Strong Language:

The MHA Glossary of Essential Business Continuity Terminology

MHA Consulting

Introduction

In everyday use, the phrase "strong language" refers to the kinds of words you do not use in polite company. There's another possible definition: words that make you stronger when you know what they mean and how to use them.

Please be advised that this glossary is filled with strong language.

It includes nearly 200 terms that form the core vocabulary of business continuity management (BCM), IT disaster recovery, and crisis management. Knowing what these words mean—and being able to use them accurately and confidently—will make you stronger as a business continuity professional. It will make you more effective in your written and spoken communications with everyone you interact with on business continuity topics and help you understand articles you read, presentations you attend, and consultants you speak with. Most important, it will help you sharpen your own thinking about the business continuity challenges facing your organization.

At MHA, our experience is that most organizational staff with business continuity responsibilities—at all levels, from entry-level to executives—lack a solid understanding of BCM terminology. This lack of understanding creates confusion all the way down the line, adding expense, creating gaps, and lowering resilience.

Of all the steps an organization can take to strengthen its business continuity program, ensuring that the people with a role in BCM have a clear, common understanding of the field's essential terms might just have the best cost-benefit ratio. Now more than ever, no organization should tolerate a reduction in its resilience due to ignorance or confusion about the key terms of business continuity, especially when eliminating the problem is relatively easy.

Our motivation for creating this glossary was partly self-interest. Having a guide to key BCM terms that we can give our clients will make our partnerships with them more efficient. However, anyone is welcome to download and share the guide (provided they indicate it was produced by MHA Consulting). We hope everyone who consults it benefits from it.

In addition to a couple of usage notes, the glossary is preceded by a section of Business Continuity Basics that lists such key information as the four main business continuity areas, the four types of disruption, and the four main risk mitigation strategies.

Knowing the words in this guide will improve your ability to diagnose, explain, and address business continuity–related challenges, thus improving your effectiveness as a professional and enhancing your organization's resilience.

We at MHA Consulting, as BCM consultants and practitioners, feel strongly that BCM terminology is strong language in the best sense of the word.

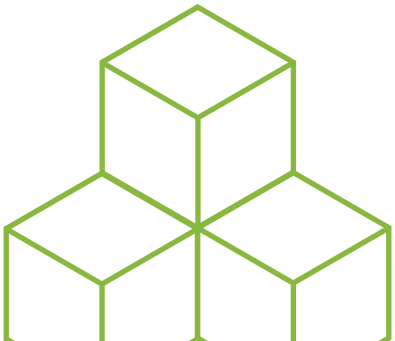
- Michael Herrera
CEO and founder, MHA Consulting

Glossary Notes

- Within the introduction and definitions, terms given in **bold** are defined in the glossary and hyperlinked to their definitions.
- For words in general usage, only the BCM definition is given.

Business Continuity Basics

- The **four main business continuity areas** are: program administration, business recovery, IT disaster recovery, and crisis management.
- The **three types of business continuity threat** are: human threats, natural threats, and technological threats.
- The **four crisis management priorities** are: life safety, incident stabilization, property preservation, and business restoration.
- The **four types of disruption** are: loss of facility or region, loss of human resources, loss of technology, and loss of supplier.
- The main **risk mitigation strategies** are: risk acceptance, risk avoidance, risk limitation, and risk transfer.
- BCM professionals use a variety of terms to denote adverse occurrences, including crisis, disaster, disruption, event, incident, and outage. Some of these overlap, and their preferred usage varies from one organization to the next.



Term	Definition
activation	The process of beginning the implementation of a recovery plan or crisis management plan.
activation checklist	Procedure employees should follow upon being notified the organization's continuity plans are being activated in response to an event.
alignment	Degree to which an organization's business continuity program meets the requirements of its chosen business continuity standard; degree to which IT capabilities match BCM expectations.
alternate command center	Backup physical location where an organization's crisis management team can gather to manage a crisis.
alternate provider	Vendor an organization can turn to as a backup provider of a critical product or service.
alternate work site	Pre-selected and -equipped physical location where employees can perform job functions if the primary work site becomes unavailable.
APIE	Widely used disaster-response process, pronounced "ay-pie." Stands for: Assess the situation, Plan your response, Implement your response, and Evaluate your performance.
audit	Assessment of an organization's BCM program by a regulatory body or other evaluator.
Backup as a Service (BaaS)	IT backup service provided by a third-party vendor.
BCM	See business continuity management.
BCM methodology	The foundational concepts and practices of business continuity management, e.g., business impact analyses, mitigation controls, recovery time objectives.
BCM practitioner	See BCM professional.

