

# Acronyms and Definitions

- Alert
  - Notification that a potential disaster situation is imminent exists or has occurred; usually includes a directive for personnel. To stand by for possible activation.
- Alternate Site
  - An alternate operating location to be used by business functions 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 of a disaster.
- Alternate Work Area
  - Recovery environment complete with necessary infrastructure (desk, telephone, workstation, and associated hardware and equipment, communications, etc.)
- Backup (Data)
  - A process by which data, electronic or paper-based, is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted.
- Business Continuity
  - The capability of an organization to continue delivery of products and services at acceptable predefined levels following a disruptive event.
- Business Continuity Coordinator
  - A role within the business continuity program that coordinates planning and implementation for overall recovery of an organization or unit(s).
- Business Continuity Plan (BCP)
  - Process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption.
- Business Impact Analysis (BIA)
  - A process designed to prioritize business essential functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact

that might result if an organization was to experience an incident, from minor to catastrophic.

- 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.
- Contact List
  - A list of team members and/or key personnel to be contacted including their backups. The list will include the necessary contact information (i.e. home phone, pager, cell, etc.) and in many cases it is considered confidential.
- 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. The Federal Government and its supporting agencies traditionally use this term to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning.
- Cost Benefit Analysis
  - A process after a BIA and risk assessment) that facilitates the financial assessment of different strategic BCM options and balances the cost of each option against the perceived savings.
- Critical/Essential Business Functions
  - The critical operational and/or business support functions that could not be interrupted or unavailable for more than a mandated or predetermined time frame without significantly jeopardizing the organization. An example of a business function is a logical grouping of processes/activities that produce a product and/or service such as Accounting, Staffing, Customer Service, etc.
- Disaster
  - A sudden, unplanned catastrophic event causing unacceptable damage or loss. 1) An event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time 2) An event where an organization's management invokes their recovery plans.
- Emergency
  - An unexpected 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 Operations Center (EOC)
  - The physical and/or virtual location from which strategic decisions are made and all activities of an event/incident/crisis are directed, coordinated and monitored.
- Emergency Preparedness
  - The capability that enables an organization or community 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 Response
  - The immediate reaction and response to an emergency situation commonly focusing on ensuring life safety and reducing the severity of the incident.
- Emergency Response Plan
  - A documented plan usually addressing the immediate reaction and response to an emergency situation.
- Emergency Response Procedures
  - The initial response to any event and is focused upon protecting human life and the organization's assets.
- Event
  - Any occurrence that may lead to a business continuity incident.
- Exercise
  - A people focused activity designed to execute business continuity plans and evaluate the individual and/or organization performance against approved standards or objectives. Exercises can be announced or unannounced and are performed for the purpose of training and conditioning team members and validating the business continuity plan. Exercise results identify plan gaps and limitations and are used to improve and revise the Business Continuity Plans. Types of exercises include: Tabletop Exercise, Simulation Exercise, Operational Exercise, Mock Disaster, Desktop Exercise, Full Rehearsal.
- Gap Analysis
  - A detailed examination to identify risks associated with the differences between Business/Operations requirements and the current available recovery capabilities.
- Incident

- An event which is not part of a standard operating business which may impact or interrupt services and, in some cases, may lead to disaster.
- Recovery
  - Implementing the prioritized actions required to return the processes and support functions to operational stability following an interruption or disaster.
- Recovery Period
  - The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.
- Recovery Point Objective (RPO)
  - The point in time to which data is restored and/or systems are recovered after an outage. RPO is often used as the basis for developing backup strategies and determining the amount of data that may require recreation after systems have been recovered. RPO for applications can be enumerated in business time (i.e., “8 business hours” after a Sunday disaster restores to close of business Thursday) or elapsed time but is always measured in terms of time before a disaster. RPO for systems typically must be established at time of disaster as a specific point in time (e.g., end of previous day’s processing) or software version/release.
- Recovery Time Objective (RTO)
  - The demonstrated amount of time in which systems, applications and/or functions have been recovered, during an exercise or actual event, at the designated recovery/alternate location (physical or virtual). As with RTO, RTC includes assessment, execution and verification activities. RTC and RTO are compared during gap analysis. The period of time within which systems, applications, or functions must be recovered after an outage. RTO includes the time required for: assessment, execution and verification. RTO may be enumerated in business time (e.g. one business day) or elapsed time (e.g. 24 elapsed hours). Assessment includes the activities which occur before or after an initiating event, and lead to confirmation of the execution priorities, timeline and responsibilities, and a decision regarding when to execute. Execution includes the activities related to accomplishing the pre-planned steps required within the phase to deliver a function, system or application in a new location to its owner. Verification includes steps taken by a function, system or application owner to ensure everything is in readiness to proceed to live operations.
- Recovery Timeline

- The sequence of recovery activities, or critical path, which must be followed to resume an acceptable level of operation following a business interruption. The timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.
- 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.
- Vital Records
  - Records essential to the continued functioning or reconstitution of an organization during and after an emergency and those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities.