Scribe</td>
<td>Captures the main events, decisions and ARs – monitors crisis, keeps master status.</td>
</tr>
<tr>
<td>Communication Coordinator</td>
<td>Drives the creation of communication material for internal audiences. External audiences are coordinated thru pre-established channels such as external affairs.</td>
</tr>
<tr>
<td>Business Recovery Team Manager</td>
<td>Provide updates to the Team at pre-defined intervals.</td>
</tr>
<tr>
<td>Emergency Response Team Manager</td>
<td>Provide updates to the Team at pre-defined intervals.</td>
</tr>
<tr>
<td>GEO Manager</td>
<td>Coordinates and reports on the activities in affected geographies. Provides a two-way communication channel to the field.</td>
</tr>
</tbody>
</table>
Response Team Roles and Responsibilities

Define expectations of all team members on the emergency response team. Some examples of responsibility follow, however, they are not necessarily required. The same person may take on multiple responsibilities.

<table>
<thead>
<tr>
<th>Position</th>
<th>Individual</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Overall issue management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Administrative responsibilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coordination responsibilities – chain of command, EHS, security, corporate services, IT, public affairs, HR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logistics responsibilities – including supplier/vendor interaction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technical expertise</td>
</tr>
</tbody>
</table>

Communication Method

Clearly identify how the team will communicate. More than one option may be needed as local services and cell phone service may not be available.

Emergency Response Location

Clearly identify where the teams will assemble in the event of a crisis or disaster (should the primary facility be unavailable). An alternate work location should be identified in the event site entry is prohibited. Transportation to the secondary site may be necessary. Secondary sites may include: a site chain of command group, a local hotel, or a mirror facility. Arrangement with the sites is needed in advance.

Crisis Management Checklist - sample

Edit the sample checklists to ensure the crisis teams can quickly and completely activate the plan. Define any additional steps that need to be included, and remove the steps that don’t apply. In some cases you may want to include more procedural detail with each step.

Crisis Management Plan execution is triggered appropriately

- links established with site chain of command groups and other emergency management teams involved in the crisis
- crisis management team convened
- establish links to business group’s Emergency Response Teams and business recovery teams

Crisis communications plan activated

- employee communications done
- customer communications done
- supplier communications done

Return to normal business operations

- return to normal communications to employees, business group’s emergency response teams and business recovery teams
- conduct post mortems
- review and update procedures based on implementation success
• disband emergency response teams and business recovery teams
• disband the crisis management team

Emergency Response Plan Checklist - sample

Emergency response plan execution is triggered appropriately
• links established with site chain of command group and other emergency management teams involved in the crisis
• emergency response team convened
• emergency response location confirmed
• crisis/recovery team convened
• link to business’ crisis/recovery team

Emergency response procedures ready
• problem identified
• solution components defined
• keys, passwords and security codes available
• replacement equipment, software ordered (if necessary)
• data recovered from off-site records
• replacement equipment confirmed and inventoried
• replacement equipment tested and loaded with software/data

Return to normal business operations
• validate readiness to return to normal operations
• business users notified
• critical business processing resumed
• document the damage assessment & recovery costs
• post-mortem the event

Crisis Management
This section contains specific crisis management information for your organization. Use the sections outlined or add your own.

Crisis Activities
The crisis management team acts as a central command point from which a business group can direct their crisis activities. Typically, the crisis teams will launch sub teams to address specific issues such as business recovery or emergency response, and link into other crisis response teams as necessary. Example: the site emergency response efforts and the site chain of command group

The flow of activity may frequently follow this sequence:
Event
↓
Trigger
↓
Activate crisis response team
↓
Activate other business group teams
Emergency response team(s)
Business recovery team(s)
↓
Assess situation
↓
Determine business group strategy
Communicate the strategy: teams, employees, internal groups, and senior management
↓
Execute strategy
Regular reports from emergency response teams and business recovery teams
Regular reports to the site chain of command, corporate chain of command (if appropriate)
↓
Communicate
↓
Regular communication to stakeholders (employees, internal groups and other crisis teams)
↓
Determine the timing and the criteria for Return to Normal operating conditions
Communicate the decision
Hold post-mortems

Critical Operating Information

Off-site Storage Information
Identify what is stored off-site, who is authorized to recall the information and the specific off-site contact information (account numbers, box numbers, and other pertinent information). If this information is also needed for recovery at alternate site, you will need to coordinate with the business recovery team for access to the data.

Vital Records
Clearly identify all key documents, contacts, forms, files, processes, etc. needed to manage the business. Clearly identify where these files are kept. You may want to maintain backup in hard copy form and on remote servers.
Keys, Electronic Codes and Passwords
During recovery or data restoration, keys, codes and passwords may be required in order to rebuild the servers or to operate remotely. They will need to be easily available. You may want to keep these keys in a secure location off-site. Passwords and codes may need to be listed in a separate document.

Vendors/Suppliers
Identify vendors for the software and hardware utilized in business operations. Identify specific contract information and PO #’s as appropriate. Include vendor contact information required to obtain authorization, assistance, etc.

<table>
<thead>
<tr>
<th>Vendor/Supplier</th>
<th>Product/Service</th>
<th>PO #</th>
<th>Alternate Supplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name &amp; address</td>
<td></td>
<td></td>
<td>Qualified alternate suppliers</td>
</tr>
</tbody>
</table>

Response Procedures Emergency
Document all emergency response resources - equipment, materials, facilities, staff, applications, computing infrastructure, procedures, checklists, or documents, required for a successful emergency response of the department/team. Ensure the correct crisis/recovery teams are notified of the problem and the estimated time required to return to normal business operating conditions. This will provide data needed to determine whether to trigger the business recovery plans.

Damage Assessment
Document how and who will perform a damage assessment of the impacted environment. This should include data, equipment, environment, etc.

Procedures for Recovering Lost or Damaged Data
Document data recovery/restoration procedures that support the plan. Define or reference the documented actions and associated procedures necessary for recovering lost or damaged data. Some examples of recovery actions include building a new database and loading it with current corrected data and restoring communications or interface connections.

Emergency Response Procedures for System/Service
Complete a separate section for each emergency response documented in the plan. Clear documentation is important, particularly for those unfamiliar with your environment. Document steps in a way that assumes the key or critical staff members are NOT available to execute the plan.
<table>
<thead>
<tr>
<th>Purpose (who should perform the task, when, and why)</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who:</td>
<td></td>
</tr>
<tr>
<td>When:</td>
<td></td>
</tr>
<tr>
<td>Why:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resources</th>
<th>Identify all resources required to respond to the emergency. Staff, computers, forms, data, documentation, books, process documents, contacts, office supplies, databases, web sites etc. <em>(resources, documentation, access/permission, keys, etc)</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>Other resources and requirements</td>
<td>What are the critical dependencies? Are there other applications, servers, and people, documents that must be in place before resuming?</td>
</tr>
<tr>
<td>Requirements</td>
<td><em>(resources, documentation, access/permission, keys, etc)</em></td>
</tr>
<tr>
<td>Knowledge and skills</td>
<td><em>(procedures, skill/knowledge, passwords, resource locations, emergency response locations, etc)</em></td>
</tr>
<tr>
<td>Emergency response procedures</td>
<td>Document the procedures or steps required and the order required. Exact “how-to” procedures may be contained in standard alone documents. Identify the location of auxiliary documents. <strong>What:</strong></td>
</tr>
<tr>
<td>Step 1</td>
<td><em>(emergency response priority sequence)</em></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>Return to normal operations</td>
<td>Describe the tests required to ensure that recovery is complete and business processes and functions are operating correctly.</td>
</tr>
</tbody>
</table>

**Restoring Normal Operations**

**Procedures for Recovering to Normal Operations**
Document the emergency response actions and associated procedures necessary to return to normal operating conditions after an incident has required the execution of the emergency response plan.

**Post-Mortem**
Assign a post-mortem team and schedule a post-mortem of the event with the business recovery team and impacted stakeholders.

**Plan Maintenance Procedures**
Plan Review and Update Process
Define responsibility for reviewing and maintaining the emergency response plan including: frequency, ownership, posting distribution requirements, etc. Implement a document management process. Provisions should be made for modifications to the plan to reflect any changes needed to correct deficiencies discovered during training sessions, testing and exercises. Additional testing should be done when changes are made to the plan.

Emergency Response Plan Distribution Procedures

Copies of the Emergency Response Plan need to be stored off-site, as well as provided to the key emergency response personnel. The document should be controlled to ensure updates and revisions are properly distributed. Designated document owners should maintain regular review cycles to manage updates. A copy of the plan should be kept with any emergency response “kits,” made available on emergency response PC’s, and stored at emergency response locations.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Revised by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reference Materials

Additional materials that support the emergency response plan

Identify additional information that is valuable or necessary as part of the emergency response plan, particularly materials which are subject to frequent change or update. Example: call lists, organization charts, etc.
Business Recovery Plan

The Business Recovery Plan should include a concise table of contents.

Overview

Plan Author(s) and Preparing Organization
Identify the author(s) of the plan and organization/application of the plan.

Recovery Strategy
Provide an overview of the recovery strategy that is supported by this recovery plan. In this section, you'll provide information about the priorities of functions, sites and personnel.

Recovery Plan Scope
Identify the recovery of the functions, services, or systems addressed in the document. Where applicable, reference the top business functions identified by your organization.

Clearly identify resources from internal groups that are required for your business recovery but not included in this document. This includes specific recovery steps that would be done by IT, software applications or other internal support teams. The plan may link to other more detailed business recovery plans (BRP). For example, a business group could have one group-level BRP that references five function-level BRPs, that in turn are tied to twenty-five process/application BRPs, and fifteen infrastructure emergency response plans (ERPs).

Structuring in this manner may help define the common elements at a group level. Specific recovery steps performed by separate teams would be addressed in more detailed BRPs. Recovery elements such as securing alternate workspace, will likely apply to all business functions, whereas the steps required to recover a particular function probably are unique. The template is designed to be used for each BRP. Content varies depending on the scope of what is covered.

Plan Objectives
This section contains clearly defined objectives of this recovery plan. The plan identifies which functions are recovered and the timing. Clear documentation is important, particularly for those persons unfamiliar with your environment. Document your steps in a way that assumes the key or critical staff members are NOT available to execute the plan.
Recovery Team
Define the team that will manage and execute recovery activities. Identify the primary and alternate recovery team members. Include members outside of the immediate organization teams, their roles, and contact information (work/home/pager). Determine who will maintain the team locator list and where it will be kept. Include names, addresses, phone numbers, and alternate contacts.

<table>
<thead>
<tr>
<th>Position</th>
<th>Primary</th>
<th>Alternate 1</th>
<th>Alternate 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name &amp; address</td>
<td>Name &amp; address</td>
<td>Name &amp; address</td>
</tr>
<tr>
<td></td>
<td>Work phone</td>
<td>Work phone</td>
<td>Work phone</td>
</tr>
<tr>
<td></td>
<td>Cell phone</td>
<td>Cell phone</td>
<td>Cell phone</td>
</tr>
<tr>
<td></td>
<td>Home phone</td>
<td>Home phone</td>
<td>Home phone</td>
</tr>
</tbody>
</table>

Communication Methods
Clearly identify how your team will communicate. You will need more than one option. Don’t assume cell phone service or local phones will work.

Recovery Team Roles and Responsibilities
Define expectations of all team members on the recovery team.

<table>
<thead>
<tr>
<th>Position</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Business Recovery Triggers

Recovery Time Objective (RTO) Requirements
Define when your business operations must be operational following an event. Clear requirements are essential. Determine if all business operations are required or only key segments. Identify the RTO for each business process.

