

DISASTER

RECOVERY

JOURNAL



Developed In Conjunction with **INTERNATIONAL**

Business Continuity Glossary

A

ACTIVATION: The implementation of business continuity capabilities, procedures, activities, and plans in response to an emergency or disaster declaration; the execution of the recovery plan. Similar terms: Declaration, Invocation.

ALERT: Notification that a potential disaster situation exists or has occurred; direction for recipient to stand by for possible escalation or activation of appropriate plans

ALTERNATE SITE: An alternate operating location to be used when the primary facilities are inaccessible. 1) Another location, computer center or work area designated for recovery. 2) Location, other than the main facility, that can be used to conduct business functions. 3) A location, other than the normal facility, used to process data and/or conduct critical business functions in the event the primary site is not available. SIMILAR TERMS: Alternate Processing Facility, Alternate Office Facility, Alternate Communication Facility, Backup Location, and Recovery Site.

ALTERNATE WORK AREA: Office recovery environment complete with necessary office infrastructure (desk, telephone, workstation, and associated hardware, communications, etc.); also referred to as Work Space or Alternative work site.

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.

ASSEMBLY AREA: The designated area at which employees, visitors, and contractors assemble when evacuated from their building/site.

AUDIT: The process by which procedures and/or documentation are measured against pre-agreed standards.

ASSET: An item of property and/or component of a business activity/process owned by an organization. There are three types of assets: physical assets (e.g. buildings and equipment); financial assets (e.g. currency, bank deposits and shares) and non-tangible assets (e.g. goodwill, reputation)

ASSOCIATE BUSINESS CONTINUITY INSTITUTE (ABCI): BCI Membership for entry-level professionals who are currently in the business continuity or related profession.

ASSOCIATIE BUSINESS CONTINUITY PLANNER (ABCP): DRI International, a non-profit corporation, certifies professionals and promotes credibility and professionalism in the business continuity industry. This is the entry level of certifications and achievable by a passing grade on an exam and approved application. Associated terms: Certified Business Continuity Professional (CBCP), Master Business Continuity Professional (MBCP).

ASYNCHONOUS REPLICATION: Data replication or mirror in which the application is allowed to continue while the data is mirrored to another site. In this case, the application data can represent a prior state of the application. It is critical to use ordered asynchronous mirroring for real-time applications. This means that each write is applied in the same order at the second or backup site as it was written in the primary site, even if the network has re-ordered the arrival of the data. Associated term: synchronous replication.

ANNUAL LOSS EXPOSURE/EXPECTANCY (ALE): A risk management method of calculating loss based on a value and level of frequency.

B

BACKLOG: The amount of work that accumulates when a system or process is unavailable. This work needs to be processed once the system or process is available and may take a considerable length of time to reduce. In extreme circumstances, this condition may become so large it may not be cleared or resolved.

BACKUP (Data): A process to copy electronic or paper based data in some form to be available if the original data is lost, destroyed or corrupted.

BACKUP GENERATOR: An independent source of power, usually fueled by diesel or natural gas.

BUSINESS CONTINUITY: The ability of an organization to ensure continuity of service and support for its customers and to maintain its viability before after and during an event.

BUSINESS CONTINUITY COORDINATOR: Designated individual responsible for preparing and coordinating the business continuity process. Similar term: disaster recovery coordinator, business recovery coordinator.

BUSINESS CONTINUITY PLAN ADMINISTRATOR: The designated individual responsible for plan documentation, maintenance, and distribution.

BUSINESS CONTINUITY MANAGEMENT (BCM): A holistic management process that identifies potential impacts that threaten an Organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities. The management of recovery or continuity in the event of a disaster. Also the management of the overall program through training, rehearsals, and reviews, to ensure the plan stays current and up to date.

BUSINESS CONTINUITY MANAGEMENT PROCESS: The Business Continuity Institute's BCM process (also known as the BC Life Cycle) combines 6 key elements: 1) Understanding Your Business 2) Continuity Strategies 3) Developing a BCM Response 4) Establishing a Continuity Culture 5) Exercising, Rehearsal & Testing 6) The BCM Management Process See: Business Continuity Lifecycle.

BUSINESS CONTINUITY MANAGEMENT PROGRAM: An ongoing management and governance process supported by senior management and resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products/services through exercising, rehearsal, testing, training, maintenance and assurance.
See: Disaster Recovery Program, Business

BUSINESS CONTINUITY MANAGEMENT TEAM: A group of individuals functionally responsible for directing the development and execution of the business continuity plan; as well as responsible for declaring a disaster and providing direction during the recovery process, both pre-disaster and post-disaster. Similar terms: disaster recovery management team, business recovery management team. Associated terms: crisis management team.

BUSINESS CONTINUITY PLANNING (BCP): Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change. SIMILAR TERMS: Contingency Planning, Disaster Recovery Planning, Business Resumption Planning, Continuity Planning,

BUSINESS CONTINUITY PROGRAM: An on-going program to ensure business continuity and recovery requirements are addressed, resources are allocated, and processes and procedures are completed and rehearsed. Most effective with management sponsorship and through regular rehearsals.

BUSINESS CONTINUITY STEERING COMMITTEE: A committee of decision makers, business owners, technology experts and continuity professionals, tasked with making strategic recovery and continuity planning decisions for the organization.

Copyright©- All Rights Reserved. Reproduction permission is granted to use in your organizations business continuity plan. Proper credit must be cited though. All other reproductions in whole or in part in any form or medium without the express written permission of Disaster Recovery Journal is prohibited. For reproduction permission, please contact us at drj@drj.com

BUSINESS CONTINUITY TEAM: Designated individuals responsible for developing, execution, rehearsals, and maintenance of the business continuity plan, including the processes and procedures. Similar terms: disaster recovery team, business recovery team, recovery team. Associated term: crisis response team.

BUSINESS IMPACT ANALYSIS (BIA): The business Impact Analysis is a process designed to identify critical business functions and workflow, determine the qualitative and quantitative impacts of a disruption, and to prioritize and establish recovery time objectives. SIMILAR TERMS: Business Exposure Assessment, Risk Analysis

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 an organization location.

BUSINESS INTERRUPTION COSTS: The costs or lost revenue associated with an interruption in normal business operations.

BUSINESS INTERRUPTION INSURANCE: Insurance coverage for disaster related expenses that may be incurred until operations are fully recovered after a disaster.

BUSINESS RECOVERY COORDINATOR: An individual or group designated to coordinate or control designated recovery processes or testing. SIMILAR TERMS: Disaster Recovery Coordinator

BUSINESS RECOVERY TIMELINE: The chronological sequence of recovery activities, or critical path, that must be followed to resume an acceptable level of operations following a business interruption. This timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.

BUSINESS RESUMPTION PLANNING (BRP): TERM Currently Being Reworked - SIMILAR TERMS: Business Continuity Planning, Disaster Recovery Planning

BUSINESS RECOVERY TEAM: A group of individuals responsible for maintaining the business recovery procedures and coordinating the recovery of business functions and processes. SIMILAR TERMS: Disaster Recovery Team

BUSINESS UNIT RECOVERY: The component of Disaster Recovery which deals specifically with the relocation of a key function or department in the event of a disaster, including personnel, essential records, equipment supplies, work space, communication facilities, work station computer processing capability, fax, copy machines, mail services, etc. SIMILAR TERMS: Work Group Recovery.

C

CALL TREE: A document that graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.

CERTIFIED BUSINESS CONTINUITY PROFESSIONAL (CBCP): The Disaster Recovery Institute International (DRI International), a not-for-profit corporation, certifies CBCPs and promotes credibility and professionalism in the business continuity industry. Also offers MBCP (Master Business Continuity Professional) and ABCP (Associate Business Continuity Professional).

CHECKLIST EXERCISE: A method used to exercise a completed disaster recovery plan. This type of exercise is used to determine if the information such as phone numbers, manuals, equipment, etc. in the plan is accurate and current.

