



GLOSSARY OF BUSINESS CONTINUITY TERMS

A • B • C • D • E • F • G • H • I • J • K • L • M • N • O • P • Q • R • S • T • U • V • W • X • Y • Z

NOTE: This glossary provides the general terminology of *Business Continuity (BC)*. Most of the terms are used in the business continuity community with the exception of the terms marked with an asterisk (*). These asterisk terms are specifically created for the understanding of *UC Ready*, the software planning tool for developing your business continuity plan.

A

ACTION ITEM*: An action item is something that could be done now (or anytime before disaster strikes) to make your organization more prepared. Action items can be big or small, costly or costless, within the scope of your department to perform, or outside your scope. Taken together, a department's action items comprise a **to-do list for readiness**.

The typical Action Item begins with a verb and can be stated in one sentence. Some examples:

- Do seismic bracing in all department laboratories.
- Develop a plan for redeploying nursing staff to critical areas.
- Cross-train two staff members to handle payroll & purchasing.
- Make an emergency contact list and ask all staff to keep a copy at home.

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.

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: 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.

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

B

BACKLOG: a) The amount of work that accumulates when a system or process is unavailable for a long period of time. This work needs to be processed once the system or process is available and may take a considerable amount of time to process. b) A situation whereby a backlog of work requires more time than is available through normal working patterns. In extreme circumstances, the backlog may become so large that the backlog cannot be cleared.

BROADBAND CONNECTION*: Broadband describes an internet connection that is faster than dial-up. The usual at-home broadband connections are DSL (telephone), cable, and wireless.

BUSINESS CONTINUITY: The ability of an organization to ensure continuity of service and support 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 MANAGER: The designated individual responsible for plan documentation, maintenance, and distribution.

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 coordinate the efforts of Emergency Management, Business Continuity Planning and Disaster Recovery. The program also guides the divisions to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of services.

BUSINESS CONTINUITY MANAGEMENT TEAM: A group of individuals functionally responsible for directing the development and execution of the business continuity plan and providing consultation during the recovery process, both pre-disaster and post-disaster.

BUSINESS CONTINUITY PLAN (BCP): Advance arrangements and procedures that enable an organization to respond to an event in such a manner that mission critical functions continue with planned levels of interruption or essential change.

BUSINESS CONTINUITY PLANNING (BCP): The 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.

BUSINESS IMPACT ANALYSIS (BIA)/RISK ASSESSMENT: 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.

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's location. Similar terms: outage, service interruption.

C

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

CENTRALLY-OWNED APPLICATION*: A computer application or system whose technical owner is your central IT department. (The functional owner of the application could be any department.)

CLUSTERED DEPARTMENTS*: Departments that share administrative staff.

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.

CONSEQUENCES*: For the purposes of the UC Ready tool, harmful consequences of slow recovery may impact the Critical Functions of a department such as disruption of teaching and departure of faculty and students.

CONTINUITY PLAN*: **Continuity planning** addresses the question: how can we prepare to **continue operations** despite those adverse events that we call disasters and if we can't continue, how can we **resume our operations** rapidly and gracefully? The mission of the University of California is teaching, research, public service, and patient care. These four enterprises, along with the infrastructure that supports them, are the focus of our continuity planning.

Your departmental continuity plan:

- Identifies your department's critical functions.
- Describes how you might carry on these functions under conditions of diminished resources (diminished staff, space, equipment, or IT infrastructure).
- Contains various information that will be needed during and after the disaster event.
- Describes how we can prepare. This is most important of all, because "a stitch in time does indeed save nine." A good continuity plan will identify action items - things that we can do now to lessen the impact of disaster events and make it easier to recover.

COST CENTER*: An accounting term denoting a department that incurs costs but does not directly produce revenue. In some organizations, this term is loosely used to divide up the organization for the purposes of allocating budget (with no reference to revenue or profit).

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 FUNCTION*: A Critical Function is an activity that is essential to the core mission of the organization. For disaster planning, a Critical Function is one that must be continued through disaster, or resumed soon after a disaster-event, to ensure either the viability of the organization or its ability to serve its customers.

