Glossary of Business Continuity Management Terms

Expert knowledge means success

Contents

Note: This publication has not been updated since it was last published. Some of the hyperlinks may have changed and may need updating. In addition, some of the information in this publication may be out of date.

Introduction

In this publication, we provide an explanation of terms used in Business Continuity Management (BCM)[1]. The glossary is intended to help you to understand the "jargon" which is used in BCM.

This glossary is limited to BCM but we publish several other glossaries as well – check our website or call us for details.

Business Continuity Management Terms Glossary

- Access Denial - See: Denial of Access.
- Activation - The implementation of business continuity procedures, activities and plans in response to a Business Continuity Emergency, Event, Incident and/or Crisis (E/I/C). See: Invocation.
- Alert - A formal notification that an E/I/C has occurred which may develop into a Business Continuity Management or Crisis Management invocation.
- Alternative Routing - The routing of information via an alternative cable routing medium (i.e. using different networks should the normal network be rendered unavailable).
- Alternate Site - A site held in readiness for use during a Business Continuity E/I/C to maintain the business continuity of an organisation's Mission Critical Activities. The term applies equally to office or technology requirements. Alternate sites may be 'cold', 'warm' or 'hot'. This type of site is also known as a Recovery Site. See: Cold Site, Warm Site, Hot Site, Recovery Site.
- Assembly Area - The designated area at which employees, visitors and contractors assemble if evacuated from their building/site.
- Asset - An item of property and/or component of a business activity/process owned by an organisation. There are 3 types of asset: physical assets (e.g. buildings and equipment); financial assets (e.g. currency, bank deposits and shares) and non-tangible assets (e.g. goodwill, reputation).
- Asset Risk - A category of risk management that looks at maximising investment related activities and managing such adverse factors as, the collapse of an investment market, currency mismatches and poor investment performance. This type of risk is also known as 'Investment Risk'.
- Assurance - The activity and process whereby an organisation can verify and validate its BCM capability.
- Audit - The process by which procedures and/or documentation are measured against pre-agreed standards.
- Backlog - The effect on the business of a build-up of work that occurs as the result of a system or process being unavailable for an unacceptable period. A situation whereby a backlog of work requires more time to action than is available through normal working patterns. In extreme circumstances, the backlog may become so marked that the backlog cannot be cleared.
- Backup - 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.
- Battle Box - A container - often literally a box or brief case - in which data and information e.g. BCP is stored so as to be immediately available to those responding to an E/I/C.
- Blue Light Services - Usually refers to the civil services of Police, Fire and Ambulance. See: Emergency Services, Statutory Services.
- Bronze Control - The agreed civil Emergency Services term for Operational Control. See: Operational Control, Level 3 Control.
- BS 7799 - A UK BSI Standard for information security management. Section 9 deals with Business Continuity Management. The corresponding international standard is known as ISO 17799.
- Building Denial – See: Denial of Access.
- Business Activity - A group of activities/processes undertaken by an organisation to produce a product and/or service and/or in pursuit of a common goal.
- Business Continuity Management (BCM) - A holistic management process that identifies potential impacts that threaten an organisation 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.

Business Continuity Management Activity - An action or series of actions that form a part of a BCM process.

- Business Continuity Management Co-ordinator - A role that is assigned the overall responsibility for co-ordinating the organisation(s)/business unit(s) BCM programme. See: Business Recovery Planner, Disaster Recovery Planner, Business Recovery Co-ordinator, Disaster Recovery Administrator.
- Business Continuity Management Life-Cycle - The complete set of activities and processes divided into various stages that are necessary to manage business continuity.
- Business Continuity Institute (BCI) - The Institute of professional Business Continuity Managers. Website www.thebci.org
- Business Continuity Management Maturity - The level and degree to which BCM activities have become standard and assured business practices within an organisation. See: Maturity.
- Business Continuity Management Plan - A clearly defined and documented plan for use at the time of a Business Continuity Emergency, Event, Incident and/or Crisis (E/I/C). Typically a plan will cover all the key personnel, resources, services and actions required to manage the BCM process. See: Business Continuity Plan (also known as BCP).
- Business Continuity Management Planning - The advance planning and preparations that are necessary to identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan(s) which ensure continuity of organisational services in the event of an E/I/C; and to deliver a comprehensive training, testing and maintenance programme. See: Contingency Planning, Disaster Recovery Planning, Business Recovery Planning.
- Business Continuity Management Policy - A BCM policy sets out an organisation's aims, principles and approach to BCM, what and how it will be delivered, key roles and responsibilities and how BCM will be governed and reported upon.
- 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 Programme - 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 Programme, Business Recovery Programme, Contingency Planning.
- Business Continuity Management Team - A defined number of roles and responsibilities for implementing the Business Continuity Management Plan. See: Business Recovery Team.
- Business Continuity Plan (BCP) - A clearly defined and documented plan. See: Business Continuity Management Plan.
- Business Continuity Management Process - A set of activities/processes with defined outcomes, deliverables and evaluation criteria that form a distinct part of the BCM lifecycle.
- Business Critical Functions - Critical operational or support activities. See: Mission Critical Activities.
- Business Critical Point - The latest moment at which the business can afford to be without a Mission Critical Activity or dependency.
- Business Function - A business unit within an organisation e.g. branch/division.
- Business Impact Analysis (BIA) - The management level analysis by which an organisation assesses the quantitative (financial) and qualitative (non-financial) impacts, effects and loss that might result if the organisation were to suffer a Business Continuity E/I/C. The findings from a BIA are used to make decisions concerning Business Continuity Management strategy and solutions.
- Business Impact Resource Recovery Analysis (BIRRA) - An assessment of the minimum level of resources e.g. personnel, workstations, technology, telephony required, overtime, after a Business Continuity E/I/C to maintain the continuity of the organisation's Mission Critical Activities at a minimum level of service/production. Generally considered to be part of a BIA it is an integral part of any subsequent resource Gap Analysis. See: Business Impact Analysis