Recovery Plan Authorization & Triggers
Identify who is authorized to initiate the plan, their alternate(s) and all detailed contact information. In addition, establish the business triggers which cause the plan to activate. Typically the business recovery plan is executed after the initial emergency response plans and crisis management teams have been activated. The triggers should be linked to the estimated time to repair the particular problem. Trigger examples: the time before a building can be occupied; the duration of a quarantine; the length of downtime predicted for key server; etc. For events that have significant impact such as the loss of a site for three plus months, the need to activate will be obvious. The real benefit to established triggers and the activation authorization is to have guidelines based on
business priorities and available data. It also establishes boundaries for times when activation is not as obvious. Activating the recovery plan (particularly if it means operations at an alternate site) often has real costs associated. Well-defined triggers will guide the decision making process. Link your triggers to the time before unacceptable business impact occurs. You may be able to do without some resources, such as email, if phones and faxes are operational.

<table>
<thead>
<tr>
<th>Triggers</th>
<th>Recovery Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of the outage – tie to the return to operations (RTO)</td>
<td>Name &amp; title of person(s) authorized to activate the recovery plan. Defined the roles &amp;</td>
</tr>
<tr>
<td>requirements listed in this plan.</td>
<td>responsibilities of the recovery team.</td>
</tr>
<tr>
<td>For example:</td>
<td>It’s better to list roles rather than names. In an emergency, the expected recovery</td>
</tr>
<tr>
<td>• core systems unavailable for more than X days;</td>
<td>team members may not be available and alternates may perform the roles.</td>
</tr>
<tr>
<td>• building unusable for Y days;</td>
<td></td>
</tr>
<tr>
<td>• site inaccessible for Z months.</td>
<td></td>
</tr>
</tbody>
</table>

Critical Recovery Information

Plan Execution Checklist - Sample
Edit this sample checklist to ensure your crisis teams can quickly and completely activate the plan. Define any additional activities that need to be included and remove the steps that don’t apply. In some cases you may want to include more procedural detail with each step.

Recovery plan execution is triggered appropriately
- links established with site chain of command and other emergency management teams involved in the crisis
- business recovery team convened
- links to crisis management team established

Crisis communications plan activated
- employee communications
- customer communications
- supplier communications
- other communications

Recovery procedures ready
- manual processes and workarounds implemented (if appropriate)
- recovery site necessary
- recovery site being prepared
- alternate work site(s) established
- travel and transportation arrangements secured
- keys, passwords and security codes available
- recovery equipment ordered
- data recovered via alternate site or from off-site records

Recovery site ready for use
- recovery equipment confirmed and inventoried
The SEMI Business Continuity Guideline for the Semiconductor Industry and its Supply Chain

- recovery equipment tested and loaded with software/data
- recovery readiness validated
- business users notified
- critical business processing resumed

**Return to normal business operations**
- shut down alternate site(s)
- document the damage assessment and recovery costs

**Recovery Priorities**
Define and document the recovery priorities for functions, applications, and infrastructure within the scope of the recovery plan. This will become the basis for recovery sequences and any necessary controlled shutdown situations. Recovery procedures and decisions should be guided by these agreed-upon priorities.

**Recovery Location**
Clearly identify where your team will assemble in the event of a crisis or disaster. Another work location should be included in the event you cannot enter the site.

**Job Descriptions**
Include job descriptions describing the key functions of your team members. In the event you need to hire additional personnel or replace team members, the job description can be used to assist in skill matching by HR or other assistance teams.

**Travel Coordination**
Define how your team will travel to recovery sites. If relocation requires travel, determine how airline tickets, hotels, and rental cars will be secured and the team member(s) responsible for the coordination. In the event of a local crisis, determine the method of pick up or transportation of team members.

**Off-site Storage Information**
Identify what is stored off-site, who is authorized to recall the information and the specific off-site contact information, account numbers, box numbers, and other pertinent information.