The UC Ready methodology defines **four levels of criticality:**

- **CRITICAL 1:** Must be continued at normal or increased service load. Cannot pause. Necessary to life, health, and security. (Examples: inpatient care, police services).
- **CRITICAL 2:** Must be continued if at all possible, perhaps in reduced mode. Pausing completely will have grave consequences. (Examples: provision of care to at-risk outpatients, functioning of data networks, at-risk research)
- **CRITICAL 3:** May pause if forced to do so, but must resume in 30 days or sooner. (Examples: classroom instruction, research, payroll, student advising)
- **DEFERRABLE:** May pause; resume when conditions permit. (Examples: elective surgery, routine building maintenance, training, marketing).

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-GATHERING FORM*: A data-gathering form is typically a paper form that is used to collect information for later entry into a database. Examples are

- templates for taking hand-written notes while interviewing a subject
- paper survey instruments
- substitute paper forms that are kept available for use during periods when a computer system is down.

DEPARTMENTALLY-OWNED APPLICATION*: A computer application or system whose technical owner is your department or another department (but not central IT).

DEPENDENCY: The reliance, directly or indirectly, of one activity or process upon another.

DISASTER RECOVERY COORDINATOR: An individual or group designated to coordinate or control designated recovery processes or testing.

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 preparation that is necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster.

DISASTER RECOVERY TEAM: A group of individuals responsible for maintaining the business recovery procedures and coordinating the recovery of business functions and processes.

DOCUMENTS*: For continuity planning, you will identify any documents that are very important to a particular Critical Function. They can be individual documents (such as policy manuals) or sets of records (such as patient files, research files, vendor invoices, etc.). The documents listed under Critical Functions may be paper or electronic. Do not include records that are stored within a database application such as a financial system, HR system, or medical records system, etc. These will be treated elsewhere.

DOWNSTREAM DEPENDENCY*: A department that depends on your department. If your department fails to perform, the ability of the downstream department to carry out its mission will be seriously impaired. For example, if your department does scheduling of nursing staff, the inpatient and/or clinical units will be among your downstream dependencies.

E

EMERGENCY CONTACT LIST*: List of all people in your unit, and perhaps some outside your unit, whom you might want to contact during and after a disaster-event. The list should include home address, home phone, personal & work cell phones, personal and work email addresses, plus any other available means of contact. The list should be kept on paper and stored in multiple locations by multiple people. It should be updated at appropriate intervals. Some emergency contact lists are organized as “calling trees”, in very large units but that is not usually necessary.

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 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).

EVENT: Any occurrence that may lead to a business continuity incident. See: Crisis and Incident

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: 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: Table Top Exercise, Simulation Exercise, Operational Exercise, Mock Disaster, Desktop Exercise, Full Rehearsal.

F

FUNCTION (NORMAL)*: These are functions that you normally perform. Some typical examples are:

- Laboratory research
- Classroom instruction
- Non-elective surgery
- Purchasing
- Paying employees
- Inpatient care
- Course scheduling
- Providing meals
- Facilities repair
- Pharmacy services
- Grant accounting

FUNCTIONAL OWNER*: The functional owner of an IT application is the unit that governs the design (and often the use) of the application. When an application implements a business process, the unit responsible for that business process is typically regarded as the functional owner of the application. Modifications to an application must be authorized by the functional owner (but are implemented by the technical owner). For example, the Admissions Office would typically be the functional owner of the on-line admissions system. The technical owner might be the Central IT department, or could be the Admissions Office itself if it has its own IT person or section.

H

HEALTH AND SAFETY: The process by which the well being of all employees, contractors, visitors, and the public is safeguarded. All business continuity plans and planning must be cognizant of Health and Safety statutory and regulatory requirements and legislation. Health and Safety considerations should be reviewed during the Risk assessment.

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

I

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.

INFORMATION SECURITY: The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization.

M

MANUAL PROCEDURES: An alternative method of working following a loss of IT systems. As working practices rely more and more on computerized activities, the ability of an organization to fall back on manual alternatives lessens. However, temporary measures and methods of working can help mitigate the impact of a business continuity event and give staff a feeling of doing something.

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.