- Business Recovery - See: Business Continuity Management (BCM).
- Business Recovery Co-ordinator - See: BCM Co-ordinator, Business Recovery Planner, Disaster Recovery Planner, Disaster Recovery Administrator.
- Business Recovery Plan - See: BCM Plan, Business Continuity Plan (BCP), Disaster Recovery Plan.
- Business Recovery Planner - See: BCM Co-ordinator, Business Recovery Co-ordinator, Disaster Recovery Planner, Disaster Recovery Administrator.
- Business Recovery Planning - See: BCM Planning, Contingency Planning, Disaster Recovery Planning.
- Business Recovery Programme - See: BCM Programme, Disaster Recovery Programme, Disaster Recovery Planning, Contingency Planning.
- Business Recovery Team - See: BCM Team.
- Business Risk - The risk that external factors, such as a fall in demand for an organisations products or services, will result in unexpected loss. Business risk, if managed well, can also result in a competitive advantage being gained.
- Call Tree - A structured cascade process (system) that enables a list of persons, roles and/or organisations to be contacted as a part of an information or plan invocation procedure. See: Contact List, Cascade System, Reverse Cascade System.
- Campus - A set of buildings which are geographically grouped together.
- Call Tree Cascade Test - A test designed to validate the currency of contact lists and the processes by which they are maintained.
- Cascade System - A system whereby one person or organisation calls out/contacts others who in turn initiate further call-outs/contacts as necessary. See: Contact List, Call Tree and Reverse Cascade System.
- Casualty Bureau - The central police controlled contact and information point for all records and data relating to casualties and fatalities.
- Cold site - A site (data centre/ work area) equipped with appropriate environmental conditioning, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by key employees required to resume business operations. See: Alternate Site.
- Command, Control and Coordination - A Crisis Management process: Command means the authority for an organisation or part of an organisation to direct the actions of its own resources (both personnel and equipment). Control means the authority to direct strategic, tactical and operational operations in order to complete an assigned function and includes the ability to direct the activities of others engaged in the completion of that function i.e. the crisis as a whole or a function within the crisis management process. The control of an assigned function also carries with it the responsibility for the health and safety of those involved Co-ordination means the harmonious integration of the expertise of all the agencies/roles involved with the objective of effectively and efficiently bringing the crisis to a successful conclusion. See: Level 1 Control: Strategic Control: Gold Control: Tactical Control: Level 2 Control: Silver Control: Level 3 Control: Operational Control: Bronze Control.
- Command Centre (CC) - The facility used by a Crisis Management Team after the first phase of a Business Continuity E/I/C. An organisation must have a primary and secondary location for a command centre in the event of one being unavailable. It may also serve as a reporting point for deliveries, services, press and all external contacts. See Emergency Control Centre (EEC): Emergency Operations Centre (EOC): Command and Control.
- Consequence - The end result following a Business Continuity E/I/C that can be defined as loss, injury, disadvantage or gain.
- Contact List - See: Call Tree and Cascade System, Reverse Cascade System.
- Contingency Fund - A budget for meeting and managing operating expense at the time of a Business Continuity E/I/C. See: also Expense Control.
- Contingency Planning - See: BCM Planning, Business Continuity Management Programme, Business Recovery Programme, Disaster Recovery Planning.
- Control - Any action which reduces the probability of a risk occurring or reduces its impact if it does occur. See: Command, Control & Co-ordination.
- Control Room Exercise - A methodology for exercising key people, communications, procedures and information flows between individuals and/or teams and different control rooms.
- Control & Risk Self Assessment (CRSA) - See: Control Self Assessment (CSA).