**Keys, Electronic Codes and Passwords**
In the event of a recovery or data restoration, keys, codes and passwords may be required in order to operate at an alternative site, or operate remotely. Ensure they are easily available. You may want to keep these keys in a secure location off-site. Passwords and codes may need to be listed in a separate document for security purposes.

**Vendors/Suppliers**
Identify vendors for the software and hardware utilized in business operations. Identify specific contract information and PO #’s as appropriate. Include vendor contact information required to obtain authorization, assistance, etc.
### Vendor/Supplier | Product/Service | PO # | Alternate Supplier
---|---|---|---
Name & address | | | Qualified alternate suppliers

### Recovery Procedures

Not all events will require the same level of business recovery. The plan should document the manual processes or work-arounds that may be used. Document all emergency response resources, equipment, materials, facilities, staff, applications, computing infrastructure, procedures, checklists, or documents, required for a successful emergency response of the department/team.

### Recovery Procedures for (group or function or process):
Complete a separate table for every recovery procedure documented in this plan.

<table>
<thead>
<tr>
<th>Purpose (who should perform the task, when, and why):</th>
<th>Purpose:</th>
<th>Who:</th>
<th>When:</th>
<th>Why:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>Identify all resources required to recover your business. Be specific, because this is what will be needed in order for your key business functions to continue to operate at an alternate site on borrowed/leased equipment. Staff, computers, forms, checks, cash, documentation, books, process documents, contacts, office supplies, data bases, web sites etc. resources, documentation, access/permission, keys, etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other resources and requirements</td>
<td>What are your critical dependencies? Are there other applications, servers, people, and documents that must be in place before you can begin processing again?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge and skills</td>
<td>Procedures, skill/knowledge, passwords, resource locations, recovery locations, etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery procedures:</td>
<td>Document the procedures or steps required and the order required. Exact “how-to” procedures may be contained in standard alone documents. Identify the location of auxiliary documents.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determine if recovery site is operational</td>
<td>Describe the tests to ensure that recovery is complete and business processes and functions are operating correctly in the recovery environment.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Normal Business Restoration

Criteria for Returning to Normal Operations
Once the emergency has passed and the normal business environments are available for use, the criteria to determine when to return the recovery operations to the normal location or environment must be defined. Identify the specific business recovery termination criteria that must be met before a normal business mode can begin. Identify at the organizational level who is authorized to initiate such procedures.

Normal Operations Startup

<table>
<thead>
<tr>
<th>Purpose (who should perform the task, when, and why):</th>
<th>Purpose:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Who:</td>
</tr>
<tr>
<td></td>
<td>When:</td>
</tr>
<tr>
<td></td>
<td>Why:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Resources, documentation, access/permission, keys, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Knowledge and skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Procedures, skill/knowledge, passwords, resource locations, recovery locations, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recovery procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document the procedures or steps required and the order required. Exact “how-to” procedures may be contained in standard alone documents. Identify the location of auxiliary documents.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery priority sequence.</td>
</tr>
</tbody>
</table>

| Step 2                                               |

| Step 3                                               |

Plan Maintenance Procedures

Plan Review and Update Process
Define responsibility for reviewing, maintaining, and updating the emergency response plan including: frequency, ownership, posting distribution requirements, etc. Implement a document management process. Provisions should be made for modifications to the plan to reflect any changes needed to correct deficiencies discovered during training sessions, testing and exercises. Additional testing should be done when changes are made to the plan.
Recovery Plan Distribution Procedures

Copies of the plan need to be stored off-site, as well as provided to the key emergency response personnel. The document should be controlled to ensure updates and revisions are properly distributed. Designated document owners should maintain regular review cycles to manage updates. A copy of the plan should be kept with any emergency response "kits," made available on emergency response PC’s, and stored at emergency response locations.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Revised by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reference Materials

Additional materials that support this recovery plan
Identify any additional information that will be valuable or necessary for the recovery plan, especially material that is subject to frequent change or update. examples: call lists, organization charts, etc.
**Drill Template**

**Design and Testing**

**Disaster Response and Business Recovery Plan Validation Overview**
A key step in Business Continuity Management (BCM) is validation of your disaster response and business recovery plans. Waiting until a crisis occurs to determine if your plans are appropriate is not an effective strategy. One of the best means of plan validation is through the use of drills.