N

NETWORK OUTAGE: An interruption of voice, data, or IP network communications.

O

OFFSITE STORAGE*: Offsite storage refers to the storage of tapes, disks, paper documents, and other materials at a location far enough from an organization's operating location that a disaster-event at one location is not likely to impact the other location.

ONSITE STORAGE*: Onsite storage refers to the storage of tapes, disks, paper documents, and other materials at an organization's operating location rather than elsewhere. Onsite storage of backups is adequate for protection against some types of disasters and is less expensive and more-quickly-accessed than offsite storage. For more valuable and less-replaceable items, offsite storage becomes desirable.

P

PEAK PERIODS*: These are months when you would expect there to be especially high activity involved in accomplishing a Critical Function. This might be a peak workload period such as the annual fiscal closing for accounting functions or it might denote activities that happen only at certain times - such as course registration that happens once per semester.

PLAN MAINTENANCE: The management process of keeping an organization's Business continuity management plans up to date and effective. Maintenance procedures are a part of this process for the review and update of the BC plans on a defined schedule. Maintenance procedures are a part of this process.

PREVENTATIVE MEASURES: Controls aimed at deterring or mitigating undesirable events from taking place.

R

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

RECOVERY POINT OBJECTIVE (RPO): From a business perspective, RPO is the maximum amount of data loss the business can incur in an event. The targeted point in time to which systems and data must be recovered after an outage as determined by the business unit.

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). RTO's 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

RESUMPTION: The process of planning for and/or implementing the restarting of defined business processes and operations following a disaster. This process commonly addresses the most critical business functions within BIA specified timeframes.

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 CATEGORIES: Risks of similar types are grouped together under key headings, otherwise known as "risk categories". These categories include reputation, strategy, financial, investments, operational infrastructure, business, regulatory compliance, outsourcing, people, technology, and knowledge.

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

SCENARIO: A pre-defined set of Business Continuity events and conditions that describe, for planning purposes, an interruption, disruption, or loss related to some aspect(s) of an organization's business operations to support conducting a BIA, developing a continuity strategy, and developing continuity and exercise plans. Note: Scenarios are neither predictions nor forecasts.

SPONSOR*: Sponsor refers to an agency or organization that provides grant funding for research projects.

T

TABLE TOP EXERCISE: One method of exercising teams in which participants review and discuss the actions they would take according to 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.

TECHNICAL OWNER*: The technical owner of an IT application is the unit that has top-level administrator and programming access, implements any modifications, and troubleshoots and fixes any technical problems.

U

UNEXPECTED LOSS: The worst-case financial loss or impact that a business could incur due to a particular loss event or risk. The unexpected loss is calculated as the expected loss plus the potential adverse volatility in this value. It can be thought of as the worst financial loss that could occur in a year over the next 20 years.

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

UPSTREAM DEPENDENCY*: An upstream dependency is a department that **your** department depends on. If the upstream department fails to perform, the ability of your department to carry out its mission will be seriously impaired. For example, the central IT department is typically an upstream dependency of most departments. The Sponsored Projects office (grants office) is an upstream dependency of the research enterprise. The food services department is an upstream dependency of inpatient units.

V

VIRTUAL PRIVATE NETWORK (VPN)*: VPN is a technology that enables a user to establish a secure connection with a remote network. For example, a VPN connection allows a user at home to connect to the campus network, access files and applications, and work from home. An advantage of the VPN connection is that one's office computer need not be running. A disadvantage of the VPN connection is that files stored on the user's office computer (i.e., on the office computer's local hard drive) will not be accessible; and client-server applications will function only if the user has pre-installed the "client" software on her home computer. As a strategy to enable working-from-home (or from any remote location) during times of crisis, a VPN connection is considered superior to a Windows Remote Desktop connection.

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

W

WINDOWS REMOTE DESKTOP*: Windows Remote Desktop is a technology that enables Windows computer users to log into and operate their computer, via the internet, from a remote location. It is commonly used by employees to operate their office computers either from home sitting at their home computer or from any other location sitting at a laptop or desktop machine. A limitation of the windows remote desktop technology for disaster recovery is that the office computer must be powered and running.

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.