- Control Culture - Sets the tone for an organisation, influencing the control consciousness of its people. Control culture factors include the integrity, ethical values and competence of the entity's people: management's philosophy and operating style; the way management assigns authority and responsibility, and organises and develops its people; and the attention and direction provided by a Board.
- Control Environment - The whole system of controls, financial and otherwise, established by a Board and management in order to carry on an organisation's business in an effective and efficient manner, in line with the organisation's established objectives and goals. Also there to ensure compliance with laws and regulations, to safeguard an organisation's assets and to ensure the reliability of management and financial information. Also referred to as Internal Control. See: Internal Control.
- Control Framework - A model or recognised system of control categories that covers all internal controls expected within an organisation. See: Risk Framework.
- Control Review/Monitoring - Involves selecting a control and establishing whether it has been working effectively and as described and expected during the period under review.
- Control Self Assessment (CSA) - A class of techniques used in an audit or in place of an audit to assess risk and control strength and weaknesses against a control framework. The 'self' assessment refers to the involvement of management and staff in the assessment process, often facilitated by internal auditors. CSA techniques can include workshop/seminars, focus groups, structured interviews and survey questionnaires. See: Control and Risk Self Assessment.
- Cordon (Inner and Outer) - The boundary line of a zone that is determined, reinforced by legislative power, and exclusively controlled by the emergency services from which all unauthorised persons are excluded for a period of time determined by the emergency services. See: Exclusion Zone(s) (EZ).
- Corporate Governance - The system/process by which the directors and officers of an organisation are required to carry out and discharge their legal, moral and regulatory accountabilities and responsibilities.
- Corporate Risk - A category of risk management that looks at ensuring an organisation meets its corporate governance responsibilities, takes appropriate actions and identifies and manages emerging risks.
- 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.
- Counselling - See: Trauma Counselling, Post Traumatic Stress Disorder, Trauma Management.
- Crisis - An occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an organisation.
- Crisis Management - The process by which an organisation manages the wider impact of a Business Continuity E/I/C until it is either under control or contained without impact to the organisation or the BCP is invoked as a part of the Crisis Management process.
- Crisis Management Team(s) (CMT) - A defined number of roles and responsibilities for implementing the organisation's Crisis Management Plan. See: Strategic, Gold. Tactical, Silver, Operational, Bronze.
- Crisis Management Plan - A clearly defined and documented plan of action for use at the time of a crisis. Typically a plan will cover all the key personnel, resources, services and actions required to implement and manage the Crisis Management process.
- Crisis Plan - See: Crisis Management Plan
- Critical - Usually applied to a resource or process that must be kept going (as soon as possible) at time of a Business Continuity E/I/C.
- Critical Data Point - The point to which data must be restored in order to achieve recovery objectives.
- Critical Service - See: Mission Critical Activities
- Damage Assessment - The process of assessing the financial/non-financial damage following a Business Continuity E/I/C. It usually refers to the assessment of damage to physical assets e.g. vital records, buildings, sites, technology to determine what can be salvaged or restored and what must be replaced.
- Database Shadowing - See: Emergency Data Services
- Data Mirroring - A process whereby critical data is copied instantaneously to another location so that it is not lost in the event of a Business Continuity E/I/C. See: Emergency Data Services.

- Data Protection - Statutory requirements to manage personal data in a manner that does not threaten or disadvantage the person to whom it refers.
- Decision Point - The latest moment at which the decision to invoke emergency procedures has to be taken in order to ensure the continued viability of the organisation.
- Denial of Access - The inability of a organisation to access and/or occupy its normal working environment. Usually imposed and controlled by the Emergency and/or Statutory Services. See: Site Access Denial.
- Dependency - The reliance, directly or indirectly, of one activity or process upon another. See: Mission Critical Activity Dependency.
- Desktop Exercise - See: Table Top Exercise.
- Disaster Recovery - See: Information Technology Disaster Recovery (ITDR).
- Disaster Recovery Administrator - See: BCM Co-ordinator. Also known as Business Recovery Planner, Disaster Recovery Planner, Disaster Recovery Co-ordinator.
- Disaster Recovery Co-ordinator - See: BCM Co-ordinator. Also known as Business Recovery Planner, Disaster Recovery Planner, Disaster Recovery Administrator.
- Disaster Recovery Plan - See: BCM Plan, Recovery Plan.
- Disaster Recovery Planning - See: BCM Planning.
- Disaster Recovery Programme - See: BCM Programme
- Diverse Routing - The routing of information through split or duplicate cable facilities.
- E/I/C - The acronym for Emergency(ies), Event(s), Incident(s) or Crisis(es).
- Electronic Vaulting - The transfer of data to an offsite storage facility using a communications link. See: Emergency Data Services.
- Emergency - An actual or impending situation that may cause injury, loss of life, destruction of property or cause the interference, loss or disruption of an organisation's normal business operations to such an extent that it poses a threat.
- Emergency Co-ordinator - The person assigned the role of co-ordinating the activities of the evacuation of a site and/or building with the statutory and/or emergency services.
- Emergency Control Centre (ECC) - The Command Centre used by the Crisis Management Team during the first phase of an E/I/C. An organisation should have both primary and secondary locations for an ECC in case one of them unavailable/inaccessible. It may also serve as a reporting point for deliveries, services, press and all external contacts. See: Command Centre (CC), Emergency Operations Centre (EOC), Command, Control and Co-ordination.
- Emergency Data Services - Remote capture and storage of electronic data, such as journalling, electronic vaulting and database shadowing/mirroring.
- Emergency Marshal - A person responsible for ensuring that all employees, visitors and contractors evacuate a site/building and report to the Emergency Coordinator when their designated floor/area is clear. See: Fire Marshal.
- Emergency Operations Centre (EOC) - See: Command Centre (CC), Emergency Command Centre (EEC), Command, Control and Co-ordination.
- Emergency Response Procedures - The initial response to any E/I/C and is focused upon protecting human life and the organisation's assets.
- Emergency Services - Usually refers to the civil services of Police, Fire and Ambulance. See: Blue Light Services, Statutory Services.
- Enterprise - See: Organisation.
- Escalation - The process by which an E/I/C is communicated upwards through an organisation's Business Continuity and/or risk E/I/C 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 E/I/C. See: Assembly Area.
- Event - Any occurrence that may lead to a business continuity incident. See: Incident
- Exclusion Zone(s) (EZ) - See: Cordon (Inner and Outer)
- Exercise - An announced or unannounced execution of business continuity plans intended to implement existing plans and/or highlight the need for additional plan development. A way of testing part of a Business Continuity Plan. An exercise may involve invoking Business Continuity procedures but is more likely to involve the simulation of

