<FACILITY/SYSTEM>
CONTINGENCY PLAN

Version ***<number>***
<Date submitted>

Submitted to:

Submitted By:

<Facility name>
<Facility address>
<Facility address>
<Facility address>

Table of Contents

1 EXECUTIVE SUMMARY

Written upon completion of document. Contains introductory descriptions from all sections.

2 INTRODUCTION

This document contains the Contingency Plan for the <Facility/System>. It is intended to serve as the centralized repository for the information, tasks, and procedures that would be necessary to facilitate the <Facility/System> management's decision-making process and its timely response to any disruptive or extended interruption of the department's normal business operations and services. This is especially important if the cause of the interruption is such that a prompt resumption of operations cannot be accomplished by employing only normal daily operating procedures.

In terms of personnel and financial resources, the information tasks and procedures detailed in this plan represent the <Facility/System> management's demonstrated commitment to response, resumption, recovery, and restoration planning. Therefore, it is essential that the information and action plans in this plan remain viable and be maintained in a state of currency in order to ensure the accuracy of its contents. To that end, this introduction is intended to introduce and familiarize its readers with the organization of the plan.

It is incumbent upon every individual who is in receipt of the <Facility/System> Contingency Plan, or any parts thereof, or who has a role and/or responsibility for any information or materials contained in the document, to ensure that adequate and sufficient attention and resources are committed to the maintenance and security of the document and its contents.

Since the information contained in this document describes <Facility/System> management's planning assumptions and objectives, the plan should be considered a sensitive document. All of the information and material contents of this document should be labeled, "Limited Official use".

The <Facility/System> management has recognized the potential financial and operational losses associated with service interruptions and the importance of maintaining viable emergency response, resumption, recovery and restoration strategies.

The <Facility/System> Contingency Plan is intended to provide a framework for constructing plans to ensure the safety of employees and the resumption of time-sensitive operations and services in the event of an emergency (fire, power or communications blackout, tornado, hurricane, flood, earthquake, civil disturbance, etc.)

Although the <Facility/System> Contingency Plan provides guidance and documentation upon which to base emergency response, resumption, and recovery planning efforts, it is not intended as a substitute for informed decision-making. Business process managers

and accountable executives must identify services for which disruption will result in significant financial and/or operational losses. Plans should include detailed responsibilities and specific tasks for emergency response activities and business resumption operations based upon pre-defined time frames.

Constructing a plan and presenting it to senior management may satisfy the immediate need of having a documented plan. However, this is not enough if the goal is to have a viable response, resumption, recovery, and restoration capability. In order to establish that capability, plans, and the activities associated with their maintenance (i.e. training, revision, and exercising) must become an integral part of <Name> *operations.*

A Contingency Plan is not a one-time commitment and is not a project with an established start and end date. Instead, a Contingency Plan is an on-going, funded business activity budgeted to provide resources required to:

- *Perform activities required to construct plans*
- *Train and retrain employees*
- *Develop and revise policies and standards as the department changes*
- *Exercise strategies, procedures, team and resources requirements*
- *Re-exercise unattained exercise objectives*
- *Report on-going continuity planning to senior management*
- *Research processes and technologies to improve resumption and recovery efficiency*
- *Perform plan maintenance activities*

Developing a Contingency Plan that encompasses activities required to maintain a viable continuity capability ensures that a consistent planning methodology is applied to all of the <Facility or Systems>. Contingency Plan elements necessary to create a viable, repeatable and verifiable continuity capability include:

- *Implementing accurate and continuous vital records, data backup, and off-site storage*
- *Implementing capabilities for rapid switching of voice and data communication circuits to alternate site(s)*
- *Providing alternate sites for business operations*
- *Constructing a contingency organization*

- *Implementing contingency strategies*

2.1 PURPOSE

The purpose of this plan is to enable the sustained execution of mission critical processes and information technology systems for <Facility/System> in the event of an extraordinary event that causes these systems to fail minimum production requirements. The <Facility/System> Contingency Plan will assess the needs and requirements so that <Facility/System> may be prepared to respond to the event in order to efficiently regain operation of the systems that are made inoperable from the event.

2.2 SCOPE

Insert information on the specific systems, locations, Facility divisions, technical boundaries and physical boundaries of the <Facility/System> Contingency Plan.

2.3 PLAN INFORMATION

The Contingency Plan contains information in two parts related to the frequency of updates required. The first part contains the plan's ***static information*** *(i.e. the information that will remain constant and will not be subject to frequent revisions). The second part contains the plan's* ***dynamic information*** *(i.e. the information that must be maintained regularly to ensure that the plan remains viable and in a constant state of readiness). This dynamic information is viewed as the action plan. The action plan should be considered a living document and will always require continuing review and modification in order to keep up with the changing <facility/system> environment.*

The static information part of the Contingency Plan is contained in a MS-Word file and printed as part of this document. This static information should be read and understood by all employees, users, and administrators of the <Facility/System>, or at least by those individuals who are involved in any phase of business response, resumption, recovery, or restoration.

The dynamic information resides in the database of the <System Name> and will be printed as output for the appendixes of this document. By using the database, dynamic information that is vital to the survival of the <Facility/System> will be easy to manage and update. The web-enabled database is designed for maintenance of personnel contact lists, emergency procedures, and technical components. It is already in operation for <Name> agencies.

For ease of use and reference, the static and dynamic information is maintained separately. While it is necessary to be familiar with the static information during resumption, it should not be necessary to read that information at the time of the event. The completed action plan of dynamic information provides all of the necessary lists, tasks, and reports used for response, resumption, or recovery.

3 CONTINGENCY PLAN OVERVIEW

3.1 APPLICABLE PROVISIONS AND DIRECTIVES

The development of the <Facility/System> Contingency Plan is required by executive decisions and to meet regulatory mandates. The <Facility/System> management must maintain an information assurance infrastructure that will ensure that its information resources maintain availability, confidentiality, integrity, and non-repudiation of its data. Furthermore, <Facility/System> management must ensure their strategic information resources management capabilities. Therefore, the <Facility/System> Contingency Plan is being developed in accordance with the following executive decisions, regulatory mandates, provisions, and directives:

- *Office of Management and Budget Circular A–130, Revised (Transmittal Memorandum No. 4), Appendix III, Security of Federal Automated Information Resources, November 2000.*
- *Computer Security Act of 1987, Public Law 100-235, January 1988.*
- *Presidential Decision Directive 63, Critical Infrastructure Protection, May 1998.*
- *Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998.*
- *Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 1988.*
- *Federal Information Processing Standards (FIPS) Publication 87, Guidelines for ADP Contingency Planning, March 1981.*
- *DOJ Order 2640.2D, Information Technology Security, July 12, 2001.*

The <Facility/System> Contingency Plan is designed to be in accordance with the strategic intent of the<Name> and the <Name>'s functional and operational mission.

3.2 OBJECTIVES

The <Facility> is dependent on the variety of systems classified as General Support Systems (GSSs), which provide mission critical functions of connectivity, Internet access, and email, or Major Applications (MAs) which are specific software programs written to produce output to fulfill the <Facility's> service to its customers or enable the <Facility/System> to operate. In addition these systems provide the means to offer electronic government (e-government). Although many threats and vulnerabilities can be mitigated, some of the threats cannot be prevented. Therefore, it is important that <Facility/System> develop contingency plans and disaster recovery plans to ensure the uninter-

rupted existence of its business functions and continued service to the<Name> and the public.

The primary focus of a contingency plan revolves around the protection of the two most important assets of any organization: personnel and data. All facets of a contingency plan should address the protection and safety of personnel and the protection and recovery of data. The primary objective of this plan is to establish policies and procedures to be used for information systems in the event of a contingency to protect and ensure functioning of those assets. This includes establishing an operational capability to process pre-designated critical applications, recovering data from off-site backup data sets, and restoring the affected systems to normal operational status. The plan seeks to accomplish the following additional objectives:

- *Minimize the number of decisions which must be made during a contingency*
- *Identify the resources needed to execute the actions defined by this plan*
- *Identify actions to be undertaken by pre-designated teams*
- *Identify critical data in conjunction with customers that will be recovered during the Hot Site phase of recovery operations*
- *Define the process for testing and maintaining this plan and training for contingency teams*

3.3 ORGANIZATION

In the event of a disaster or other circumstances which bring about the need for contingency operations, the normal organization of the <Facility> will shift into that of the contingency organization. The focus of the <Facility/System> will shift from the current structure and function of "business as usual" to the structure and function of an <Facility/System> working towards the resumption of time-sensitive business operations. In this plan, the <Facility/System's> contingency organization will operate through phases of response, resumption, recovery, and restoration. Each phase involves exercising procedures of the <Facility/System> Contingency Plan and the teams executing those plans. The teams associated with the plan represent functions of a department or support functions developed to respond, resume, recover, or restore operations or facilities of the <Facility/System> and its affected systems. Each of the teams is comprised of individuals with specific responsibilities or tasks, which must be completed to fully execute the plan. Primary and alternate team leaders, who are responsible to the plan owner, lead each team.

Each team becomes a sub-unit of the <Facility's> contingency organization. Coordination teams may be singular for the <Facility>, whereas technical teams will likely be system specific. Figure 3-1, Contingency Planning Organizational Chart, shows the base

organizational structure. The teams are structured to provide dedicated, focused support in the areas of their particular experience and expertise for specific response, resumption and recovery tasks, responsibilities, and objectives. A high degree of interaction among all teams will be required to execute the corporate plan. Each team's eventual goal is the resumption/recovery and the return to stable and normal business operations and technology environments. Status and progress updates will be reported by each team leader to the plan owner. Close coordination must be maintained with <system> and <Name> management and each of the teams throughout the resumption and recovery operations.