There are several types of drills ranging from departmental desktop drills to full-blown integrated simulation drills that impact multiple groups including manufacturing and facilities. Your team should determine the best type of drill(s) based on your organization’s experience and BCM maturity.

**Designing the Drill**
Effective drills start with good planning. A single team comprised of individuals who are familiar with the disaster response plan (DRP) and business recovery plan (BRP) should be included in the drill development. Early in the planning process, the team should identify key stakeholders and engage all additional individuals that will be supportive with the drill design. The team should define drill objectives and assumptions, the success criteria, the specific drill scenario details, and all drill messages. Some considerations in your drill design:

- Establish and communicate the drill purpose, timeframe and any anticipated impact to groups that are involved. Departments such as production may need to know about the drill well in advance to make appropriate plans to ensure the drill does not cause business interruption.
- Include all decision makers and their alternates in the drills. It is important to train the alternates. This may require multiple iterations of the drill. You will not be able to predict who will be available during a real crisis. Teams may also be active many days, requiring multiple shifts.
- Review the drill logistics well in advance, including conference rooms and phone bridges.
- Schedule the drill in advance for all necessary participants and their alternates. An exception to this rule might apply if the drill objective is to create a more realistic crisis event where the element of surprise is required.
  - Drills that are not announced in advance provide an excellent means of testing your activation processes and validation of the contact information contained within the plan.
Success criteria for the drill include key learning’s. Identify what worked and what did not. Gaps between the plan and the implementation are to be expected as a result of a drill. Once identified, these gaps can be addressed and solutions identified prior to the crisis.

When designing the drill, determine with your design team how much data and background information to provide prior to the drill. A balance must be established in order to maintain a sense of reality.

Establish a balance between the maturity of the group and what will be tested.

Additional items to consider are included in the drill-planning checklist.

**Drill Planning Checklist**

- Communicate the drill purpose, timeframe and impact to manufacturing and other groups that have a need to know (i.e. IT, facilities.)
- Design your drill based on the experience and the skill set of the team.
  - if drills are new to the participants, keep the first tabletop drill simple
  - drill coordinators should be able to “think on their feet” and be familiar with the plans to help the group navigate through the drill
- Design the drill so that you involve all your key managers and the response team leaders.
- Leverage individuals who are knowledgeable about your organization and have a good imagination to help script the drill scenario.
- Utilize drill scenarios that have already been scripted and adjust them to fit your organization.
- Ensure that your organization has an accurate contact list containing information on how to contact your key individuals. Include work phone, cell phone, pager, email, and home phone.
- Ensure that you have clearly-identified roles and responsibilities for all drill participants.
- Cover the logistics well in advance – rooms, communications, etc.
- Schedule the drill for all necessary participants and their alternates.
- When multiple locations are involved, plan for communication between sites.
- Set the success criteria for the drill prior to the exercise and share the expectations with all participants.
- Schedule observers who are familiar with the business operations, the DRP/BRP and/or drill processes. There should be at least one observer available for every team that will be activated in the drill.
- Clearly communicate to drill participants that the intent is not to determine how accurate the scenario is, but to focus on the team response to the crisis.
- If the drill is large (involving multiple groups and sites) you may want to have a reactive question and answer document prepared by your Public Affairs group. This will be particularly helpful if the drill involves outside agencies such as local fire or police departments.
- Brief local authorities prior to the exercise if the drill is large or activities will be visible from outside of the buildings (i.e. large scale evacuation or mock chemical spill) to prevent unnecessary panic, alarm, or issues.
Drill Frequency