a Business Continuity E/I/C in which participants role-play in order to assess what issues may arise, prior to a real invocation. 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 Directors - A role in both tabletop and command centre 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 organisation or the exercise players (individually or team) or to learn lessons or training or awareness. Their role in subsequent debriefing is crucial.
- Exercise Umpire - 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 role differs from the Exercise Directors in that it does not have any responsibility for the mechanics of the exercise. Their role in subsequent debriefing is crucial.
- Expected Loss - The average financial loss or impact that can be anticipated for a particular loss event or risk. It is calculated based on experience and past information. It is normally given as the average loss amount over a specified period of time e.g. the expected amount loss per year.
- Expense Control - The essential logging and control of all expenditure at time of an E/I/C in a separate and distinct manner from the 'normal' procedure. The loss assessment and adjustment process will require this information to be readily available, once the BCM/Crisis Management process is complete. See: Contingency Funding.
- Exposure - The susceptibility to loss, or the vulnerability to a particular risk.
- Extreme or Catastrophic Emergency, Event, Incident and/or Crisis - A Business Continuity E/I/C of immense proportions that has severe consequences, often damaging a large proportion of the organisation's assets that results in a loss greater than an expected loss.
- Facilities Management (FM) - The function that manages all aspects of an organisation's real estate assets and infrastructure.
- Fallback - Another term for alternative e.g. a fallback facility is another site/building that can be use when the original site/building is unusable or unavailable.
- Financial Services Authority (FSA) - The UK Government Body that supervises and regulates the Financial Services Sector under the Financial Services & Markets Act 2000 (FSMA). The FSA's objectives are: 1) maintaining confidence in the UK financial system 2) Promoting public understanding of the financial system 3) Securing the appropriate degree of protection for consumers 4) Reducing financial crime.
- Fire Marshal - See: Emergency Marshal.
- Friends and Relatives Reception Centre - A secure area set aside by the Emergency Services or Local Authority for use and the interview of friends and relatives arriving at the scene of a major incident.
- Full Rehearsal - A simulation exercise involving a Business Continuity E/I/C where the organisation or some of its component parts are suspended until the exercise is completed. See: Exercise, Desktop Exercise
- Gap Analysis - A survey whose aim is to identify the differences between BCM/Crisis Management requirements (what the business says it needs at time of an E/I/C) and what is in place and/or available.
- Gold Control - The agreed civil Emergency Services term for Strategic Control. See: Strategic Control and Level 1 Control.
- Goodwill - Value attributed to an organisation over and above the value of its physical assets as a result of its reputation in the market place.
- Governance - See: Corporate Governance.
- Hazard - A source of potential harm or a situation with a potential to cause loss.
- Health & 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 cognisant of H&S statutory and regulatory requirements and legislation.

- Hot Site - A site (data centre, work area) that provides a BCM facility with the relevant work area recovery, telecommunications and IT interfaces and environmentally controlled space capable of providing relatively immediate backup data processing support to maintain the organisation's Mission Critical Activities. See: Warm Site, Cold Site, Alternate Site.
- Hot Standby - A term that is normally reserved for Technology Recovery. An alternate means of processing that minimises downtime so that no loss of processing occurs. Usually involves the use of a standby system or site that is permanently connected to business users and is often used to record transactions in tandem with the primary system.
- Housekeeping - The process of maintaining procedures, systems, people and plans in a state of readiness.
- Human Resources - Human Resources (HR) (also known as Personnel Department). See Personnel Department.
- Human Resource Disaster Recovery (HRDR) - A specific strategy for dealing with risk assessment, prevention, control and business recovery for both critical (key) and non-critical (non-key) personnel. See: Trauma Counselling, Post Traumatic Stress Disorder and Trauma Management.
- Impact - The potential level of impact and effect of a Business Continuity E/I/C over time on an organisation. The level of impact and effect is usually relative to the size of the organisation and its BCM resilience. The types of business impact are usually described as financial and non-financial and are further divided into specific types of impact. See: Business Impact Analysis
- Incident - Any event that may be, or may lead to, a business interruption, disruption, loss and/or crisis.
- Incident Management - The process by which an organisation responds to and controls an incident using Emergency Response Procedures. See: Emergency Response Procedures.
- Information Security - The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organisation. See: BSI 7799.
- Infrastructure - A building and all of its supporting services. Infrastructure is usually divided into technology infrastructure (e.g. computers, cabling, telephony, etc.) and real estate infrastructure (e.g. buildings, utility supplies, air conditioning, etc.).
- Inherent Risk - The possibility that some human activity or natural event will have an adverse affect on the asset(s) of an organisation and which cannot be managed or transferred away.
- Insurance - A contract to finance the cost of risk. Should a named risk event (loss) occur, the insurance contract will pay the holder the contractual amount. See: Risk Financing and Self-Insurance
- Integrated Risk Management - Where current risks are managed in an integrated way across the whole breath of the organisation.
- Internal Audit - An organisation's own in-house team of auditors. Responsible primarily for evaluating the effectiveness of internal control systems and contributing to their ongoing effectiveness by providing advice and support to management.
- Internal Control - All the means, tangible and intangible that can be employed or used to ensure that established objectives are met. See: Control Culture.
- Invocation - The act by which a Business Continuity Management or Crisis Management process is formally started. The term is often used to refer to the act of using a service such as work area recovery as offered by a commercial or third-party provider. See: Activation.
- Information Technology Disaster Recovery (ITDR) - An integral part of the organisation's BCM plan by which it intends to recover and restore its IT and telecommunications capabilities after an E/I/C. See: BCM, BCM Plan, BCM Programme, Disaster Recovery.
- IT Recovery Planning - See: Technology Recovery Planning.
- Journalling - See: Emergency Data Services
- Key Task(s) - Tasks identified within a Business Continuity Plan as a priority action typically to be carried out within the first few minutes/hours of the plan invocation.
- Lead Time - The time it takes for a supplier – either equipment or a service – to make that equipment or service available. Business continuity plans should try to minimise this by agreeing Service Levels (Service Level Agreement) with the supplier in advance of a Business Continuity E/I/C rather than relying on the supplier's best efforts. See: Service Level Agreement.
- Legislative - Actions within a Business Continuity Plan that must be prioritised as a result of legal, statutory or regulatory requirements. See: Statutory, Regulatory.