The <Facility/System> contingency organization's primary duties are:

- *To protect employees and information assets until normal business operations are resumed.*
- *To ensure that a viable capability exists to respond to an incident.*
- *To manage all response, resumption, recovery, and restoration activities.*
- *To support and communicate with employees, system administrators, security officers, and managers.*
- *To accomplish rapid and efficient resumption of time-sensitive business operations, technology, and functional support areas.*
- *To ensure regulatory requirements are satisfied.*
- *To exercise resumption and recovery expenditure decisions.*
- *To streamline the reporting of resumption and recovery progress between the teams and management of each system.*

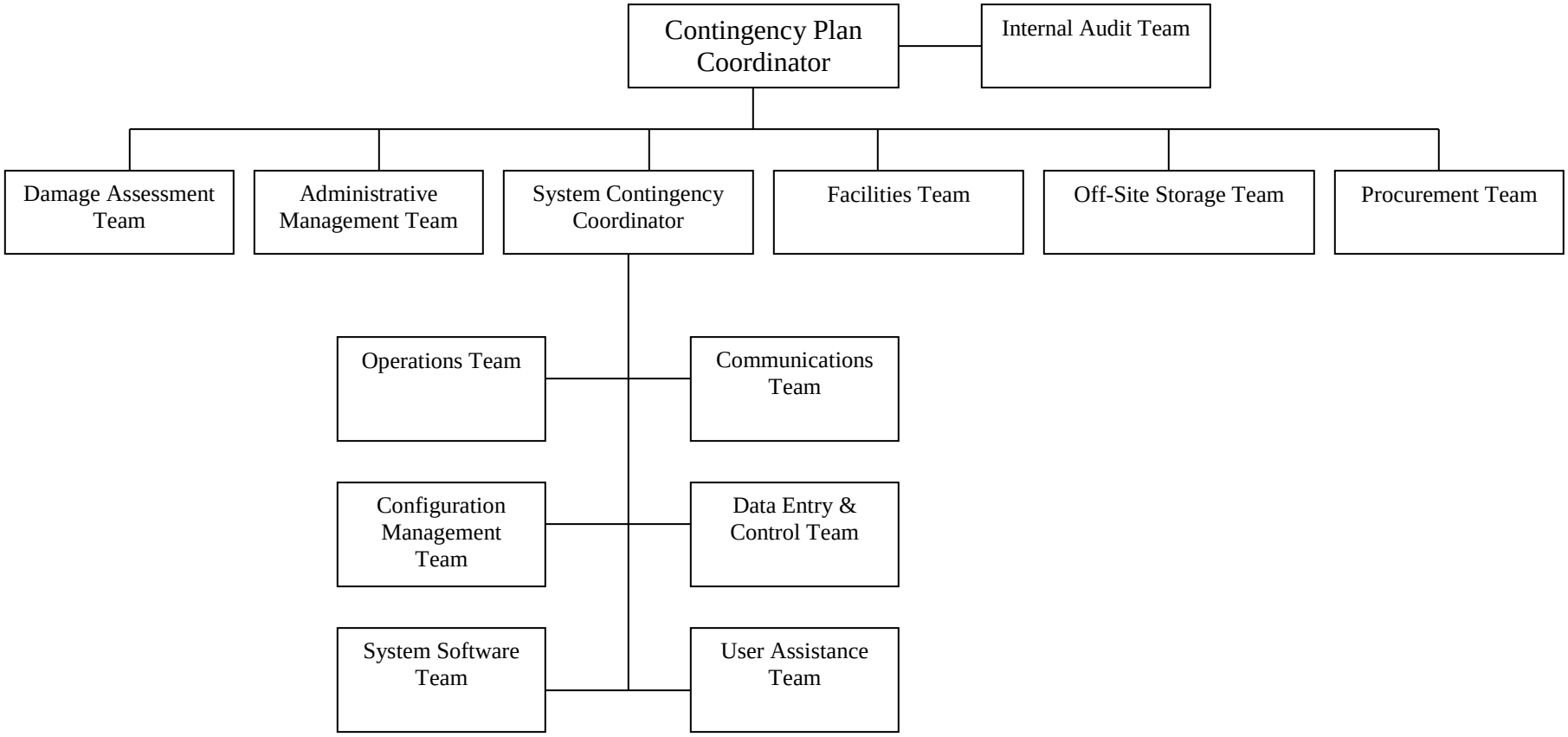

Figure 3-1 Contingency Planning Organizational Chart

3.4 CONTINGENCY PHASES

The <Facility/System> Contingency Plan Coordinator, in conjunction with <Facility/System> and <Name> *management will determine which Teams/Team members are responsible for each function during each phase. As tasking is assigned, additional responsibilities, teams, and task lists need to be created to address specific functions during a specific phase.*

3.4.1 RESPONSE PHASE

- *To establish an immediate and controlled <system> presence at the incident site.*
- *To conduct a preliminary assessment of incident impact, known injuries, extent of damage, and disruption to the <system's> services and business operations.*
- *To find and disseminate information on if or when access to the <system's> facility will be allowed.*
- *To provide <system> management with the facts necessary to make informed decisions regarding subsequent resumption and recovery activity.*

3.4.2 RESUMPTION PHASE

- *To establish and organize a management control center and headquarters for the resumption operations.*
- *To mobilize and activate the support teams necessary to facilitate and support the resumption process.*
- *To notify and appraise time-sensitive business operation resumption team leaders of the situation.*
- *To alert employees, vendors and other internal and external individuals and organizations.*

3.4.3 RECOVERY PHASE

- *To prepare and implement procedures necessary to facilitate and support the recovery of time-sensitive business operations.*

- *To coordinate with higher headquarters to discern responsibilities that will fall upon <system> Business Operations Recovery Teams and Technology Recovery Teams*

- *To coordinate with employees, vendors, and other internal and external individuals and organizations.*

3.4.4 RESTORATION PHASE

- *To prepare procedures necessary to facilitate the relocation and migration of business operations to the new or repaired facility.*

- *Implement procedures necessary to mobilize operations, support and technology department relocation or migration.*

- *Manage the relocation/migration effort as well as perform employee, vendor, and customer notification before, during, and after relocation or migration.*

3.5 ASSUMPTIONS

Include any assumptions that the Contingency Plan will hinge on. This could range from absolutely necessary conditions to helpful information in support of the contingency plan phases.

- *Telecommunications connectivity and fiber optic cabling will be intact and provided by General Services Administration (GSA).*

- *That all necessary Memorandums of Agreement (MOAs) and Memorandums of Understanding (MOUs) have been executed.*

3.6 CRITICAL SUCCESS FACTORS AND ISSUES

This section addresses the factors and issues that specifically apply to the <Facility/System> Contingency Plan project that have been identified to be critical to the successful implementation of the Contingency Plan. These factors are as follows:

- *Absolute commitment by senior management to Contingency Planning and Disaster Recovery.*

- *Budgetary commitment to Disaster Recovery.*

- *Modifications and improvements to the current scheduling procedures for the retention and transportation of back up files to the offsite storage facility.*

- *Development and execution of the necessary Memorandums of Agreement (MOAs), Memorandums of Understanding (MOUs), and Service Level Agreements (SLAs).*

- *Completion of requirement assessment for, and then completion of the procurement of a diesel generated alternate power source.*

3.7 MISSION CRITICAL SYSTEMS/APPLICATIONS/SERVICES

The following essential mission critical systems/applications/services that must be recovered at the time of disaster in the following order due to critical interdependencies:

<Facility/System> has identified the applications and services shown in Figure 1.2 as mission critical:

SYSTEMS ACRONYM	SYSTEM NAME
Exchange Mail	*Microsoft E-mail system*
Internet Connectivity	*UUNet*

Figure 3-2 Mission Critical Systems

3.8 THREATS

When developing strategies for a contingency plan, it is helpful to consider the entire range of probable and possible threats that present a risk to an organization. From that range of threats, likely scenarios can be developed and appropriate strategies applied. A disaster recovery plan should be designed to be flexible enough to respond to extended business interruptions, as well as major disasters.

The best way to achieve this goal is to design a contingency plan that could be used to address a major disaster, but is divided into sections that can be used to address extended business interruptions. While each of the identified threats could result in a disaster by itself, in a major disaster several of the threats might be present concurrently or occur sequentially, depending on the circumstances.

As a result, it is advisable to develop several levels of strategies that can be applied as needed. For example, a localized fire in the computing center may render some of that space unusable. An appropriate strategy for that event may be temporary relocation of personnel to another office within <Name> headquarters or in other suitable local office space in another office building or hotel. An event that required temporary evacuation of the computer center, such as a truck accident in the tunnel and a chemical spill that may require several days to resolve, may necessitate switchover capabilities and possible regional mirrored redundancy capabilities that would be transparent to the users. An event of greater magnitude, such as an explosion, may render the <Name of headquarters or national office> unusable for an extended duration of time and might necessitate a strategy based on mirrored redundancy as well as a secondary strategy involving a commercial hot site. Time sensitivity and mission criticality in conjunction with budgetary limitations, level of threat and degree of risk will be major factors in the development of recommended strategies. (See § 6 for Recommended Strategies)

3.8.1 PROBABLE THREATS

The table depicts the threats most likely to impact the <Facility> and components of <systems> and their management. The specific threats that are represented by (XX) are considered the most likely to occur within the <system> environment.

PROBABILITY OF THREATS			
Probability of Occurrence:	**High**	**Medium**	**Low**
Air Conditioning Failure		***X***	
Aircraft Accident			***X***
Blackmail		***X***	
Bomb Threats		***X***	
Chemical Spills / HazMat	***X***		
Cold / Frost / Snow			***X***
Communications Loss		***X***	
Data Destruction		***X***	
Earthquakes			***X***
Fire	***XX***		
Flooding / Water Damage			***X***
Nuclear Mishaps			***X***
Power Loss / Outage	***XX***		
Sabotage / Terrorism		***X***	
Storms / Hurricanes			***X***
Vandalism / Rioting		***X***	

Figure 3-3 *<System>*: Risk Analysis Matrix

4 SYSTEM DESCRIPTION

In this section include information for each system under ownership or controlling authority of the <Facility/System>. Controlling authority assumes that a function or mission element of a Facility/System has been contracted to an outside entity that provides the facilities, hardware, and software and personnel required to perform that task. <Name> and the Facility retain the oversight of that operation and therefore are the controlling activity for that system.

4.1 PHYSICAL ENVIRONMENT

Include the building location, internal facilities, entry security measures, alarms, and access control.

4.2 TECHNICAL ENVIRONMENT

Include accurate description of hardware (processors, memory, media storage) and system software (operating system, applications). Include number of users, interconnected systems, and operational constraints.

Put specific software and hardware inventories, SLAs, vendor contacts in appendixes.

5 PLAN

5.1 PLAN MANAGEMENT

5.1.1 CONTINGENCY PLANNING WORKGROUPS

The development of recovery strategies and work-arounds require technical input, creativity, and pragmatism. The best way to create workable strategies and cohesive teams that leverage out-of-the-box thinking is to involve management and information resource management personnel in an ongoing informative dialogue. The <Facility/System Name> management has developed and is facilitating Contingency Planning workgroups to assist in the development and review of strategies, teams, and tasks.

5.1.2 CONTINGENCY PLAN COORDINATOR

A coordinator and an alternate should be appointed by <Facility> management and system owners to monitor and coordinate the <Facility/System> Contingency Plan, training and awareness, exercises, and testing. Additionally, this person will coordinate strategy development with Contingency Planning Workgroups, System Contingency Coordinator, Team Leaders, Business Process Owners, and Management. The Contingency Planning Coordinator should work closely with system technical managers to ensure the viability of the <Facility/System> Contingency Plan. The Contingency Plan Coordinator will manage contingency teams that are not system specific (see section 5.2). It is recommended that the individual(s) appointment(s) be documented in writing, and that specific responsibilities be identified and included in their job descriptions.

5.1.3 SYSTEM CONTINGENCY COORDINATORS

A coordinator and an alternate should be appointed for EACH SYSTEM under ownership or controlling authority of the <Facility/System> by <Facility> management and system owners. Their primary task will be to monitor and coordinate the <Facility/System> contingency planning, training and awareness, exercises, and testing. Additionally, this person will manage contingency teams (see Section 5.2) that are assigned specifically to their system and report directly to the Contingency Plan Coordinator. It is recommended that the individual(s) appointment(s) be documented in writing, and that specific responsibilities be identified and included in their job descriptions.

5.1.4 INCIDENT NOTIFICATION

The facilities managers for the locations where the critical components of the <Facility's> systems are located should be provided with the telephone numbers of <Facility/System> Emergency Response Team members. Upon notification, the team will meet in (TBD) for the purpose of conducting initial incident assessment and issuing advisory reports of status to the <Facility/System> and <Name> management. If the facilities manager, emergency response personnel, or <Facility> Emergency Response Team Leader has determined that the building cannot be entered, the alternate meeting place will be the (TBD).

5.1.5 INTERNAL PERSONNEL NOTIFICATION

The <Facility/System's> "Emergency Notification" procedure, or a modified version thereof, should be developed and used for notification of the Crisis Management Team and other Disaster Recovery Teams regarding specific response actions taken during response operations. Within the "personal contact" database, a single source personal information table should readily available that includes home addresses, contact telephone phone numbers, and emergency contact information. In the event of a disaster, a lack of specific personal data, including home addresses, cell phone numbers, pager numbers, and alternate contact information, could result in the inability to locate and contact key personnel and team members. This automated personnel database should be maintained and updated continuously. This database may be maintained internally or somewhere else within the department, as long as the information contained therein remains current and accessible.

5.1.6 EXTERNAL CONTACT NOTIFICATION

The <Facility/System's> "Emergency Notification" procedure, or a modified version thereof, should be developed and used for notification of its Contingency Plan service providers, <Name> agencies, external contacts, vendors, suppliers, etc.

5.1.7 MEDIA RELEASES

All incident related information (printed or spoken), concerning the <Name> will be coordinated and issued through the Department or Component Office of Public Affairs (OPA).

5.1.8 ALTERNATE SITE (S)

Include location of pre-positioned Information Technology Assets for activation in a contingency operation mode. It is suggested that local sites for facility-/system-specific contingencies be maintained, such as a "Tech Hotel," where the contingency planner rents space and information technology equipment.

Additional local alternatives could be in the form of reciprocating MOAs and/or MOUs with *<Name>* or other Federal agencies for the utilization of space for the installation of equipment, connectivity infrastructure and personnel accommodations should the need arise.

An alternate site with a distance of at least 100 miles should be considered. Should a regional event take place that renders Facility systems ineffective and the inability for physical access, a relocation site would serve the needs for contingency operations.

5.2 TEAMS

The following are suggested teams that will be assigned to execute the contingency plan: Some teams may not be necessary depending on the system. If this is the case you should simply remove the heading and table. Certain teams will be replicated for each system and placed under the System Contingency Coordinator given the vast differences in hardware, software, and external communications for each system. Each team will have a roster and task list of actions and responsibilities generated by the IMS database to be included in an appendix.

5.2.1 DAMAGE ASSESSMENT TEAM

The Damage Assessment Team is a technical group responsible for assessing damage to the Facility/System and its components. It is composed of personnel with a thorough understanding of hardware and equipment and the authority to make decisions regarding the procurement and disposition of hardware and other assets. This team is primarily responsible for initial damage assessment, accounting of damage assessment, loss minimization, salvage and procurement of necessary replacement equipment and interfaces. This team should include vendor representatives.

The Damage Assessment Team will enter the facility as soon as they have received permission to do so from emergency services. A written detailed account should be made of the general status of the work area, with specific attention to the condition of hardware, software, furnishings, and fixtures. Recommendations should be made that all damaged equipment, media, and documentation be routed immediately to disaster recovery and restoration experts for a determination as to its ability to be salvaged or restored.

5.2.2 OPERATIONS TEAM

The Operations Team consists of operators responsible for running emergency production for critical systems, coordinating with Backup Team to ensure that applications system data and operating instructions are correct, and with the Liaison Team to advise of the production status and any unusual problems requiring assistance. Data Input/Control Teams could be separate groups or subgroups of the Operations Team. Also, the PC Support Team under the Operations Recovery Team is responsible for re-establishing microcomputer operations at the backup site or remote sites and for assisting with reinstating PC applications.

5.2.3 COMMUNICATIONS TEAM

The Communications Team is composed of <Facility/System's> communications specialists responsible for restoring voice, data, and video communications links between users and the computers, regardless of location in the event of a loss or outage. Communication vendor (carrier) input in designing and implementing the recovery plan is very important. Influential factors in developing recovery procedures for this team include: the type of network, the time requirement for restoration, percentage of the network to be recovered, and budget considerations.

5.2.4 DATA ENTRY AND CONTROL TEAM

The Data Entry and Control Team is responsible for entering data as it is restored. They ensure that the data is the best available backup and meets validation for the system.

5.2.5 OFF-SITE STORAGE TEAM

The Off-site Storage Team is responsible for retrieving backup copies of operating systems applications, systems, applications data, and ensuring security of the data, backup facilities, and original facilities. The team is composed of members of <Facility/System> familiar with vital records archival and retrieval.

5.2.6 ADMINISTRATIVE MANAGEMENT TEAM

The Administrative Management Team coordinates Primary and Alternate Site security and specialized clerical and administrative support for the Contingency Plan Coordinator and all other teams during disaster contingency proceedings. The Administrative Team may also assist groups outside the information resources area as needed. The Administrative Team is responsible for reassembling all documentation for standards, procedures, applications, programs, systems, and forms, as required at the backup site. The Administrative Team is responsible for arranging for transportation of staff, equipment, supplies, and other necessary items between sites.

5.2.7 PROCUREMENT TEAM

The Procurement Team consists of persons knowledgeable of the information resources and supplies inventory and the budgetary, funding, and acquisition processes responsible for expediting acquisition of necessary resources.

5.2.8 CONFIGURATION MANAGEMENT TEAM

The Configuration Management Team is composed of individuals with teleprocessing skills. They work closely with the Communications Teams in establishing voice and data communication capabilities.

5.2.9 FACILITIES TEAM

The Facilities Team is responsible for arranging for the primary and backup facilities and all components.

5.2.10 SYSTEM SOFTWARE TEAM

The System Software Team consists of system software programmers responsible for providing the system software support necessary for production of critical applications systems during recovery.

5.2.11 INTERNAL AUDIT TEAM

The Internal Audit Team is responsible for observation and oversight participation in the recovery effort.

5.2.12 USER ASSISTANCE TEAM

The User Assistance team is composed of individuals with application use knowledge. The team is made up of major user area managers, production control, and applications lead analysts responsible for coordination and liaison, with the information resources staff for applications recovery and restoration of data files and databases. Under the general leadership of the User Assistance Team, technical applications specialist and database administration sub-teams perform necessary application restoration activities. Setting priorities for applications recovery is a primary influence on procedures for this team and its subgroups.

5.3 DATA COMMUNICATIONS

Depending on the location of the cabling, a cable cut by a backhoe could render an <Facility/System> and associated buildings without connectivity. Oftentimes, "redundant cabling" can mean two fiber optic cables laid in the same trench for failover connectivity. While this may be adequate for routine telecommunication interruptions, it represents a single point of failure for communications and connectivity.

The level of data connectivity required will be determined pending the final decision regarding the disaster declaration. Data communications specifications should be documented in APPENDIX <H> , Communication Requirements, in this plan and should be stored in the secure offsite storage location or <Name>, in the event that a permanent replacement facility is required.

5.4 BACKUPS

The most important physical asset in any Facility/System is its data and information. Data and information processing are a major reason for the existence of <Name>. Moreover, all of the <Name> systems are dependent on the preservation of data, including

software manuals and documentation. In order to minimize the impact of a disaster, it is extremely important to protect the sensitivity or confidentiality of data; to preserve the authenticity and accuracy of data, and to maintain the availability of data. These three goals are commonly defined as "Confidentiality, Integrity, and Availability". The protection of the confidentiality, integrity, and availability of data is of singular importance in information security and disaster recovery planning. Confidentiality, integrity, and availability of data are intrinsic to disaster recovery planning.

Effective procedures to perform full data back ups on a regular weekly basis must be implemented. A copy of the weekly back ups should be securely transported on a weekly basis and stored off site in an environmentally controlled storage facility, preferably outside the immediate regional area. Frequent backups should be implemented to ensure the recovery of the most current data version and to increase the likelihood of usable media in a post-event scenario.

5.4.1 VITAL RECORDS/DOCUMENTATION

Vital records and important documentation should be backed up and stored off site. Vital records are any documents or documentation that is essential to the operations of an organization, such as personnel records, software documentation, legal documentation, legislative documentation, benefits documentation, etc.

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures in detail helps to eliminate security lapses and oversights, gives new personnel detailed instructions on how to operate equipment or do a particular task, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently every time.

Security documentation should be developed to fulfill the needs of those who use it. For this reason, many organizations separate documentation into policy and procedures for each user level. For example, a functional security procedures manual should be written to inform end users how to do their jobs securely while a technical and operational security procedures manual should be written for systems operations and support staff focusing on system administrations concerns in considerable detail.

There should be at least two copies of current system security documentation. One copy should be stored on site and be immediately accessible. A back up copy must be stored off site and should include documents such as system security plans (SSP), contingency plans, risk analyses, and security policies and procedures. Additional copies may be necessary for some documentation, such as contingency plans, which should be easily accessible in the event of a disaster. It is recommended that copies of the Contingency Plan be distributed to the <Facility/System> Contingency Plan Coordinator, Executive Management, and Team Leaders for safekeeping.

Documentation should be duplicated either in hard copy or compatible media format and stored at the off-site storage or the (recovery site) location. The original primary on-site unit retains the original copies of all information. Updates to documentation should be rotated on an as-required basis, under the control of the responsible team. Off-site documentation should include technical and operational documentation.

Many of the below listed documents may be found in the completed certification and accreditation package (the System Security Authorization Agreement (SSAA) and Appendices). If the information is in the SSAA, keep it current and maintain a copy off-site.

The following documentation should be maintained off site:

- *Security related Information Technology (IT) policy & procedure memorandum, circulars, publications*
- *Department or component mission statement*
- *Letters of delegation for key Information System security personnel*
- *Complete hardware and software listings*
- *Internal security, Information System audits*
- *Detailed IT architecture schematics (logical/physical, network, devices)*
- *Network cable routing schematics (on floor overlay)*
- *System testing plans/procedures*
- *Review and approval of plans/procedures*
- *System Configuration*
- *Review and approval of proposed configuration*
- *Changes made to the system configuration*
- *Evaluation of changes for security implications*
- *Technical standards for system design, testing and maintenance to reflect security objectives*
- *Contingency plans for incident response procedures and backup operations*
- *Data backup/restoration procedures and procedures for storage, transportation and handling of backup tapes*

- *Reports of security related incidents*
- *Sensitivity and criticality determination*
- *Baseline security checklist for each system*
- *Software licensing information*

Additionally, it is recommended that <Facility/System> management personnel develop detailed procedural manuals specifying how their functional responsibilities are to be discharged in the event of their unavailability. This is especially important for key personnel. Copies of these manuals should be kept off-site with other documentation.