The number of drills your group needs depends on the complexity of the business and the current level of preparedness within the organization. In general, plan at least one major integrated drill for each core business function per year, and two shorter, more focused desktop drills. The actual number of drills your group needs will vary depending upon several factors:

- **Maturity** - if BCM is relatively new, your group will need to conduct several smaller drills before staging an all-encompassing integrated drill.
- **Familiarity** - the level of familiarity with your organization’s DRP and BRP and the participants knowledge of their roles will determine drill frequency.
- **Change** - when your organization has implemented new systems, changed applications, or business operations, drills may be required to re-validate the plan.
- **If you’ve successfully weathered a major crisis in your organization, you may choose to postpone a drill or use the drill to test another area that was identified for improvement.**
Execution

Pre-Drill Steps

- To avoid unintentional interruption, concern and confusion, inform everyone participating of the drill, as well as those potentially affected.
  - all internal and external communications (such as press releases and notices to employees) should clearly state that the activity is only a drill. Clearly state the drill objectives.
- Participants in the drill may need to notify colleagues, customers, etc. to avoid panic and rumors.
- Brief all participants involved in the drill on the drill objectives, the success criteria, the role of the drill observers and all additional drill essentials.
- Ensure that all participants know the rules of engagement, the roles they are expected to play, the process, and any pre-work.
- Inform all participants that if a real emergency occurs during any phase of the drill, the drill will be stopped.

Drill Initiation

- Initiate the drill by implementing the plan activation process. This will provide an opportunity to test this aspect of the plan.
  - to test the activation process separately, you may choose to pre-schedule the drill activation approximately 10 to 15 minutes prior to the drill start time, and once completed, restart the drill.

After the Drill: Assessing what went well and what didn’t

To drive effective closure on the drill, discuss the activity with all of the participants and capture all the lessons learned and suggestions.

- Input should be documented and incorporated into the DRP and/or BRP.
- Gather the input from the drill participants immediately following the end of the drill.
- Meet with drill observers and drill coordinator to discuss comments and inputs from the drill.
- Action items identified should be tracked until closure.

Note: A team’s ability to function effectively during a crisis improves with practice. Don’t be discouraged if your first drill or two seem a bit shaky. Consider it a good learning experience and factor those learnings into the next drill.
Scenario and Scripting Template

Drill Date: ________________________________

Scenario Name: _____________________________

Items to consider including in your Drill Scenario:

- Initiating chain of command (COCA) notification
- Setting priorities
- Safety issues
- Injury / Fatality
- External agencies/authorities
- Utility systems
- Repair/replacement time
- Financing
- Resources
- Employee impact
- Customer impact
- Damaged equipment
- Destroyed equipment
- Product disposition
- Finance advice
- Other business impacts
- Media
- Site security
- Employee, employee family member issues
- Securing resources / supplies food service
- Clean up
- Logistic and materials commitments

Drill Scenario Design Team:
List the names of the individuals who developed the drill scenario

<table>
<thead>
<tr>
<th>Department</th>
<th>Individual</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identify areas as suggested in the table below:

<table>
<thead>
<tr>
<th>Plan Area</th>
<th>Plan Information</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Disaster scenario</td>
<td>Describe the scenario briefly</td>
<td></td>
</tr>
<tr>
<td>2 Scenario details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Immediate issues</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Artificial assumptions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 In scope</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>6 Out of scope</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>7 Initial briefing communication</td>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>

**Scenario Participant List**

This chart may be used to identify the positions and names of primary and alternate individuals for the drill. The positions may vary depending upon your organization’s business structure and needs.

<table>
<thead>
<tr>
<th>Position</th>
<th>Primary</th>
<th>Alternate</th>
</tr>
</thead>
<tbody>
<tr>
<td>COCA director</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COCA scribe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency operations manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public affairs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Materials/Purchasing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Building services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EHS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Initial Assessment

Example:

Event Details: Describe the initial event that has occurred. The following sample demonstrates the possible scripting of a drill.