- Level of Business Continuity (LBC) - The minimum level of business continuity of services and/or products that is acceptable to the organisation or industry to achieve its business objectives that may be influenced or dictated by regulation or legislation.
- Level 1 Control - See: Strategic Control, Gold Control.
- Level 2 Control - See: Tactical Control, Silver Control.
- Level 3 Control - See: Operational Control, Bronze Control.
- Likelihood - See: Probability.
- Line Re-routing - A facility offered by telephone service providers to re-route dedicated telephone lines to backup or other sites.
- Local Authority Emergency Planning Officer (EPO) - The civil authority role for civil emergency planning. The role interfaces with industry especially where legislation requires.
- Logistics/Transportation Team - A team comprised of various members of departments associated with supply acquisition and material transportation, responsible for ensuring the most effective acquisition and mobilisation of hardware, supplies and support materials.
- Loss - A negative consequence, which may be financial e.g. loss of cash, or nonfinancial e.g. loss of information or loss of goodwill.
- Loss Adjuster - Invaluable at the time of a Business Continuity E/I/C to assist in managing the financial implications of the E/I/C and should be involved as part of the management team where possible. Loss Adjusters often have useful contacts within the local community that can ease the burden at time of an E/I/C. Involving the Loss adjuster with the CMT will improve the speed and effectiveness of any ensuing insurance claim.
- Maturity - See: Business Continuity Management Maturity
- Major Incident - An Emergency Services definition. Any emergency that requires the implementation of special arrangements by one or more of the Emergency Services, National Health Service or a Local Authority.
- Manual Procedures - An alternative method of working following a loss of IT systems. As working practices rely more and more on computerised activities, the ability of an organisation to fallback to manual alternatives lessens. However, temporary measures and methods of working can help mitigate the impact of a Business Continuity E/I/C and give staff a feeling of doing something.
- Marshal - See: Emergency Marshal.
- Marshalling Area A safe area where resources and personnel not immediately required can be directed to standby to await further instruction.
- Maximum Acceptable Outage (MAO) - This is the timeframe during which a recovery must become effective before an outage compromises the ability of an organisation to achieve its business objectives and or survival. See: Outage, MTD, MTA.
- Maximum Tolerable Downtime (MTD) - See: Recovery Time Objective, Maximum Acceptable Outage
- Maximum Time in Alternative Operations (MTA) - See: Maximum Acceptable Outage (MAO).
- Media - News reporting function including TV, radio, internet, e-mail and newspapers.
- Mirroring - See: Data Mirroring.
- Mission Critical Activities - The critical operational and/or business support activities (either provided internally or outsourced) without which the organisation would quickly be unable to achieve its business objective(s) i.e. services and/or products. See Critical Service.
- Mission Critical Activity Dependency(ies) - The critical operational or support activities (either provided internally or outsourced) upon which a Mission Critical Activity is dependent to enable it to fully complete the Mission Critical Activity. See: Dependencies.
- Mobile Standby - A transportable operating environment - often a large trailer – complete with office facilities and computer equipment that can be delivered and set up at a suitable site at short notice.
- Mobilisation - The activation of the recovery organisation in response to BCM invocation.
- Offsite Location - A site at a safe distance from the primary site where critical data (computerised or paper) and/ or equipment is stored from where it can be recovered and used at the time of a Business Continuity E/I/C if original data, material or equipment is lost or unavailable.
- Operational Control - The role of the operational control is to implement the tactical control action plan by allocating specific tasks within the determined areas of responsibility and command of allocated resources. See: Strategic, Tactical and Operational Control, Gold Silver and Bronze Control and Level 1,2 and 3 Control.
- Operational Risk - The risk that deficiencies in information systems or

internal controls will result in unexpected loss. The risk is associated with human error, system failures and inadequate procedures and controls.