5.5 OFFICE EQUIPMENT, FURNITURE AND SUPPLIES

Although the current strategy is for office equipment, furniture, and supplies to be ordered on an "emergency as required" basis at the time of the disaster, it is recommended that <Facility/System> management review supply needs and coordinate with the local procurement office to develop a revolving emergency inventory of workspace and survival supplies for immediate use in the event of a disaster. The revolving inventory of workspace supplies should include not only basic essential workspace supplies like pens, pencils, note pads, and paper, but also <Facility and System> specific forms and templates. Additionally, a revolving inventory of survival supplies should be maintained, including bottled drinking water, personal products, and food rations, in the event personnel cannot be evacuated or are temporarily prevented from leaving the confines of the building due to weather conditions.

5.6 RECOMMENDED TESTING PROCEDURES

The <Facility/System> Contingency Plan should be maintained routinely and exercised/tested at least annually. Contingency procedures must be tested periodically to ensure the effectiveness of the plan. The scope, objective, and measurement criteria of each exercise will be determined and coordinated by the <Facility or System> Contingency Plan Coordinator on a "per event" basis. The purpose of exercising and testing the plan is to continually refine resumption and recovery procedures to reduce the potential for failure.

There are two categories of testing: announced and unannounced. In an announced test, personnel are instructed when testing will occur, what the objectives of the test are, and what the scenario will be for the test. Announced testing is helpful for the initial test of procedures. It gives teams the time to prepare for the test and allows them to practice their skills. Once the team has had an opportunity to run through the procedures, practice, and coordinate their skills, unannounced testing may be used to test the completeness of the procedures and sharpen the team's abilities. Unannounced testing consists of testing without prior notification. The use of unannounced testing is extremely helpful in

preparing a team for disaster preparation because it focuses on the adequacy of in-place procedures and the readiness of the team. Unannounced testing, combined with closely monitored restrictions, will help to create a simulated scenario that might exist in a disaster. This more closely measures the teams' ability to function under the pressure and limitations of a disaster. Once it has been determined whether a test will be announced or unannounced, the actual objective(s) of the test must be determined. There are several different types of tests that are useful for measuring different objectives.

A recommended schedule for testing is as follows:

- *Desktop testing on a quarterly basis*
- *One structured walk-through per year*
- *One integrated business operations/information systems exercise per year*

The Contingency Plan Coordinator, Contingency System Coordinators, and Team Leaders, together with the <Facility> Office Management and <System Owners>, will determine end-user participation.

6 RECOMMENDED STRATEGIES

The following information represents potential recommendations to the <Facility/System> Director, and other technical management positions as appropriate. These should be considered as solutions that potentially may assist in the continued development of their recovery capabilities in a post-disaster situation.

6.1 CRITICAL ISSUES

6.1.1 POWER

The <Facility> technology director should work to develop power requirements necessary to provide uninterrupted service for the <Facility or System> data center. After the determination of power requirements has been developed for the continuous operability of the <System> the <Facility> should follow the standard procurement process to obtain, install, test, and maintain such a system. It should be noted that the standard life cycle for the amortization of a diesel powered backup generator is 20 years.

6.1.2 DIVERSIFICATION OF CONNECTIVITY

As it stands, the current connectivity configuration represents a single point of failure to the entire <System>. The dedicated connectivity from all the regional offices converges in the <System> data center. A single occurrence of fire, power failure, terrorist act, or civil unrest could completely disrupt email and Internet based connectivity between the building and the regions. Additionally, <System> users rely upon Internet connectivity

to provide outside email availability to the Department and the regions therefore, based upon any of the aforementioned scenarios that function, would also cease to function.

6.1.3 OFFSITE BACKUP STORAGE

The current schedule implemented for the transfer of backup tapes to the offsite storage facility is inconsistent with the objectives of Contingency Planning. The schedule has the <System> staff maintaining the most current backup tapes onsite in the building for a 30 day period prior to transfer to the offsite storage facility. Thus, all data extracted from office backup tapes will be more than 30 days old. In today's data intensive environment this provides stale information to the <System> end users. This is especially critical in view of the fact that the only time a staff must rely on the offsite backup media is when the system has failed and any incremental backups are ineffective and/or inefficient to resolve the situation. The loss of thirty (30) days of work and data based on the impact of a disaster is not acceptable.

The schedule controlling this process should be re-visited and modified to reflect a more frequent transfer timeline. The accepted standard is the transfer of backup media to the offsite storage on a weekly basis to establish a continuously current flow of data into the backup copies. This will allow the staff to execute restorations utilizing the most updated information available. This is particularly true regarding the e-mail systems.

7 TERMS AND DEFINITIONS

The following is a comprehensive list of terms that are important in contingency planning and recovery operations. Add any Facility specific and system specific terms with definitions relevant to the Contingency Plan in the appropriate alphabetical positions.

ABC Fire Extinguisher - Chemically based devices used to eliminate ordinary combustible, flammable liquid, and electrical fires.
Acceptable Level of Risk - typically refers to the point at which the level of risk is more acceptable than the cost to mitigate the risk (in dollars or affect on computer system function).
Access - the ability to do something with a computer resource. This usually refers to a technical ability (e.g., read, create, modify, or delete a file, execute a program, or use an external connection); admission; entrance.
Access control - the process of limiting access to the resources of an IT system only to authorized users, programs, processes, or other IT systems.
Accountability - the property that enables activities on a system to be traced to individuals, who may then be held responsible for their actions.
Actuator - A mechanical assembly that positions the read/write head assembly over the appropriate tracks.
Activation - When all or a portion of the recovery plan has been put into motion.
Adequate security - security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of information.

This includes assuring that systems and applications used by *<Name>* operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Alert - Notification that a disaster situation has occurred - stand by for possible activation of disaster recovery plan.

Alternate Site - A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster. *Similar Terms: Alternate Processing Facility, Alternate Office Facility, Alternate Communication Facility.*

Application - the use of information resources (information and information technology) to satisfy specific set of user requirements.

Application program - A software program comprising a set of statements, defining certain tasks.

Application Recovery - The component of Disaster Recovery that deals specifically with the restoration of business system software and data, after the processing platform has been restored or replaced. Similar Terms: Business System Recovery.

Array - An arrangement of two or more disk drives: may be in Redundant Array of Inexpensive Disks (RAID) or daisy-chain fashion.

Asset – a value placed on goods owned by an organization

Assumptions - Basic understandings about unknown disaster situations that the disaster recovery plan is based on.

Assurance - a measure of confidence that the security features and architecture of an automated information system accurately mediate and enforce the security policy.

Asynchronous Transfer Mode (ATM) - A network architecture that divides messages into fixed-size units (cells) and establishes a switched connection between the originating and receiving stations; enables transmission of various types of data (video, audio, etc.) over the same line without one data type dominating the transmission

Audit system - an independent review, examination of the records, and activities to access the adequacy of system controls; to ensure compliance with established policies and operational procedures. The audit system is an essential tool for the determination and recommendation of necessary changes in controls, policies, or procedures.

Audit trail - a series of records of computer events about an operating system, an application, or user activities.

Auditing - the review and analysis of management, operational, and technical controls.

Authentication - proving (to some reasonable degree) a user's identity. It can also be a measure designed to provide protection against fraudulent transmission by establishing the validity of a transmission, message, station, or originator.

Authorization - the permission to use a computer resource. Permission is granted, directly or indirectly, by the application or system owner.

Automated – means computerized for the purpose of this document.

Availability - the property of being accessible and usable, upon demand by an authorized entity, to complete a function. The information technology system or installation contains information or provides services that must be available on a timely basis, to meet mission requirements or to avoid substantial losses. Controls to protect the availability of information are required, if the information is critical to the *<Name>*'s activity's functions. Access to some information requires *<Name>* to ensure the availability of that information within a short period of time.

Back Office Location - An office or building, used by the organization to conduct support activities, that is not located within an organization's headquarters or main location.
Backbone - the underlying network communication conduit or line by which all main servers and devices are connected; backbone devices are typically servers, routers, hubs, and bridges; client computers are not connected directly to the backbone.
Backup - means either procedures or standby equipment that are available for use in the event of a failure or inaccessibility of normally used equipment or procedures or to make a copy of data or a program in case the original is lost, damaged, or otherwise unavailable.
Backup Agreement - A contract to provide a service that includes the method of performance, the fees, the duration, the services provided, and the extent of security and confidentiality maintained.
Backup Position Listing - A list of alternative personnel who can fill a recovery team position when the primary person is not available.
Backup Strategies (Recovery Strategies) - Alternative operating method (i.e., platform, location, etc.) for facilities and system operations in the event of a disaster.
Bandwidth - the amount of data that can be transmitted via a given communications channel (e.g., between a hard drive and the host PC) in a given unit of time.
Block - a portion of a volume usually 512 bytes in size; often referred to as a "logical block."
Burst mode - a temporary, high-speed data transfer mode that can transfer data at significantly higher rates than would normally be achieved with non-burst technology; the maximum throughput a device is capable of transferring data.
Bus - the main communication avenue in a computer; an electrical pathway along which signals are sent from one part of the computer to another.
Business Continuity Planning (BCP): An all encompassing, "umbrella" term covering both disaster recovery planning and business resumption planning. *Also see disaster recovery planning and business resumption planning*
Business Impact Analysis (BIA) - The process of analyzing all business functions and the effect that a specific disaster may have upon them.
Business Interruption - Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at a corporate location.
Business Interruption Costs - The costs or lost revenue associated with an interruption in normal business operations.
Business Recovery Coordinator - *See Disaster Recovery Coordinator.*
Business Recovery Process - The common critical path that all companies follow during a recovery effort. There are major nodes along the path that are followed regardless of the organization. The process has seven stages: 1) Immediate response, 2) Environmental restoration, 3) Functional restoration, 4) Data synchronization, 5) Restore business functions, 6) Interim site, and 7) Return home.
Business Recovery Team - A group of individuals responsible for maintaining and coordinating the recovery process. *Similar Terms: Recovery Team*
Business Resumption Planning (BRP): The operations piece of business continuity planning. *Also see: Disaster Recovery Planning*

Business Unit Recovery - The component of Disaster Recovery which deals specifically with the relocation of key organization personnel in the event of a disaster, and the provision of essential records, equipment supplies, work space, communication facilities, computer processing capability, etc. *Similar Terms: Work Group Recovery.*
Byte - The fundamental data unit for personal computers, comprising 8 contiguous bits.
Cache - A large bank of random access memory used for temporary storage of information.
Computer-Aided Design (CAD) -; the use of a computer in industrial design applications such as architecture, engineering, and manufacturing.
Call back - a procedure for identifying a remote terminal. In a call back, the host system disconnects the caller and then dials the authorized telephone number of the remote terminal to reestablish the connection. Synonymous with dial back.
Central Office - a secure, self-contained telecommunications equipment building that houses servers, storage systems, switching equipment, emergency power systems, and related devices that are used to run telephone systems.
Certified Disaster Recovery Planner (CDRP): CDRP's are certified by the Disaster Recovery Institute, a not-for-profit corporation, which promotes the credibility and professionalism in the DR industry.
Checklist Test - A method used to test a completed disaster recovery plan. This test is used to determine if the information such as phone numbers, manuals, equipment, etc. in the plan is accurate and current.
Clustered servers - The concept of combining multiple host computers together through a private communication line, such as Ethernet backbone, to form a ring of host computers; this ring of host computers act as a single entity, capable of performing multiple complex instructions by distributing the workload across all members of the ring.
Clustered storage - the concept of combining multiple storage servers together to form a redundant ring of storage devices; clustered storage systems typically perform multiple read and write requests through parallel access lines to the requesting computer.
Cold Site - An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed in such a facility to duplicate the critical business functions of an organization. Cold-sites have many variations depending on their communication facilities, Uninterruptible Power Source (UPS) systems, or mobility (Relocatable-Shell). *Similar Terms: Shell-site; Back-up site; Recovery site; Alternative site.*
Command And/Or Control Center (CAC/CNC/CCC) - A centrally located facility having adequate phone lines to begin recovery operations. Typically it is a temporary facility used by the management team to begin coordinating the recovery process and used until the alternate sites are functional.
Commerce service provider (CSP) - A company that provides e-commerce solutions for retailers.
Competitive local exchange carrier (CLEC) - a long distance carrier, cable company, or small startup local exchange carrier that competes for business in a local telephone market; many CLECs also offer Internet services.
Computer virus - A program that "infects" computer systems in much the same way, as a biological virus infects humans. The typical virus "reproduces" by making copies of

itself and inserting them into the code of other programs—either in systems software or in application programs.

Communications Failure - An unplanned interruption in electronic communication between a terminal and a computer processor, or between processors, as a result of a failure of any of the hardware, software, or telecommunications components comprising the link. (Also refer to Network Outage.)

Communications Recovery - The component of Disaster Recovery which deals with the restoration or rerouting of an organization's telecommunication network, or its components, in the event of loss. *Similar Terms: (Telecommunication Recovery, Data Communications Recovery)*

Computer Recovery Team (CRT) - A group of individuals responsible for assessing damage to the original system, processing data in the interim, and setting up the new system.

Confidentiality - the assurance that information is not disclosed to unauthorized entities or processes. The information technology system or installation contains information that requires protection from unauthorized or inappropriate disclosure. Some information must be protected from unauthorized or accidental disclosure. *<Name>* is required to prevent some information from release to persons without the proper qualifications. Information requiring protection from unauthorized disclosure includes classified information, information related to military operations and equipment, confidential commercial business information, confidential *<Name>* business information, Privacy Act information, law enforcement confidential information, procurement-sensitive information, budgetary information prior to OMB release, and information exempt from disclosure under the Freedom of Information Act (FOIA).

Configuration control - the process of controlling modifications to the system's hardware, software, and documentation that provide sufficient assurance that the system is protected against the introduction of improper modifications before, during, and after system implementation.

Configuration management (CM) - The management of changes made to a system's hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the development and operational life of the system.

Consortium Agreement - An agreement made by a group of organizations to share processing facilities and/or office facilities, if one member of the group suffers a disaster. *Similar Terms: Reciprocal Agreement.*

Contingency plan - a plan for emergency response, back-up operations, and post-disaster recovery for information technology systems and installations in the event normal operations are interrupted. The contingency plan should ensure minimal impact upon data processing operations in the event the information technology system or facility is damaged or destroyed.

Contingency planning - a plan that addresses how to keep an organization's critical functions operating in the event of any kind of disruptions. *See Disaster Recovery Plan*

Contingency Planning - *See also Disaster Recovery Planning.*

Controller - a unit or circuitry that manages the information flow between storage disks and the computer.

Cooperative Hot sites - A hot site owned by a group of organizations available to a group member should a disaster strike. *Also See Hot-Site.*

Cost Benefit Analysis - the assessment of the costs of providing data protection for a system versus the cost of losing or compromising a system.
Cost of ownership - the purchase price of equipment plus the cost of operating this equipment over its projected life span.
Commercial Off-the-Shelf (COTS) -; Commercially available products that can be purchased and integrated with little or no customization, thus facilitating customer infrastructure expansion and reducing costs.
Countermeasure - any action, device, procedure, technique, or other measure that reduces the vulnerability of, or threat to a system.
Crate & Ship - A strategy for providing alternate processing capability in a disaster, via contractual arrangements with an equipment supplier to ship replacement hardware within a specified time period. *Similar Terms: Guaranteed Replacement, Quick Ship.*
Crisis - A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate.
Crisis Management - The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.
Crisis Simulation - The process of testing an organization's ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.
Critical Functions - Business activities or information, which could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization.
Critical Records - Records or documents, which, if damaged or destroyed, would cause considerable inconvenience and/or require replacement or recreation at considerable expense.
Cryptography - the principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form.
Computer Telephony Integration (CTI) - Providing a link between telephone systems and computers to facilitate incoming and outgoing call handling and control; the physical link between a telephone and server.
Digital Audio Tape (DAT) - A digital magnetic tape format originally developed for audio recording and now used for computer backup tape; the latest DAT storage format is DDS (Digital Data Storage).
Damage Assessment - The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc. and determining what can be salvaged or restored and what must be replaced.
Data Center Recovery - The component of Disaster Recovery that deals with the restoration, at an alternate location, of data centers services and computer processing capabilities. *Similar Terms: Mainframe Recovery.*
Data Center Relocation - The relocation of an organization's entire data processing operation.
Declaration Fee - A one-time fee, charged by an Alternate Facility provider, to a customer who declares a disaster. *Similar Terms: Notification Fee.* *NOTE: Some recovery vendors apply the declaration fee against the first few days of recovery.*

Decryption - the process of taking an encrypted file and reconstructing the original file. This is the opposite of encryption.
Dedicated Line - A pre-established point-to-point communication link between computer terminals and a computer processor, or between distributed processors, that does not require dial-up access.
Departmental Recovery Team - A group of individuals responsible for performing recovery procedures specific to their department.
Dynamic Growth and Reconfiguration (DGR) - A Dot Hill technology that allows the system administrator to quickly and easily add capacity or change RAID levels while the system is in use.
Dial Backup - The use of dial-up communication lines as a backup to dedicated lines.
Dial-Up Line - A communication link between computer terminals and a computer processor, which is established on demand by dialing a specific telephone number.
Disaster - Any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time. *Similar Terms: Business Interruption; Outage; Catastrophe.*
Disaster Prevention - Measures employed to prevent, detect, or contain incidents that, if unchecked, could result in disaster.
Disaster Prevention Checklist - A questionnaire used to assess preventative measures in areas of operations such as overall security, software, data files, data entry reports, microcomputers, and personnel.
Disaster Recovery - The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.
Disaster Recovery Administrator - The individual responsible for documenting recovery activities and tracking recovery progress.
Disaster Recovery Coordinator - The Disaster Recovery Coordinator may be responsible for overall recovery of an organization or unit(s). *Similar Terms: Business Recovery Coordinator.*
Disaster Recovery Period - The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.
Disaster Recovery Plan (DRP) - The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.
Disaster Recovery Planning - The technological aspect of business continuity planning. The advance planning and preparations that are necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster. *Similar Terms: Contingency planning; business resumption planning; corporate contingency planning; business interruption planning; disaster preparedness.*
Disaster Recovery Software - An application program developed to assist an organization in writing a comprehensive disaster recovery plan.
Disaster Recovery Teams (Business Recovery Teams): A structured group of teams ready to take control of the recovery operations if a disaster should occur.
Disk array (see array) - an arrangement of two or more hard disks, in RAID or daisy-chain configuration, organized to improve speed and provide protection of data against loss.

Distributed computing environment - A set of middleware standards that defines the method of communication between clients and servers in a cross-platform computing environment; enables a client program to initiate a request that can be processed by a program written in a different computer language and housed on a different computer platform.
Digital Linear Tape (DLT) - A serpentine technology first introduced by Digital Equipment Corporation and later developed by Quantum for tape backup/archive of networks and servers; DLT technology addresses midrange to high-end tape backup requirements.
Electronic Industries Association (EIA) - A trade association that establishes electrical and electronics-oriented standards.
Electronic Vaulting - Transfer of data to an offsite storage facility via a communication link rather than via portable media. Typically used for batch/journaled updates to critical files to supplement full backups taken periodically.
Emergency - A sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property.
Emergency Preparedness - The discipline which ensures an organization, or community's readiness to respond to an emergency in a coordinated, timely, and effective manner.
Emergency Procedures - A plan of action to commence immediately to prevent the loss of life and minimize injury and property damage.
Electro Magnetic Interference (EMI) –; What occurs when electromagnetic fields from one device interfere with the operation of some other device.
Employee Relief Center (ERC) - A predetermined location for employees and their families to obtain food, supplies, financial assistance, etc., in the event of a catastrophic disaster.
Encryption - The process of coding a message to make it unintelligible.
Enterprise storage network (ESN) - an integrated suite of products and services designed to maximize heterogeneous connectivity and management of enterprise storage devices and servers; a dedicated, high-speed network connected to the enterprise's storage systems, enabling files and data to be transferred between storage devices and client mainframes and servers.
Environment - the aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system.
Ethernet - a local area network standard for hardware, communication, and cabling.
Extended Outage - A lengthy, unplanned interruption in system availability due to computer hardware or software problems, or communication failures.
Extra Expense Coverage - Insurance coverage for disaster related expenses that may be incurred until operations are fully recovered after a disaster.
Facilities - A location containing the equipment, supplies, voice and data communication lines, to conduct transactions required to conduct business under normal conditions. *Similar Terms: Primary Site, Primary Processing Facility, Primary Office Facility.*
Failover - the transfer of operation from a failed component (e.g., controller, disk drive) to a similar, redundant component to ensure uninterrupted data flow and operability.
Fault tolerance - the ability of a system to cope with internal hardware problems (e.g., a disk drive failure) and still continue to operate with minimal impact, such as by bringing a backup system online.