COLD SITE: An alternate site that contains physical space and building infrastructure that must be provisioned at time of disaster to support recovery operations. **SIMILAR TERMS:** Shell Site; Backup Site; Recovery Site; Alternate Site

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:** Telecommunications Recovery, Data Communications Recovery

COMPUTER RECOVERY TEAM: A group of individuals responsible for assessing damage to the original system, processing data in the interim, and setting up the new 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.

COMMAND CENTER: A physical or virtual facility located outside of the affected area used to gather, assess, and disseminate information and to make decisions to effect recovery.

CONTACT LIST: A list of team members and/or key players to be contacted including their backups. The list will include the necessary contact information (i.e. home phone, pager, cell, etc.) and in most cases be considered confidential.

CONTINGENCY PLANNING: Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances.

CONTINGENCY PLAN: A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations. A contingency plan may use any number of resources including workaround procedures, an alternate work area, a reciprocal agreement, or replacement resources.

CONTINUITY OF OPERATIONS PLAN (COOP): A COOP provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. This term traditionally is used by the Federal Government and its supporting agencies to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning.

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, Drop Ship, 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 MANAGEMENT TEAM: A crisis management team will consist of key executives as well as key role players (i.e. media representative, legal counsel, facilities manager, disaster recovery coordinator, etc.) and the appropriate business owners of critical organization functions

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 that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization.

CRITICAL INFRASTRUCTURE: Systems whose incapacity or destruction would have a debilitating impact on the economic security of an organization, community, nation, etc

CRITICAL RECORDS: Records or documents that, if damaged or destroyed, would cause considerable inconvenience and/or require replacement or recreation at considerable expense.

D

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 BACKUPS: The back up of system, application, program and/or production files to media that can be stored both on and/or offsite. Data backups can be used to restore corrupted

or lost data or to recover entire systems and databases in the event of a disaster. Data backups should be considered confidential and should be kept secure from physical damage and theft.

DATA BACKUP STRATEGIES: Those actions and backup processes determined by an organization to be necessary to meet its data recovery and restoration objectives. Data backup strategies will determine the timeframes, technologies, media and offsite storage of the backups, and will ensure that recovery point and time objectives can be met.

DATA CENTER RECOVERY: The component of Disaster Recovery which deals with the restoration, at an alternate location, of data centers services and computer processing capabilities. **SIMILAR TERMS:** Mainframe Recovery, Technology Recovery.

DATA RECOVERY: The restoration of computer files from backup media to restore programs and production data to the state that existed at the time of the last safe backup.

DATABASE REPLICATION: The partial or full duplication of data from a source database to one or more destination databases. Replication may use any of a number of methodologies including mirroring or shadowing, and may be performed synchronous, asynchronous, or point-in-time depending on the technologies used, recovery point requirements, distance and connectivity to the source database, etc. Replication can if performed remotely, function as a backup for disasters and other major outages. (Similar Terms: File Shadowing, Disk Mirroring)

DECLARATION: A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged mitigating actions (e.g. a move to an alternate site.)

DECLARATION FEE: A one-time fee, charged by an Alternate Facility provider, to a customer who declares a disaster. **NOTE:** Some recovery vendors apply the declaration fee against the first few days of recovery. 1) An initial fee or charge for implementing the terms of a recovery agreement or contract. **SIMILAR TERMS:** Notification Fee.

DEPENDENCY: The reliance, directly or indirectly, of one activity or process upon another. See: Mission Critical Activity

DESK CHECK: One method of testing a specific component of a plan. Typically, the owner or author of the component reviews it for accuracy and completeness and signs off.

DESKTOP EXERCISE: See: Table Top Exercise.

DISASTER: A sudden, unplanned calamitous event causing great damage or loss as defined or determined by a risk assessment and BIA; 1) Any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time. 2) In the business environment, any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time. 3) The period when company management decides to divert from normal production responses and exercises its disaster recovery plan. Typically signifies the beginning of a move from a primary to an alternate location. **SIMILAR TERMS:** Business Interruption; Outage; Catastrophe

Copyright©- All Rights Reserved. Reproduction permission is granted to use in your organizations business continuity plan. Proper credit must be cited though. All other reproductions in whole or in part in any form or medium without the express written permission of Disaster Recovery Journal is prohibited. For reproduction permission, please contact us at drj@drj.com