- Organisation - An enterprise, a corporate entity; a firm, an establishment, a public or government body, department or agency; a business or a charity.
- Organisation (large scale or super) - An organisation that is large and complex, in the sense that it could absorb the impact of losing a complete location or business unit. The normal terminology, and perspective, needs to be scaled down by regarding individual locations or business units as self-sustaining entities.
- Organisation Risk Management - Where both current and emerging risks are managed in an integrated way across the whole organisation.
- Outage - Period of time that a service, system, process or business function is expected to be unusable or inaccessible which has a high impact on the organisation, compromising the achievement of the organisation's business objectives. An outage is different to 'downtime' where process or system failures happen as a part of normal operations, and where the impact merely reduces the short-term effectiveness of processes. See: Maximum Acceptable Outage.
- Outsourcing - The transfer of business functions to an independent (internal and/or external) third party supplier.
- Period of Tolerance - The period of time in which a Business Continuity E/I/C can escalate to a potential disaster without undue impact to the organisation.
- Plan Currency - Business Continuity Plans must be maintained (housekeeping) to an adequate state. The measure of how up-to-date BC and CMT plans are kept. A good (recent) plan currency is vital if plans are to be reliable.
- Plan Maintenance - The management process of keeping an organisation's BCM competence and capability up-to-date, fit-for-purpose and effective.
- Post Traumatic Stress Disorder (PTSD) - PTSD is caused by a major traumatic E/I/C where a person experienced, witnessed or was confronted with an E/I/C that involved actual or threatened death or serious injury or threat to the physical integrity of self or others, and the person's response involved intense fear, helplessness or horror. See: Trauma Counselling and Trauma Management.
- Pre-positional Resource Material - (i.e. equipment, forms and supplies) stored at an offsite location to be used in business recovery operations.
- Press Conference - The provision of an organisation spokesperson(s) at a specific venue and time(s) to brief and answer any questions or enquiries from the media.
- Press Briefings - See: Press Conference.
- Press Statements - Prepared statements issued to the press during and/or after a Business Continuity E/I/C. See: Press Briefings.
- Preventative - Measures put in place to lessen the likelihood of a Business Continuity E/I/C.
- Prioritisation - The order in which Mission Critical Activities and their dependencies are addressed following invocation of the BCM process.
- Probability - The chance of a risk occurring.
- Project Management - The techniques and tools used to describe, control and deliver a series of activities with given deliverables, timeframes and budgets.
- Qualitative Assessment - A form of assessment that analyses the general structures and systems currently in place. A descriptive methodology, which typically involves risk mapping and risk matrices. These assessments do not involve detailed measurements.
- Quantitative Assessment - A form of assessment that analyses the actual numbers and values involved. This type of methodology typically applies mathematical and statistical techniques and modeling.
- Quantification - The objective measure of the seriousness of risk or impact, often measured in financial or regulatory terms.
- Reception Centre - A secure area to which the uninjured can be taken for shelter, first aid, interview and documentation as appropriate to the E/I/C. See: Friends and Relatives Reception Centre.
- Reciprocal Agreement - An arrangement by which one organisation agrees to use another's resources in the event of a Business Continuity E/I/C.
- Recoverable Loss - Financial losses due to a loss E/I/C that may be reclaimed in the future, e.g. through insurance or litigation.
- Recovery - See: System Recovery.

- Recovery Management Team - A team of people that are responsible for recovering an aspect of the organisation, or obtaining the resources required for the recovery. See: BCM Team.
- Recovery Plan - See: BCM Plan.
- Recovery Point Objective (RPO) - The point in time to which work should be restored following a Business Continuity E/I/C that interrupts/disrupts the business e.g. 'start of day'.
- Recovery Site - See: Alternate Site.
- Recovery Strategy - See: BCM strategy.
- Recovery Team - See: BCM Team.
- Recovery Time Objective (RTO) - An essential output from the BIA that identifies the time by which Mission Critical Activities and/or their dependencies must be recovered. See: BIA, Dependencies, Mission Critical Activities.
- Recovery Timeline - The critical path of actions and activities that describe the speed and prioritisation of the recovery process.
- Recovery Window - See: Recovery Time Objective.
- Redundancy - In human resource terms, redundancy can be used to mean the provision of delegates or alternates for key employees or BCM/Crisis Management Team members. See: Backup, Alternate Site.
- Regulatory - See: Legislative, Statutory.
- Rendezvous Point (RVP) - A secure and safe location (point) to which all Emergency Services resources arriving at an emergency/statutory services outer cordon are directed for logging, briefing, equipment issue and deployment. See: Emergency Services.
- Residual Risk - The level of uncontrolled risk remaining after all cost-effective actions have been taken to lessen the impact and probability of a specific risk or group of risks, subject to the organisations risk appetite. See: Inherent Risk, Risk Appetite.
- Resilience - The ability of an organisation, staff, system, network, activity or process to absorb the impact of a business interruption, disruption and/or loss and continue to provide a minimum acceptable level of service. See: Level of Business Continuity (LBC), Component Failure.
- Response - The reaction to a Business Continuity E/I/C in order to assess the level of containment and control activity required.
- Rest Centre - A building taken over by the Local Authority for the temporary accommodation of evacuees.
- Restart - The procedure or procedures that return applications and data to a known start point. Application restart is dependent upon having an operable system. See: Start Point.
- Resumption - The implementation of steps to enable the recovery and continuity of an organisation's Mission Critical Activities and/or their dependencies immediately following a Business Continuity E/I/C.
- Reverse Cascade System - A reversal of the cascade system that enables the whereabouts and safety of personnel to be established. See: Cascade System, Call Tree, Contact List.
- Risk - The chance of something happening, measured in terms of probability and consequences. The consequence may be either positive or negative. Risk in a general sense can be defined as the threat of an action or inaction that will prevent an organisation's ability to achieve its business objectives. The results of a risk occurring are defined by the impact. See: Impact.
- Risk Analysis - The systematic process of identifying the nature and causes of risks to which an organisation could be exposed and assessing the likely impact and probability of those risks occurring.
- Risk Appetite - The willingness of an organisation to accept a defined level of risk in order to conduct its business cost-effectively. Different organisations at different stages of their existence will have different risk appetites. See: Risk Context.
- Risk Assessment - The overall process of risk identification, analysis and evaluation.
- Risk Avoidance - An informed decision not to become involved in a risk situation.
- Risk Based Auditing - Audits that focus on risk and risk management as the audit objective.
- 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, people, technology and knowledge.
- Risk Classification - The categorisation of risk, normally focusing on likely impact to the organisation or likelihood of occurrence.