Fiber Channel-Arbitrated Loop (FC-AL) - A fast serial bus interface standard intended to replace SCSI on high-end servers. A Fibre Channel implementation in which users are attached to a network via a one-way ring (loop) cabling scheme.
Fiber Channel Community (FCC) -; An international non-profit organization whose members include manufacturers of servers, disk drives, RAID storage systems, switches, hubs, adapter cards, test equipment, cables and connectors, and software solutions.
Fiber Channel - A high-speed storage/networking interface that offers higher performance, greater capacity and cabling distance, increased system configuration flexibility and scalability, and simplified cabling.
Fiber Distributed Data Interface (FDDI) - A 100 Mbit/s ANSI standard LAN architecture, defined in X3T9.5. The underlying medium is optical fiber (though it can be copper cable, in which case it may be called CDDI) and the topology is a dual-attached, counter-rotating token ring.
File Backup - The practice of dumping (copying) a file stored on disk or tape to another disk or tape. This is done for protection case the active file gets damaged.
File Recovery - The restoration of computer files using backup copies.
File Server - The central repository of shared files and applications in a computer network (LAN).
Footprint - the amount of floor space that a piece of equipment (e.g., a rackmount enclosure) occupies.
Form factor - the physical size and shape of a device; often used to describe the size of disk arrays in a rack mount enclosure.
Forward Recovery -The process of recovering a data base to the point of failure by applying active journal or log data to the current backup files of the database.
Full Recovery Test An exercise in which all recovery procedures and strategies are tested (as opposed to a Partial Recovery Test.)
Generator - An independent source of power usually fueled by diesel or natural gas.
Gigabyte - approximately one billion bytes, 1,024 megabytes.
Host Bus Adapter (HBA) -; a hardware card that resides on the PC bus and provides an interface connection between a SCSI device (such as a hard drive) and the host PC.
Halon - A gas used to extinguish fires effective only in closed areas.
High Priority Tasks - Activities vital to the operation of the organization. Currently being phased out due to environmental concerns. *Similar Terms: Critical Functions*
Home page - The main page on a Web site that serves as the primary point of entry to related pages within the site and may have links to other sites as well.
Host-attached storage - A storage system that is connected directly to the network server; also referred to as server-attached storage.
Hot site -An alternate facility that has the equipment and resources to recover the business functions affected by the occurrence of a disaster. Hot-sites may vary in type of facilities offered (such as data processing, communication, or any other critical business functions needing duplication). Location and size of the hot-site will be proportional to the equipment and resources needed. *Similar Terms: Backup site; Recovery site; Recovery Center; Alternate processing site.*
Hot spare - a backup component (e.g., disk or controller) that is online and available should the primary component go down.

Hot swappable - the ability to replace a component (e.g., disk drive, controller, fan, power source) while the system is on line, without having to power down; also referred to as hot-plug removable.
Hierarchical Storage Management (HSM) -; a storage system in which new, frequently used data is stored on the fastest, most accessible (and generally more expensive) media (e.g., RAID) and older, less frequently used data is stored on slower (less expensive) media (e.g., tape).
Hub - A device that splits one network cable into a set of separate cables, each connecting to a different computer; used in a local area network to create a small-scale network by connecting several computers together.
Human Threats - Possible disruptions in operations resulting from human actions (i.e., disgruntled employee, terrorism, etc.).
Heat, Ventilation, and Air Conditioning (HVAC) – The system that provides and maintains a controlled environment with conditions conducive to continuous and uninterrupted computer operations.
Identification - The process that enables, generally by the use of unique machine-readable names, recognition of users or resources, as indistinguishable, to those previously described to the automated information system.
Institute of Electrical and Electronics Engineers (IEEE) - The largest technical society in the world, consisting of engineers, scientists, and students; has declared standards for computers and communications.
Initiator- A Small Computer System Interface (SCSI) device that requests another SCSI device (a target) to perform an operation; usually a host computer acts as an initiator and a peripheral device acts as a target.
Information system - The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.
Information technology system - an information system that is automated or is an assembly of computer hardware and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing and retrieving data with a minimum of human intervention. The term includes single application programs, which operate independently of other program applications. A "sensitive information technology system" means an information technology system that contains sensitive information.
Information technology installation - one or more computer or office automation systems, including related telecommunications, peripheral and storage units, central processing units, and operating and support system software. Information technology installations may range from information technology installations, such as large centralized computer centers, to individual stand-alone microprocessors, such as personal computers. A "sensitive information technology installation" means an information technology installation, which contains or provides processing for a sensitive information technology system.
Infrastructure –(1) the physical equipment (computers, cases, racks, cabling, etc.) that comprises a computer system; (2) the foundational basis that supports the information management capabilities, including the telecommunications and network connectivity.
Integrity, data - That attribute of data relating to the preservation of (1) its meaning and completeness, (2) the consistency of its representation(s), and (3) its correspondence to

what it represents. The information technology system or installation contains information that must be protected from unauthorized, unanticipated, or unintentional modification or destruction, including detection of such activities. Integrity is important to all information because inaccuracy compromises the value of the information system. Law enforcement, mission and life critical, and financial information are examples of information requiring protection to preserve integrity.

Integrity, system - That attribute of a system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

InterFacility Contingency Planning Regulation A regulation written and imposed by the Federal Financial Institutions Examination Council concerning the need for financial institutions to maintain a working disaster recovery plan.

Interface - A connection between hardware devices, applications, or different sections of a computer network.

Interim Organizational Structure - An alternate organization structure that will be used during recovery from a disaster. This temporary structure will typically streamline chains of command and increase decision-making autonomy.

Internal Hot sites - A fully equipped alternate processing site owned and operated by the organization.

Internet - A worldwide system of linked computer networks.

Internet Service Provider (ISP) - A company that provides Internet access services to consumers and businesses; ISPs lease connections from Internet backbone providers; while most ISPs are small companies that service a local area, there are also regional and national ISPs (such as America Online).

Interoperability - The ability of one computer system to control another, even though the two systems are made by different manufacturers.

Interruption - An outage caused by the failure of one or more communications links with entities outside of the local facility.

Intranet - a computer network, based on Internet technology, which is designed to meet the internal needs for sharing information within a single organization or company.

Input/Output (I/O) -; Reception (read) or transmission (write) of computer signals; the entire connection path between the CPU bus and the disk drives.

I/Os Per Second (IOPS) - A measure of performance for a host-attached storage device or RAID controller.

Just A Bunch Of Disks (JBOD) - A disk array without a controller.

Kernel - The core of an operating system such as Windows 98, Windows NT, Mac OS or Unix; provides basic services for the other parts of the operating system, making it possible for it to run several programs at once (multitasking), read and write files and connect to networks and peripherals.

Local Area Network (LAN) - A LAN consists of personal computers that are connected together through various means, so that they can communicate with each other. A network of computers, within a limited area (e.g., a company or organization); Computing equipment, in close proximity to each other, connected to a server which houses software that can be access by the users. This method does not utilize a public carrier. *See Also WAN.*

LAN Recovery - The component of Disaster Recovery which deals specifically with the replacement of LAN equipment in the event of a disaster, and the restoration of essential data and software *Similar Terms: Client/Server Recovery*
Leased Line - Usually synonymous with dedicated line.
Legacy - A computer, system, or software that was created for a specific purpose but is now outdated; anything left over from a previous version of the hardware or software.
Line Rerouting - A service offered by many regional telephone companies allowing the computer center to quickly reroute the network of dedicated lines to a backup site.
Line Voltage Regulators - Also known as surge protectors. These protectors/regulators distribute electricity evenly.
Logic Bomb - A computer code that is preset to cause a malfunction, at a later time, when a specified set of logical conditions occurs. For example, a specific social security number in a payroll system is processed and the logic bomb is activated, causing an improper amount of money to be printed on the check.
Loss - The unrecoverable business resources that are redirected or removed as a result of a disaster. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.
Loss Reduction - The technique of instituting mechanisms to lessen the exposure to a particular risk. Loss reduction is intended to react to an event and limit its effect. Examples of Loss Reduction include sprinkler systems.
Linear Tape Open (LTO) -; A new standard tape format developed by HP, IBM, and Seagate; expected availability in 2000.
Logical Unit Number (LUN) - An addressing scheme used to define SCSI devices on a single SCSI bus.
Machine-readable Media - Media that can convey data to a given sensing device, e.g., diskettes, disks, tapes, computer memory.
Mainframe Computer - A high-end computer processor, with related peripheral devices, capable of supporting large volumes of batch processing, high performance on-line transaction processing systems, and extensive data storage and retrieval. *Similar Terms: Host Computer.*
Malicious Software - Any of a family of computer programs developed with the sole purpose of doing harm. Malicious code is usually embedded in software programs that appear to provide useful functions but, when activated by a user, cause undesirable results.
Media Transportation Coverage - An insurance policy designed to cover transportation of items to and from an EDP center, the cost of reconstruction and the tracing of lost items. Coverage is usually extended to transportation and dishonesty or collusion by delivery employees.
Megabyte - Approximately one million bytes, 1,024 kilobytes
Magnetic Ink Character Reader (MICR) Equipment - Equipment used to imprint machine-readable code. Generally, financial institutions use this equipment to prepare paper data for processing, encoding (imprinting) items such as routing and transit numbers, account numbers, and dollar amounts.
Mirroring - A method of storage in which data from one disk is duplicated on another disk so that both drives contain the same information, thus providing data redundancy.

Mission critical - Any computer process that cannot fail during normal business hours; some computer processes (e.g., telephone systems) must run all day long and require 100 percent uptime.
Mobile Hot Site - A large trailer containing backup equipment and peripheral devices delivered to the scene of the disaster. It is then hooked up to existing communication lines.
Modulator Demodulator Unit (MODEM) - Device that converts data from analog to digital and back again.
Monitoring - An ongoing activity that checks on the system, its users, or the environment.
Mean Swaps Between Failure (MSBF) -A statistical calculation used to predict the average usefulness of a robotic device (e.g., a tape library) with any interruption of service.
Mean Time Between Failure (MTBF) - A statistical calculation used to predict the average usefulness of a device without any interruption of service.
Mean Time To Repair (MTTR) - The average amount of time required to resolve most hardware or software problems with a given device.
Multi-platform - .The ability of a product or network to support a variety of computer platforms (e.g. IBM, Sun, Macintosh); also referred to as cross-platform.
Natural Threats - Events caused by nature causing disruptions to an organization.
Network - The Open Systems Interconnect (OSI) seven-layer model attempts to provide a way of partitioning any computer network into independent modules from the lowest (physical) layer to the highest (application) layer. Many different specifications exist at each of these layers. The network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.
Network Architecture - The basic layout of a computer and its attached systems, such as terminals and the paths between them.
Network-Attached Storage (NAS) - A disk array storage system that is attached directly to a network rather than to the network server (i.e., host attached); functions as a server in a client/server relationship, has a processor, an operating system or micro-kernel, and processes file I/O protocols such as SMB and NFS.
Network Service Provider (NSP) - a company that provides the national or international packet-switching networks that carry Internet traffic; also called a backbone operator.
Network Outage - An interruption in system availability as a result of a communication failure affecting a network of computer terminals, processors, or workstations.
Node (or network node) - Any device that is directly connected to the network, usually through Ethernet cable; nodes include file servers and shared peripherals; the name used to designate a part of a network. This may be used to describe one of the links in the network, or a type of link in the network (for example, Host Node or Intercept Node).
Nonessential Function/Data - Business activities or information that could be interrupted or unavailable indefinitely without significantly jeopardizing critical functions of an organization.
Nonessential Records - Records or documents, which, if irretrievably lost or damaged, will not materially impair the organization's ability to conduct business.
NT (Microsoft Windows NT) - An operating system developed by Microsoft for high-performance processors and networked systems.

Original Equipment Manufacturer (OEM) - A company that manufactures a given piece of hardware (unlike a value-added reseller, which changes and repackages the hardware).

Off-Host Processing - A backup mode of operation in which processing can continue throughout a network despite loss of communication with the mainframe computer.

Off-Line Processing - A backup mode of operation in which processing can continue manually or in batch mode if the on-line systems are unavailable.

Off-Site Storage Facility - A secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored.