DISASTER RECOVERY: Activities and programs designed to return the entity to an acceptable condition. 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 OR BUSINESS CONTINUITY COORDINATOR: A role of the BCM program that coordinates planning and implementation for overall recovery of an organization or unit(s). **SIMILAR ROLES:** Business Recovery Coordinator, Business Recovery Planner, Disaster Recovery Planner, Disaster Recovery Administrator

DISASTER RECOVERY INSTITUTE INTERNATIONAL (DRI INTERNATIONAL): A not-for-profit organization that offers certification and educational offerings for business continuity professionals.

DISASTER RECOVERY PLAN: The management approved document that defines the resources, actions, tasks and data required to manage the recovery effort. Usually refers to the technology recovery effort. This is a component of the BCM Program. See: BCM Plan, Recovery Plan.

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 MIRRORING: Disk mirroring is the duplication of data on separate disks in real time to ensure its continuous availability, currency and accuracy. Disk mirroring can function as a disaster recovery solution by performing the mirroring remotely. True mirroring will enable a zero recovery point objective. Depending on the technologies used, mirroring can be performed synchronously, asynchronously, semi-synchronously, or point-in-time. Similar terms: data mirroring, data replication, file shadowing, journaling

E

ELECTRONIC VAULTING: Electronically forwarding backup data to an offsite server or storage facility. Vaulting eliminates the need for tape shipment and therefore significantly shortens the time required to move the data offsite. Similar terms: vaulting, electronic backup. Associated terms: electronic journaling.

EMERGENCY: An unexpected actual or impending situation that may cause injury, loss of life, destruction of property or cause the interference, loss or disruption of an organization's normal business operations to such an extent that it poses a threat.

EMERGENCY COORDINATOR: The person assigned the role of coordinating the activities of the evacuation of a site and/or building with the statutory and/or emergency services.

EMERGENCY OPERATIONS CENTER (EOC): A site from which response teams/officials (municipal, county, state and federal) exercise direction and control in an emergency or disaster. Associated term: command center.

EMERGENCY PREPAREDNESS: The discipline that ensures an organization or community's readiness to respond to an emergency in a coordinated, timely, and effective manner to prevent the loss of life and minimize injury and property damage.

EMERGENCY PROCEDURES: A plan of action to commence immediately to prevent the loss of life and minimize injury and property damage.

EMERGENCY RESPONSE TEAM (ERT): Teams of individuals who have been trained to provide rapid response to all type of emergencies and to provide assistance and act as a contact to responding outside agencies. Associated term: medical emergency response team (MERT).

ENVIRONMENT RESTORATION: Recreation of the critical business operations in an alternate location, including people, equipment and communications capability.

ESCALATION: The process by which event related information is communicated upwards through an organization's Business Continuity and/or risk management reporting process.

ESSENTIAL SERVICE: A service without which a building would be 'disabled'. Often applied to the utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks.

EVACUATION: The movement of employees, visitors and contractors from a site and/or building to a safe place (assembly area) in a controlled and monitored manner at time of an event.

EVENT: Any occurrence that may lead to an incident or crisis.
See: Incident, crisis

EXECUTIVE / MANAGEMENT SUCCESSION: A predetermined plan for ensuring the continuity of authority, decision-making, and communication in the event that key members of senior management suddenly become incapacitated, or in the event that a crisis occurs while key members of senior management are unavailable.

EXERCISE: An announced or unannounced execution of business continuity plans intended to implement existing plans and/or highlight the need for additional plan development. An activity that is performed for the purpose of training and conditioning team members, improving their performance, and validating the business continuity plan.. Types of exercises include: Table Top Exercise, Simulation Exercise, Operational Exercise, and Mock Disaster. See: Desktop Exercise, Full Rehearsal.

EXERCISE CONTROLLER: A role that is appointed to have overall management oversight and control of the exercise and the authority to alter the exercise plan. This also includes the early termination of the exercise for reasons of safety or the aim(s)/objective(s) of the exercise cannot be met due to an unforeseen or other internal or external influence.

EXERCISE DIRECTOR: A role in both tabletop and command center or live exercises. They have access to details of the whole exercise plan and ensure that it proceeds to plan. They are responsible for the mechanics of running the exercise.

EXERCISE OBSERVER: An exercise observer has no role within the exercise but is employed to observe the exercise to either assess the preparations of the organization or the exercise players (individually or team) or to learn lessons or training or awareness. Their role in subsequent debriefing is crucial.

EXERCISE AUDITOR: A role within the exercise that is employed to assess whether the exercise aim(s)/objective(s) are being met and to measure whether activities are occurring at the right time and involve the correct people to facilitate their achievement. The exercise auditor does not have responsibility for the mechanics of the exercise. Their role in the subsequent debriefing is crucial.

EXPOSURE: The potential susceptibility to loss; the vulnerability to a particular risk.

EXTRA EXPENSE: The extra cost necessary to implement a recovery strategy and/or mitigate a loss. An example is the cost to transfer inventory to an alternate location to protect it from further damage, cost of reconfiguring lines, overtime costs, etc. Typically reviewed during BIA and is a consideration during insurance evaluation.

F

FILE SHADOWING: The asynchronous duplication of the production database on separate media to ensure data availability, currency and accuracy. File shadowing can be used as a disaster recovery solution if performed remotely, to improve both the recovery time and recovery point objectives. **SIMILAR TERMS:** Data Replication, Journaling, Disk Mirroring.

FINANCIAL IMPACT: The asynchronous duplication of the production database on separate media to ensure data availability, currency and accuracy. File shadowing can be used as a disaster recovery solution if performed remotely, to improve both the recovery time and recovery point objectives. **SIMILAR TERMS:** Data Replication, Journaling, Disk Mirroring.

Copyright©- All Rights Reserved. Reproduction permission is granted to use in your organizations business continuity plan. Proper credit must be cited though. All other reproductions in whole or in part in any form or medium without the express written permission of Disaster Recovery Journal is prohibited. For reproduction permission, please contact us at drj@drj.com

FIREWALL V0001: Technology designed to prevent unauthorized access to specific places on the Internet. Generally used by organizations to ensure that unauthorized access is not obtained to internal network and resources.

FORWARD RECOVERY: The process of recovering a database to the point of failure by applying active journal or log data to the current backup files of the database.

G

H

HAZARD OR THREAT IDENTIFICATION: The process of identifying situations or conditions that have the potential to cause injury to people, damage to property, or damage to the environment.

HIGH AVAILABILITY: Systems or applications requiring a very high level of reliability and availability. High availability systems typically operate 24x7 and usually require built in redundancy built-in redundancy to minimize the risk of downtime due to hardware and/or telecommunication failures.

HIGH-RISK AREAS: Heavily populated areas, particularly susceptible to high-intensity earthquakes, floods, tsunamis, or other disasters, for which emergency response may be necessary in the event of a disaster.

HOTSITE: An alternate facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems.

HUMAN THREATS: Possible disruptions in operations resulting from human actions. (i.e., disgruntled employee, terrorism, blackmail, job actions, riots, etc.)

I

INCIDENT COMMAND SYSTEM (ICS): Combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure with responsibility for management of assigned resources to effectively direct and control the response to an incident. Intended to expand, as situation requires larger resources, without requiring new, reorganized command structure. (NEMA Term)

INCIDENT MANAGER: Commands the local EOC reporting up to senior management on the recovery progress. Has the authority to invoke the local recovery plan.

INCIDENT RESPONSE: The response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.

INTEGRATED TEST: A test conducted on multiple components of a plan, in conjunction with each other, typically under simulated operating conditions

INTERIM SITE: A temporary location used to continue performing business functions after vacating a recovery site and before the original or new home site can be occupied. Move to an interim site may be necessary if ongoing stay at the recovery site is not feasible for the period of time needed or if the recovery site is located far from the normal business site that was impacted by the disaster. An interim site move is planned and scheduled in advance to minimize disruption of business processes; equal care must be given to transferring critical functions from the interim site back to the normal business site.

INTERNAL HOTSITE: A fully equipped alternate processing site owned and operated by the organization.