- Risk Concentration - The risks associated with having Mission Critical Activities and/or their dependencies, systemic processes and people located either in the same building or close geographical proximity (zone), that are not reproduced elsewhere i.e. a single point of failure and lack of organisational resilience.
- Risk Context - The environment in which risks exist. This can be broken down into the strategic context such as the relationship between the organisation and the external business environment, and the organisational context such as goals, objectives, capabilities, resources, culture and strategies. See: Risk Appetite.
- Risk Control - That part of risk management which involves the implementation of policies, standards, procedures and physical changes to eliminate or minimise adverse risks. See: Risk Management.
- Risk Evaluation -The process of comparing actual risk levels with previously established risk criteria. As a result of this comparison, risks can be prioritised for further action.
- Risk Event - An event that could potentially lead to an adverse impact on the business or function. The manifestation of a risk into a reality.
- Risk Factors - Measurable or observable manifestations or characteristics of a process that either indicates the presence of risk or tend to increase exposure.
- Risk Financing - The application of techniques to fund the treatment and consequences of risk e.g. using insurance. A means of accounting for potential loss exposures. Examples include various types of risk retention (e.g. internal contingency funds or reserves funding losses out of operating budgets, etc.) and risk transfer techniques including insurance contracts, self-insurance, captives, sinking funds, etc.
- Risk Framework Measurable or observable manifestations or characteristics of a process that either indicates the presence of risk or tend to increase exposure. See: Control Framework.
- Risk Identification - The process of identifying what can happen, why and how.
- Risk Level - See: Risk Profile.
- Risk Management - The culture, processes and structures that are put in place to effectively manage potential opportunities and adverse effects. As it is not possible or desirable to eliminate all risk, the objective is to implement cost effective processes that reduce risks to an acceptable level, reject unacceptable risks and treat risk by financial interventions i.e. transfer other risks through insurance or other means, or by organisational intervention i.e. BCM. See: Risk Control.
- Risk Management Process - The systematic and documented process of clarifying the risk context and identifying, analysing, evaluating, treating, monitoring, communicating and consulting on risks.
- Risk Mitigation - Measure taken to reduce exposures to risks.
- Risk Perception People view risks differently; this is usually related to their attitude to risk and whether they lean more towards being a risk taker or being risk averse.
- Risk Prioritisation - The relation of acceptable levels of risks among alternatives. See: Risk Ranking.
- Risk Profile - The combined result of consequence and probability. See: Risk Level.
- Risk Profiling - The systematic method by which all the risks and associated controls relating to an entity are identified, assessed and documented using risk management tools.
- Risk Ranking - The ordinal or cardinal rank prioritisation of the risks in various alternatives, projects or units. See: Risk Prioritisation.
- Risk Reduction or Mitigation - A selective application of appropriate techniques and management principles to reduce or mitigate either likelihood of an occurrence or its consequences, or both.
- Risk Retention - Intentional (or unintentional) retaining the responsibility for loss or risk financing within the organisation.
- Risk Scenarios - A method of identifying and classifying risks through creative application of probabilistic events and their consequences. Typically a brainstorming or other creative technique used to stimulate "what might happen." This can be achieved through creative techniques, such as brainstorming, or through the application of mathematical and statistical techniques and modelling e.g. fault tree analysis and event tree analysis.
- Risk Standards - Various Risk Standards have been published around the world providing guidance for business on managing risk. For example: the Australian/New Zealand Standard on Risk Management (AS/NZS4360: 1999).
- Risk Systemic - See: Systemic Risk.

- Risk Transfer - A series of techniques describing the various means of addressing risk through insurance and similar products. This includes recent developments such as the securitisation of risk and creation of, for example, catastrophe bonds.
- Risk Treatment - The selection and implementation of relevant options for managing risk. The key treatments include:
  - Acceptance - risks are retained by the organisation
  - Avoidance - deciding not to carry on with the proposed activities due to the risk being unacceptable or finding another alternative that is more acceptable.
  - Reduction - reducing the likelihood and/or consequence of the risk
  - Transfer - transferring the risk in part or in totality to another. Insurance is an example of risk transfer.
- Roll Call - The process of ensuring that all employees, visitors and contractors have been safely evacuated and accounted for following an evacuation of a building or site.
- Salvage - The recovery of personal effects, documentation, office and computer equipment.
- Scenario - A pre-defined set of Business Continuity E/I/C and conditions that describe an interruption, disruption or loss related to some aspect(s) of an organisation's business for purposes of exercising a plan(s) and the people that would manage a Business Continuity E/I/C.
- Security Review - A periodic review of the security of tangible and intangible assets which should cover security policy, effectiveness of policy implementation, restriction of access to the assets, accountability for access and basic safety.
- Self-Insurance - The decision to bear the losses that could result from a Business Continuity E/I/C rather than take insurance to cover the risk.
- Service Level Agreement (SLA) - A formal agreement between a service provider (whether internal or external) and their client (whether internal or external) which covers the nature, quality, availability, scope and response of the service provider. The SLA should cover day-to-day situations and disaster situations, as the need for the service may vary in a disaster.
- Silver Control - The agreed civil Emergency Services term for Tactical Control. See: Tactical Control, Level 2 Control.
- Single Point of Failure - The only (single) source of a service, activity and/or process i.e. there is no alternative, whose failure would lead to the total failure of a Mission Critical Activity and/or dependency.
- Site Access Denial - See: Denial of Access.
- Social Impact - The affect and effect of a Business Continuity E/I/C on the overall wellbeing of a population/community.
- Sourcing - See: Supplier, Third Party Supplier, Outsourcing.
- Speculative Risk - A risk where there is uncertainty as to whether a gain or loss will occur. An example would be exposure to movements in exchange rates.
- Stand Down - Formal notification that the response to a Business Continuity E/I/C has been concluded.
- Standby Service - The provision of the relevant recovery facilities. See: Cold Site, Warm Site, Hot Site, Work Area and Mobile Standby.
- Statutory - See: Legislative, Regulatory.
- Statutory Services - Those services whose responsibilities are laid down by law e.g. Fire and Rescue Service, Coast Guard Service. See: Emergency Services, Blue Light Services.
- Strategic Control - The purpose of the strategic level of control is to establish a framework of policy within which tactical control will work and a strategy that tactical control will implement. In particular the provision of resources for tactical command, the resolution and prioritisation of multiple and/or conflict demands and to determine plans for the return to business as usual or return home.
- Structured Walk-through - A type of exercise in which team members physically implement and verbally review each step of a plan to assess its effectiveness, identify enhancements, constraints and deficiencies. See: Testing.
- Supplier - A person or company who supplies goods or services to the organisation. See; Sourcing
- Syndication Ratio - The number of times that a work area is sold by the third party providers at a resource recovery location and its availability at the time of a Business Continuity E/I/C is on a first-come-first-served basis.
- System Denial - A failure of the IT system for a protracted period, which may impact an organisation's ability to sustain its normal business activities.