On-Line Systems - An interactive computer system supporting users over a network of computer terminals.

Open systems network - A network comprised of equipment that conforms to industry standards of interoperability between different operating systems (e.g., Unix, Windows NT).

Operating Software - A type of system software supervising and directing all of the other software components plus the computer hardware.

Operating System - The master control program (e.g., Windows) that manages a computer's internal functions and provides a means of control to the computer's operations and file system.

Organization Chart - A diagram representative of the hierarchy of an organization's personnel.

Organization-Wide - A policy or function applicable to the entire organization.

Outage - *See Systems Outage.*

Outsourcing - The transfer of data processing functions to an independent third party.

Owner - The individual designated as being responsible for the protection of IT resources. The owner generally falls into two broad categories: custodial and owner. For example, the "owner" of the resources, may be the manager of that facility. Resources located within user areas may be "owned" by the manager of those areas. To assist with the determination of ownership, individual system boundaries must be established. A system is identified by logical boundaries being drawn around the various processing, communications, storage, and related resources. They must be under the same direct management control with essentially the same function, reside in the same environment, and have the same characteristics and security needs. Ownership of information and/or information processing resources may be assigned to an organization, subordinate functional element, a position, or a specific individual. When ownership is assigned to an organizational or functional element, the head of the unit so designated will be considered the resource owner. Some, but not necessarily all factors to be considered in the determination of ownership are:

1.The originator or creator of data.

2.The organization or individual with the greatest functional interest.

3.Physical possession of the resource.

Parallel Test- A test of recovery procedures in which the objective is to parallel an actual business cycle.

Parity data - A block of information mathematically created from several blocks of user data to allow recovery of user data contained on a drive that has failed in an array; used in RAID levels 3 and 5.

Password - A string of alphanumeric characters chosen by an individual to help ensure that their computer access is protected. Passwords are changed frequently to minimize the risk of unauthorized disclosure. Additional passwords may be assigned by the user to particular files or data sets.
Personal Computer Interconnect (PCI) - An industry-standard bus used in servers, workstations, and PCs.
Peripheral Equipment- Devices connected to a computer processor that perform such auxiliary functions as communications, data storage, printing, etc.
Petabyte - 1,024 terabytes.
Physical Safeguards - Physical measures taken to prevent a disaster, such as fire suppression systems, alarm systems, power backup and conditioning systems, access control systems, etc.
Platform - A hardware standard, such as IBM, Sun, or Macintosh.
Portable Shell - An environmentally protected and readied structure that can be transported to a disaster site so equipment can be obtained and installed near the original location.
Procedural Safeguards - Procedural measures taken to prevent a disaster, such as safety inspections, fire drills, security awareness programs, records retention programs, etc.
Proprietary - Privately developed and owned technology.
Protocol - A standard that specifies the format of data and rules to be followed in data communication and network environments.
RAID Advisory Board (RAB) -; an organization of storage system manufacturers and integrators dedicated to advancing the use and awareness of RAID and associated storage technologies; started in 1992, RAB states its main goals as education, standardization and certification.
Rackmount - The cabinet that houses a server/storage workstation (also referred to as a server rack); to mount equipment into a cabinet.
Redundant Array of Independent (or inexpensive) Disks (RAID) - A collection of storage disks with a controller (or controllers) to manage the storage of data on the disks.
Redundant Data Path (RDP) - Dot Hill's software technology that creates an alternate data path between the server and the storage system in the event of system component failures to ensure continuous access to data.
Real-time - Immediate processing of input or notification of status.
Reciprocal Agreement - An agreement between two organizations with compatible computer configurations allowing either organization to utilize the other's excess processing capacity in the event of a disaster.
Record Retention - Storing historical documentation for a set period of time, usually mandated by state and federal law or the Internal Revenue Service.
Recovery Action Plan - The comprehensive set of documented tasks to be carried out during recovery operations.
Recovery Alternative - The method selected to recover the critical business functions following a disaster. In data processing, some possible alternatives would be manual processing, use of service bureaus, or a backup site (hot or cold-site). A recovery alternative is usually selected following a Risk Analysis, Business Impact Analysis, or both. *Similar Terms: Backup site, backup alternative.*

Recovery Capability -This defines all of the components necessary to perform recovery. These components can include a plan, an alternate site, change control process, network rerouting, and others.
Recovery Management Team - A group of individuals responsible for directing the development and on-going maintenance of a disaster recovery plan. Also responsible for declaring a disaster and providing direction during the recovery process.
Recovery Planning Team - A group of individuals appointed to oversee the development and implementation of a disaster recovery plan.
Recovery Point Objective (RPO) - The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data projection strategy is developed.
Recovery Team - *See Business Recovery Team.*
Recovery Time - The period from the disaster declaration to the recovery of the critical functions.
Relocatable Shell - *See Portable Shell*
Recovery procedures - the actions necessary to restore a system's processing capability and data files after a system failure.
Risk - A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact.
Risk analysis - A formal systematic approach to assessing the vulnerability of an information technology system or installation. Risk analysis is the process of analyzing threats to and vulnerabilities of an information system to determine the risks (potential for losses). The resulting data is then analyzed. The analysis is used as a basis for identifying appropriate and cost-effective measures to counter the identified threats and vulnerabilities. The risk analysis identifies threats, quantifies the potential losses from threat realization, examines the cost benefit of applying alternative measures to counter the identified threats and reduces potential loss, and defines or documents the degree of acceptable risk. *Similar Terms: Risk assessment; impact assessment; corporate loss analysis; risk identification; exposure analysis; exposure assessment.*
Risk management - The process of the identification, measurement, control, and minimization of security risk in information systems. Also, it means to assess risk, take actions to reduce risk to an acceptable level, and maintain risk at that level. Inherent in this definition are the concepts that risk cannot be completely eliminated and the most secure computer system is the one that no one uses.
Router - An electronic device that connects two or more networks and routes incoming data packets to the appropriate network.
Safeguards - The protective measures and controls that are prescribed to meet the security requirements specified for a system.
Salvage & Restoration - The process of reclaiming or refurbishing computer hardware, vital records, office facilities, etc. following a disaster.
Salvage Procedures - Specified procedures to be activated if equipment or a facility should suffer any destruction.
Sample Plan - A generic disaster recovery plan that can be tailored to fit a particular organization.

Storage Area Network (SAN) - A network infrastructure of shared multi-host storage, linking all storage devices as well as interconnecting remote sites.
Satellite Communication - Data communications via satellite. For geographically dispersed organizations, may be viable alternative to ground-based communications in the event of a disaster.
Scalable - The ability of a product or network to accommodate growth.
Scan - To examine computer coding/programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices. (E.g., changes to an executable file, direct writes to specific disk sectors, et al.).
Scope - Predefined areas of operation for which a disaster recovery plan is developed.
Small Computer System Interface (SCSI) - An interface that serves as an expansion bus that can be used to connect hard disk drives, tape drives, and other hardware components.
Secure - In terminology, such as e.g., secure LAN or secure device, means that the routing addresses on the network are monitored and allowed to proceed only for authorized users. This network traffic monitoring and authorization process is referred to as *<Name>*'s "firewalls". Systems and devices, not being monitored, are referred to as being outside of *<Name>*'s secure firewall and the term "non-secure" is applied.
Security features - Are controls that protect against the identified vulnerabilities, i.e. fire and water alarms, passwords and other access protection, use of removable media for data storage, data validation controls, audit trails, un-interruptible power sources (UPS) to protect against electrical outages, personnel screening, computer security awareness training of users, etc.
Security infraction - The failure to follow applicable laws and regulations and established *<Name>* policies and procedures pertaining to the protection of *<Name>* information and computer resources. Henceforth, infraction and violation are to be used interchangeably throughout this document.
Security policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Security specification - A detailed description of the security requirements and specifications necessary to protect an information technology system or installation.
Sensitive information - Information that requires a degree of protection due to its nature, magnitude of loss, or harm that could result from inadvertent or deliberate disclosure, modification, or destruction. This includes information that is

1.Mission critical (i.e., loss or harm would be such that an *<Name>* office could not perform essential functions).
2.Should not be disclosed under the Freedom of Information Act, such as proprietary data and economic forecasts. Proprietary data includes trade secrets, commercial, or financial data obtained in the course of Government business, from or relating to a person or persons outside the government, not generally available to the public, and which is privileged, would cause competitive harm if released, or impair the ability of the government to obtain data in the future.
3.Complies with OMB Circular A-127 Financial Management Systems.
4.Complies with the Privacy Act of 1974. Data, which pertains to a specific individual by name, Social Security Number or by some other identifying means, and is part of a system of records as defined in the Privacy Act of 1974.

5.Classified.

Server - A computer that stores application and data files for all workstations on a network; also referred to as a file server.

Shadow File Processing - An approach to data backup in which real-time duplicates of critical files are maintained at a remote processing site. *Similar Terms: Remote Mirroring*

Simulation Test - A test of recovery procedures under conditions approximating a specific disaster scenario. This may involve designated units of the organization actually ceasing normal operations while exercising their procedures.

Skills Inventory - A listing of employees that lists their skills that apply to recovery.

Spindle - Mechanism inside a hard disk drive that moves the heads into place; the axle on which a disk turns.

Serial Storage Architecture (SSA) - A high-speed method of connecting disk, tape, and CD-ROM drives, printers, scanners, and other devices to a computer.

Stand-Alone Processing - Processing, typically on a PC or mid-range computer, which does not require any communication link with a mainframe or other processor.

Striping - A method of storage in which a unit of data is distributed and stored across several hard disks, which improves access speed but does not provide redundancy.

Structured Walk-Through Test - Team members walk through the plan to identify and correct weaknesses.

Subscription - Contract commitment providing an organization with the right to utilize a vendor recovery facility for recovery of their mainframe processing capability.

Super-user - A system account that has full system-wide administrative privileges. Most UNIX machines have a log on account called "**root**", which acts as the super-user.

Sustained mode - The measured transfer rate of a given device during normal operation.

Switch - A network traffic-monitoring device that controls the flow of traffic between multiple network nodes.

System - A generic term used for its brevity to mean either a major application or a general support system. A system is identified by logical boundaries drawn around the various processing communications, storage, and related resources. They must be under same direct management control (not responsibility), perform essentially the same function, reside in the same environment, and have the same characteristics and security needs. A system does not have to be physically connected.

Systems Downtime - A planned interruption in system availability for scheduled system maintenance.

Systems integrator - An individual or company that combines various components and programs into a functioning system, customized for a particular customer's needs.

System Outage - An unplanned interruption in system availability as a result of computer hardware or software problems, or operational problems.

System Security Plan (SSP) - A plan to be developed by *<Name>* in accordance with OMB and NIST guidelines implementing the Computer Security Act of 1987, to safeguard the security of its information technology systems and installations.

Target - a SCSI device that performs an operation requested by an initiator.

TCQ - Tag command queuing; a feature introduced in the SCSI-2 specification that permits each initiator to issue commands accompanied by instructions for how the target should handle the command; the initiator can either request the command to be executed

at the first available opportunity, in the order in which the command was received, or at a time deemed appropriate by the target.

Technical Threats - A disaster causing event that may occur regardless of any human elements.

Telco - Abbreviation for a "telecommunications company."

Temporary Operating Procedures - Predetermined procedures, which streamline operations while maintaining an acceptable level of control and auditability during a disaster situation.

Terabyte - Approximately one trillion bytes, 1,024 gigabytes.

Test Plan - The recovery plans and procedures that are used in a systems test to ensure viability. A test plan is designed to exercise specific action tasks and procedures that would be encountered in a real disaster.

Test scenarios - Are descriptions of the tests to be performed to check the effectiveness of the security features. They may include validation of password constraints, such as length and composition of the password, entry of erroneous data to check data validation controls, review of audit information produced by the system, review of contingency plans and risk analyses, etc.

Threat - Any circumstance or event with the potential to cause harm to a system in the destruction, disclosure, modification of data, and/or denial of service.

Throughput - Measures the number of service requests on the I/O channel per unit of time.

Time Bomb - Computer code that is preset to cause a later malfunction after a specific date, time, or a specific number of operations. The "Friday the 13th" computer virus is an example. This virus infects the system several days or even months before and lies dormant until the date reaches Friday the 13th.

Topology - Geometric arrangement of nodes and cable links in a local area network; may be either centralized or decentralized.

Transfer rate - The number of megabytes of data that can be transferred from the read/write heads to the disk controller in one second.

Trap Door - A set of instruction codes embedded in a computer operating system that permits access, while bypassing security controls.

Trojan Horse - A program that causes unexpected (and usually undesirable) effects when willingly installed or run by an unsuspecting user. A Trojan horse is commonly disguised as a game, a utility, or an application. A person can either create or gain access to the source code of a common, frequently used program and then add code, so that the program performs a harmful function, in addition to its normal function. These programs are generally deeply buried in the code of the target program, lie dormant for a preselected period, and are triggered in the same manner as a logic bomb. A Trojan horse can alter, destroy, disclose data, or delete files.

Turnkey - A product or system that can be plugged in, turned on, and operated with little or no additional configuring.

Uninterruptible Power Supply (UPS) - A backup power supply with enough power to allow a safe and orderly shutdown of the central processing unit should there be a disruption or shutdown of electricity.

UNIX - An operating system that supports multitasking and is ideally suited to multi-user applications (such as networks).

Uploading - Connecting to another computer and sending a copy of program or file to that computer. *SEE ALSO Downloading*
Useful Records - Records that are helpful but not required on a daily basis for continued operations.
User - A person or a process accessing an automated information system, either by direct or indirect connection.
User Contingency Procedures - Manual procedures to be implemented during a computer system outage.
User ID - A group of characters and/or numbers that uniquely identify an individual and are used to gain valid access to a computer system. A user id is normally coupled with a password that is set by the owner of the user id.
Value-Added Reseller (VAR) - A business that repackages and improves hardware manufactured by an original equipment manufacturer.
Virus - A code segment that replicates by attaching copies of itself to existing executable programs. This is usually done in such a manner that the copies will be executed when the file is loaded into memory, allowing them to infect still other files, and so on. The new copy of the virus is executed when a user executes the new host program. The virus may include any additional "payload" that is triggered when specific conditions are met. For example, some viruses display a text string on a particular date. There are many types of viruses including variants, overwriting, resident, stealth, and polymorphic. Viruses often have damaging side effects, sometimes intentionally, sometimes not.
Virus detection software - Software written to scan machine-readable media on computer systems. There are a growing number of reputable software packages available that are designed to detect and/or remove viruses. In addition, many utility programs can search text files for virus signatures or potentially unsafe practices.
Virus signature - A unique set of characters, which identify a particular virus. This may also be referred to as a virus marker.
Vital Records - Records or documents, for legal, regulatory, or operational reasons, cannot be irretrievably lost or damaged without materially impairing the organization's ability to conduct business.
Voice Recovery - The restoration of an organization's voice communications system.
Vulnerability - A weakness in an information system or component (e.g., security procedures, hardware design, internal controls) that could be exploited, attacked or fail. Vulnerabilities include susceptibility to physical dangers, such as fire or water, unauthorized access to sensitive data, entry of erroneous data, denial of timely service, fraud, etc.
Wide Area Network (WAN) - A network that uses high-speed, long-distance communications technology (e.g., phone lines and satellites) to connect computers over long distances. Similar to a LAN, except that parts of a WAN are geographically dispersed, possible in different cities or even on different continents. Public carriers like telecommunications carriers are included in most WANs; very large WANs may have incorporate satellite stations or microwave towers.
Warm Site - An alternate processing site which is only partially equipped (As compared to Hot Site which is fully equipped).
Web cache - A Web cache fills requests from the Web server, stores the requested information locally, and sends the information to the client; the next time the web cache

gets a request for the same information, it simply returns the locally cached data instead of searching over the Internet, thus reducing Internet traffic and response time.

Web site - A location on the World Wide Web that is owned and managed by an individual, company or organization; usually contains a home page and additional pages that include information provided by the site's owner, and may include links to other relevant sites.

World Wide Web (WWW) - A global hypertext system operating on the Internet that enables electronic communication of text, graphics, audio, and video.

Worm - A complete program that propagates itself from system to system, usually through a network or other communication facility. A worm is similar to a virus. It is able to infect other systems and programs usually by spawning copies of itself in each computer's memory. A worm differs from a virus, in that a virus replicates itself, while a worm does not. A worm copies itself to a person's workstation over a network or through a host computer and then spreads to other workstations. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system, either for fun or with intent to damage or destroy information. It can easily take over a network, as the "internet" worm did. The "internet" worm was intentionally released into the ARPANET (predecessor to the internet) by Robert Morris in 1976, as an experiment. Unlike a trojan horse, a worm enters a system uninvited.

XOR engine: Process or set of instructions that calculates data bit relationships in a RAID subsystem.

8 APPENDICES

All the items in this section should receive a separate appendix. In many cases information will be generated from the IMS database. Frequent updates and reviews should be made for this data. A printed copy should be made for inclusion in the Contingency Plan. However, as this is the dynamic information, the official record should be the IMS. Access to the IMS should be available from outside the *<Facility's>* normal operation location. IMS data should be stored in a location geographically separate from *<Facility's>* offices. A means to access this data from alternate locations should be in place and tested.

APPENDIX A – CONTINGENCY PLAN CONTACT INFORMATION

This appendix should include all points of contact of positions described in the Contingency Plan and key organizational personnel. Include home and mobile telephone numbers. Include emergency location assignments. Include a telephone tree, which lists the order of contact when a contingency situation or disaster is declared.

The contact list should indicate the system and organization within the *<Facility>* that each individual is associated with.

A reference list of emergency services and public utilities should be included.

APPENDIX B – EMERGENCY PROCEDURES

Include Emergency Procedures for *<Name>* and the Facility. Describe actions to be taken by employees emphasizing personnel safety. Address potential scenarios including fire, bomb threat or event, and civil disorders. Include evacuation procedures.

APPENDIX C – TEAM STAFFING AND TASKINGS

Include a roster and list of actions and responsibilities for each team created by *<Facility>* in Section 5.2. The following is an example of two tables for each team:

Role	***Name***
Contingency Plan Coordinator (Team Leader)	
Facilities Representative (To coordinate closely with Facility Engineer)	
Technical Representative (s)	

Pre-Contingency
Action 1
Action 2
Disaster Contingency Immediate Response
Action 1
Action 2
Post-Contingency
Action 1
Action 2

APPENDIX D – ALTERNATE SITE PROCEDURES

This appendix should include detailed procedures on standing up the selected alternate site(s). Include contact individuals and numbers, maps for reaching the facility, equipment on site that should be brought on line, equipment required for procurement, telecommunications providers for contact. There should be separate procedures based on the *<Facility's>* maintained availability of a hot site and a cold site.

APPENDIX E – DOCUMENTATION LIST

Include a list of all *<Name>*, *<Facility>,* and system documentation pertinent to the operation and maintenance of each system. This list should include but is not limited to system architecture, operating manuals, system security plans, risk assessments, MOUs, MOAs, SLAs, testing procedures and results, system interdependencies, asset inventory, hardware inventory, software inventory, backup procedures, configuration guidelines, alternate site status and inventory, and standard operating procedures.

Documentation must be developed, updated and/or modified to reflect the most current information and then entered into an automated DRP relational database. A copy should then be stored at the offsite storage facility. This data should be reviewed and modified as changes occur within the environment.

APPENDIX F – SOFTWARE INVENTORY

This appendix should be populated with the most current data that directly reflects the current software, being tested and evaluated, operational in the acceptance environment pending final review, implemented in production, owned whether onsite or offsite ,and deployed by the *<Facility>*. This should include the licensing agreements. A copy of this data should be stored at the offsite storage facility along with the Contingency Plan. An automated tool could assist with the development and implementation of this type of product.

APPENDIX G – HARDWARE INVENTORY

This appendix should be populated with the most accurate data reflective of the hardware assets currently owned and deployed by the <Facility>. In addition the inventory of the alternate site hardware assets should be included as well. The purchase and implementation of an automated tool could assist in this effort.

APPENDIX H – COMMUNICATIONS REQUIREMENTS

This appendix should include the most accurate data associated with the data and voice communications in place for *<Facility>*. It should include an inventory of all communications equipment, diagrams and uniquely identified data WAN and LAN circuits, data network backup alternatives, and voice network specifications.

APPENDIX I -VENDOR CONTACT LISTS

This appendix should be populated with the listing of all vendors and contractors that currently provide support or will provide support in a post-disaster environment. Additionally, any Service Level Agreements (SLAs) that have been executed and all subsequent modifications should be included with accurate Points of Contact (POCs) and emergency contact information.

APPENDIX J - EXTERNAL SUPPORT AGREEMENTS

This appendix should include documentation for service and emergency maintenance agreements with manufacturers, data storage facilities, telecommunications providers, and staff transportation providers. It should include points of contact and authorization procedures for delivery of services.

APPENDIX K - DATA CENTER/COMPUTER ROOM EMERGENCY PROCEDURES AND REQUIREMENTS

This appendix should include additional emergency procedures for all secured data center or computer room facilities hosting *<Facility>* systems. Information on fire, smoke, water, and intrusion alarms should be included. Power down procedures should be included. Facility layout, power requirements, cable diagrams, and media connection outlets should be included. A Data Center inventory should be extracted from Appendixes F, G, and H and included in this appendix.

APPENDIX L - PLAN MAINTENANCE PROCEDURES

This appendix should include the frequency of review for the plan. It can be divided into static information and dynamic information. This responsibility should be assigned to an individual associated with the Contingency Plan and included in their official job description.

APPENDIX M - CONTINGENCY LOG

This appendix should include the assessments and results of any exercise or real contingency operations. It should be written from available documentation after recovery and restoration. Include a comprehensive lessons learned documenting unanticipated difficulties, staff participation, restoration of system backups, permanent lost data and equipment, and shut down of temporary equipment used for the resumption, recovery, and restoration.