J

JOURNALING: The process of logging changes or updates to a database since the last full backup. Journals can be used to recover previous versions of a file before updates were made, or to facilitate disaster recovery, if performed remotely, by applying changes to the last safe backup. SIMILAR TERMS: File Shadowing, Data Replication, Disk Mirroring.

K

L

LAN RECOVERY: The component of business continuity that deals specifically with the replacement of LAN equipment and the restoration of essential data and software in the event of a disaster. SIMILAR TERM: Client/Server Recovery.

LINE REROUTING: A short-term change in the routing of telephone traffic, which can be planned and recurring, or a reaction to an outage situation. Many regional telephone companies offer service that allows a computer center to quickly reroute a network of dedicated lines to a backup site.

LOSS REDUCTION: The technique of instituting mechanisms to lessen the exposure to a particular risk. Loss reduction involves planning for, and reacting to, an event to limit its impact. Examples of loss reduction include sprinkler systems, insurance policies, and evacuation procedures.

LOST TRANSACTION RECOVERY: Recovery of data (paper within the work area and/or system entries) destroyed or lost at the time of the disaster or interruption. Paper documents may need to be requested or re-acquired from original sources. Data for system entries may need to be recreated or reentered.

M

MISSION-CRITICAL APPLICATION: An application that is essential to the organization's ability to perform necessary business functions. Loss of the mission-critical application would have a negative impact on the business, as well as legal or regulatory impacts.

MOBILE RECOVERY: A mobilized resource purchased or contracted for the purpose of business recovery. The mobile recovery center might include: computers, workstations, telephone, electrical power, etc.

MOCK DISASTER: One method of exercising teams in which participants are challenged to determine the actions they would take in the event of a specific disaster scenario. Mock disasters usually involve all, or most, of the applicable teams. Under the guidance of exercise coordinators, the teams walk through the actions they would take per their plans, or simulate performance of these actions. Teams may be at a single exercise location, or at multiple locations, with communication between teams simulating actual 'disaster mode' communications. A mock disaster will typically operate on a compressed timeframe representing many hours, or even days.

N

NATURAL THREATS: Events caused by nature that have the potential to impact an organization.

NETWORK OUTAGE: An interruption in system availability resulting from a communication failure affecting a network of computer terminals, processors, and/or workstations.

O

OFF-SITE STORAGE: Alternate facility, other than the primary production site, where duplicated vital records and documentation may be stored for use during disaster recovery.

OPERATIONAL EXERCISE: One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. Operational exercises,

Copyright©- All Rights Reserved. Reproduction permission is granted to use in your organizations business continuity plan. Proper credit must be cited though. All other reproductions in whole or in part in any form or medium without the express written permission of Disaster Recovery Journal is prohibited. For reproduction permission, please contact us at drj@drj.com

which may involve one or more teams, are typically performed under actual operating conditions at the designated alternate location, using the specific recovery configuration that would be available in a disaster.

OPERATIONAL IMPACT ANALYSIS: Determines the impact of the loss of an operational or technological resource. The loss of a system, network or other critical resource may affect a number of business processes.

OPERATIONAL TEST: A test conducted on one or more components of a plan under actual operating conditions.

P

PLAN ADMINISTRATOR: The individual responsible for documenting recovery activities and tracking recovery progress.

PEER REVIEW: One method of testing a specific component of a plan. Typically, the component is reviewed for accuracy and completeness by personnel (other than the owner or author) with appropriate technical or business knowledge.

PLAN MAINTENANCE PROCEDURES: Maintenance procedures outline the process for the review and update of business continuity plans.

R

RECIPROCAL AGREEMENT: Agreement between two organizations (or two internal business groups) with basically the same equipment/same environment that allows each one to recover at each other's site.

RECOVERY: Process of planning for and/or implementing expanded operations to address less time-sensitive business operations immediately following an interruption or disaster. 1) The start of the actual process or function that uses the restored technology and location.

RECOVERY PERIOD: The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.