First hour  COCA director requests an update from all groups on impacts and issues noted.

13:10  Production floor systems indicated alerts and errors related to network connectivity problems. Connectivity failures started at different lines (same modules at different lines), but was quickly spread across the lines and new modules started to show same network issues.

13:30  It was confirmed the networking problems were impacting all production floor areas at the site.

13:55  Check-in from all office areas received; IT confirmed network problems across the entire site.

Second hour  COCA director requests an update from all groups on impacts and issues noted over the last hour.

Third hour  COCA director calls for an update from all groups on impacts and issues noted as well as an update on actions over the last hour.

Fourth hour  COCA director calls for an update from all groups on impacts and issues noted as well as an update on actions over the last hour.
**Master Scenario Script Events**

*Develop various messages you want to interject throughout your drill to help test your plans. It is important to understand the expected response. The table is to be used by the Drill Design Team and the Drill Coordinator. At the time of the event, messages may be sent via email, phone or as a written text message given to the intended group. You may want to create more messages than you think will be necessary. Some drills will go smoothly providing groups the opportunity to handle more information during the actual drill.*

<table>
<thead>
<tr>
<th>Time</th>
<th>Sender</th>
<th>Receiving Group</th>
<th>Message</th>
<th>Expected Response Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Assessment Template

Event title: __________________________________________

Site(s) involved: _________________________________

Date of drill : _________________________________

Duration of event: _________________________________

Objective:

Example: To identify and document key learnings (both positive and negative) in order to provide feedback to the disaster response plan and/or business recovery plan.

Drill Scenario

(brief statement describing the drill scenario)

Drill Root Cause:

(brief statement identifying the primary cause of the event)

Impact:

•

•

•

Roles / Attendees:

<table>
<thead>
<tr>
<th>Roles / Attendees</th>
<th>Event owner</th>
<th>(name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilitator (if applicable)</td>
<td>(name)</td>
<td></td>
</tr>
<tr>
<td>Scribe (if applicable)</td>
<td>(name)</td>
<td></td>
</tr>
<tr>
<td>Attendees</td>
<td>(name)</td>
<td></td>
</tr>
<tr>
<td>Observers</td>
<td>(name)</td>
<td></td>
</tr>
<tr>
<td>Etc</td>
<td>(name)</td>
<td></td>
</tr>
<tr>
<td>....</td>
<td>(name)</td>
<td></td>
</tr>
<tr>
<td>....</td>
<td>(name)</td>
<td></td>
</tr>
<tr>
<td>What went right?</td>
<td>Actions: (list corresponding activity that should be repeated)</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>•</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What went wrong?</th>
<th>Corrections: (list corresponding actions, improvements, processes, and modifications needed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key Learnings:</th>
<th>list items learned from the event</th>
</tr>
</thead>
<tbody>
<tr>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change Control:</th>
<th>Was this the result of a change in the scenario?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Did the change go through change control?</td>
</tr>
<tr>
<td></td>
<td>If not, should it have?</td>
</tr>
<tr>
<td></td>
<td>Were changes made during the event that needed to go through change control?</td>
</tr>
<tr>
<td></td>
<td>Was this a crisis?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Timeline</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>mm/dd/yy</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AR #</th>
<th>Owner</th>
<th>Due Date</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>mm/dd/yy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process Improvements</th>
<th>Key Objectives</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>mm/dd/yy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Identified Gap / Issue Tracking Form

**Operation:** ________________________________

**Drill lead by:** ________________________________

**Date of drill:** xx/xx/xx_________________________

Observer(s) may use this form to capture gaps/issues and track the items to closure.

<table>
<thead>
<tr>
<th>Item</th>
<th>Gap/Issue</th>
<th>Owner</th>
<th>Closure Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E1.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E2.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E2.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E2.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E2.4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E3.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E3.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E3.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misc.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misc.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misc.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process 4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>