- System Recovery - The procedures for rebuilding a computer system to the condition where it is ready to accept data and applications.
- System Restore - The procedures necessary to get a system into an operable condition where it is possible to run the application software against the available data. System restore depends upon having a live system available i.e. follows system recovery
- Systemic Risk - The risk that the failure of one participant or part of a process, system, industry or market to meet its obligations will cause other participants to be unable to meet their obligations when due causing significant liquidity and other problems thereby threatening the stability of the whole process, system, industry or market.
- Tabletop Exercise - A paper feed scenario based method of testing plans, procedures and people. See: Desktop Exercise.
- Tactical Control- A primary role of a tactical level of control is to provide and co-ordinate an action plan to deal with the Business Continuity E/I/C and/or implement the policy and strategy of the strategic level of control (where the latter exists). Also, to determine the priority in the allocation of resources in the co-ordination of the implementation of the plan. See: Level 2 Control, Silver Control.
- Task List - Defined mandatory and discretionary tasks allocated to teams and/or individual roles within a plan.
- Tape Backup - Key data being backed up onto tapes at a given point in time.
- Technology Recovery Planning - The process of planning for and writing procedures to address recovery of the IT and telecommunications components for the Mission Critical Activities and/or their dependencies. See: Information Technology Disaster Recovery (ITDR).
- Telecommunications - The technology of communications by telephony, radio, television, etc.
- Test - An activity in which some part(s) of a business continuity plan(s) is followed to ensure that the plan contains the appropriate information and produces the desired result. A test is distinct from an exercise in that a test occurs at an alternate site whereas an exercise is generally a simulation. See: Exercise
- Test Plan - A schedule of work designed to plan for testing a business continuity plan, people, systems and processes.
- Test Script - A detailed description of the tasks that will be undertaken whilst conducting a test. The test script details the scope of the test and defines the success criteria.
- Third-Party Provider/Supplier - An external provider of services, goods and solutions. See: Sourcing, Outsourcing, Supplier.
- Tolerance Threshold - The maximum period of time during which a business can afford to be without a Mission Critical Activity and/or its dependency(ies). See: Mission Critical Activities.
- Trauma Counselling - The provision of assistance to staff, customers and others who have suffered mental or physical injury through being involved in an E/I/C. See: Post Traumatic Stress Disorder & Trauma Management.
- Trauma Management - Trauma Management involves helping employees deal with trauma in a systematic way following a disaster through the delivery of appropriate support systems and coping strategies with the objective of restoring employees psychological wellbeing. See: Trauma Counselling, Post Traumatic Stress Disorder.
- Unexpected Loss - The worst case financial loss or impact that a business could incur due to a particular loss E/I/C 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.
- Uninterrupted Power Supply (UPS) - Equipment (usually a bank of batteries) that offers short-term protection against power surges and outages. Note that UPS usually only allows enough time for vital systems to be correctly powered down.
- Utilities - Companies and organisations providing essential services e.g. gas, water, electricity.
- Virus - An unauthorised programme that inserts itself into a computer system and then propagates itself to other computers via networks or disks. When activated, it interferes with the operation of the computer systems.
- Vital Record - Computerised or paper record which is considered to be essential to the continuation of the business following an E/I/C.
- Vital Record Location - A designated storage location for holding Vital Records. Must be away from the normal site and be secure. See: Offsite Location, Records.
- Voice Recovery - Restoration of voice telephony services to another site.

- Warm Site - A site (data centre/work area) which is partially equipped with hardware, communications interfaces, electricity and environmental conditioning capable of providing backup operating support. See: Cold Site, Hot Site, Warm Site, Alternate Site.
- Work Area Facility - A pre-designated space provided with desks, telephones, PCs, etc. ready for occupation by business recovery teams at short notice. May be internally or externally provided. See Cold Site, Hot Site, Warm Site, Alternate Site.
- Work Area Recovery Planning - The business continuity planning process of preparing procedures for use at the work area facility.
- Zone - A region or area characterised by a common feature or quality that should be considered in BCM planning e.g. a high risk concentration of business and/or industry Mission Critical Activities in an area. See. Mission Critical Activities.

Acknowledgement

[1] This glossary has been provided by The Business Continuity Institute at www.bci.org and their copyright therein is acknowledged.

Further Information

This guide is for general interest - it is always essential to take advice on specific issues. We believe that the facts are correct as at the date of publication, but there may be certain errors and omissions for which we cannot be responsible.

Publication issued or updated on:
31 March 2009

Ref: 248