(RECOVERY SERVICES CONTRACT): A contract with an external organization guaranteeing the provision of specified equipment, facilities, or services, usually within a specified time period, in the event of a business interruption. A typical contract will specify a monthly subscription fee, a declaration fee, usage costs, method and amount of testing, termination options, penalties and liabilities, etc.

RECOVERY STRATEGY: An approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major outage. Plans and methodologies are

determined by the organizations strategy. There may be more than one methodology or solution for an organizations strategy. Examples of methodologies and solutions include, contracting for Hotsite or Coldsite, building an internal Hotsite or Coldsite, identifying an Alternate Work Area, a Consortium or Reciprocal Agreement, contracting for Mobile Recovery or Crate and Ship, and many others.

RECOVERY POINT OBJECTIVE (RPO): The point in time to which systems and data must be recovered after an outage. (e.g. end of previous day's processing). RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that may need to be recreated after the systems or functions have been recovered.

RECOVERY TIME OBJECTIVE (RTO): The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. **SIMILAR TERMS:** Maximum Allowable Downtime.

RESPONSE: The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required. In addition to addressing matters of life safety and evacuation, Response also addresses the policies, procedures and actions to be followed in the event of an emergency. 1) The step or stage that immediately follows a disaster event where actions begin as a result of the event having occurred. **SIMILAR TERMS:** Emergency Response, Disaster Response, Immediate Response, and Damage Assessment.

RESTORATION: Process of planning for and/or implementing procedures for the repair or relocation of the primary site and its contents, and for the restoration of normal operations at the primary site.

RESUMPTION: The process of planning for and/or implementing the restarting of defined business operations following a disaster, usually beginning with the most critical or time-sensitive functions and continuing along a planned sequence to address all identified areas required by the business. 1) The step or stage after the impacted infrastructure, data, communications and environment has been successfully re-established at an alternate location.

RISK: Potential for exposure to loss. Risks, either man-made or natural, are constant. The potential is usually measured by its probability in years.

RISK ASSESSMENT / ANALYSIS: Process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

RISK MITIGATION: Implementation of measures to deter specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner.

S

SALVAGE & RESTORATION: The process of reclaiming or refurbishing computer hardware, vital records, office facilities, etc. following a disaster.

SIMULATION EXERCISE: One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises, which may involve one or more teams, are performed under conditions that at least partially simulate 'disaster mode'. They may or may not be performed at the designated alternate location, and typically use only a partial recovery configuration.

STANDALONE TEST: A test conducted on a specific component of a plan, in isolation from other components, typically under simulated operating conditions.

STRUCTURED WALKTHROUGH: One method of testing a specific component of a plan. Typically, a team member makes a detailed presentation of the component to other team members (and possibly non-members) for their critique and evaluation.

SUBSCRIPTION: Contract commitment that provides an organization with the right to utilize a vendor recovery facility for processing capability in the event of a disaster declaration.

SYSTEM DOWNTIME: A planned or unplanned interruption in system availability.

T

TABLE TOP EXERCISE: One method of exercising teams in which participants review and discuss the actions they would take per their plans, but do not perform any of these actions. The exercise can be conducted with a single team, or multiple teams, typically under the guidance of exercise facilitators.

TEST: An activity that is performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Types of tests include: Desk Check, Peer Review, Structured Walkthrough, Standalone Test, Integrated Test, and Operational Test.

TEST PLAN: A document designed to periodically exercise specific action tasks and procedures to ensure viability in a real disaster or severe outage situation.

U

UNINTERRUPTIBLE POWER SUPPLY (UPS): A backup supply that provides continuous power to critical equipment in the event that commercial power is lost.

V

VITAL RECORD: A record that must be preserved and available for retrieval if needed.

W

WARM SITE: An alternate processing site which is equipped with some hardware, and communications interfaces, electrical and environmental conditioning which is only capable of providing backup after additional provisioning, software or customization is performed.

WORKAROUND PROCEDURES: Interim procedures that may be used by a business unit to enable it to continue to perform its critical functions during temporary unavailability of specific application systems, electronic or hard copy data, voice or data communication systems, specialized equipment, office facilities, personnel, or external services. **SIMILAR TERMS:** Interim Contingencies.

X

Y

Z