Term	Definition
BCM professional	Person professionally engaged in applying BCM methodology to promote organizational resilience and protect organizations and their stakeholders.
BCM standard	See business continuity standard.
best practices	Procedures widely recognized as being effective in promoting resilience and protecting organizations.
BIA	See business impact analysis.
BIA interview	Session in which BCM professionals ask questions of departmental representatives to gain information about the criticality of that department's business processes for the purpose of completing a business impact analysis.
BIA pre-work	Preliminary phase of a business impact analysis in which a business department provides the BCM office with information about its business processes in response to a questionnaire.
BIA questionnaire	Form submitted by BCM professionals to a business department as part of the BIA pre-work. Usually in online format.
BIA report	Document prepared at the conclusion of a business impact analysis summarizing its findings. Sets forth the relative criticality of the organization's business processes and computer systems and applications.
BIA software	Digital tool to facilitate the conducting of business impact analyses.
BIA validation	Process of verifying the data and conclusions in a business impact analysis by circulating it to knowledgeable parties for review.
brand protection	The activity of safeguarding the reputation of an organization.

Term	Definition
building loss	See loss of facility or region.
business continuity	An organization's ability to resume the performance of its business functions in a timely manner following an outage or crisis.
business continuity consultant	An independent advisor who provides organizations with business continuity expertise and services.
BCI Good Practice Guidelines	Business continuity standard issued by the UK-based Business Continuity Institute. Industry-agnostic standard similar to but somewhat deeper than ISO 22301.
business continuity life cycle	The ongoing process of assessing threats, prioritizing business processes, devising recovery strategies and plans, conducting training and mock disaster exercises, and identifying and closing gaps that is necessary to keep a business continuity program up-to-date and an organization resilient.
business continuity management (BCM)	Professional activity devoted to protecting organizations by using recognized methodologies to promote resilience and ensure that organizations that experience an outage or crisis can recover in such a manner as to minimize the impact on the organization and its stakeholders.
business continuity planning	Term formerly common as a synonym for business continuity management.
business continuity standard	Set of business continuity benchmarks issued by an industry body or government organization that are intended to provide the framework for a sound BC program. The leading BC standards are: BCI Good Practice Guidelines, FFIEC, ISO 22301, NIST 800, and NFPA 1600.
business continuity template	Publicly available form that can be filled in with an organization's unique data to create a resource for its BCM program.

Term	Definition
business impact analysis (BIA)	An assessment that determines the relative criticality of an organization's business processes. Provides critical guidance in developing recovery plans and allocating BC resources.
business process	Activity that enables an organization to carry out its mission and sustain its operations, e.g., manufacturing, customer service, accounting.
business recovery	The process of restoring business processes in a timely manner following an outage or event. One of the four main business continuity areas.
business restoration	The task of restoring the functioning of the business processes of an organization following an event. One of the four crisis management priorities.
checklist	Series of steps to complete, with a box by each step for adding a check mark when accomplished. The best format to use in writing business recovery plans and crisis management plans.
command center	A real, virtual, or hybrid space from which an event is managed.
compliance	Fulfillment of the requirements of a government regulation or business continuity standard.
contingency planning	Synonym for business continuity management, used primarily by non–BCM professionals.
continuity of operations planning (COOP)	Synonym for business continuity management, favored by the public sector.
corporate supply chain	See supply chain.
crisis	Severe adverse occurrence posing a significant threat to the organization's ability to carry out its essential operations.

Term	Definition
crisis communication scripts	Organizational statements about likely adverse events that are written and approved ahead of time for customization and release at the time of an event.
crisis communications plan	Plan detailing how an organization will communicate internally and externally in the event of a crisis.
crisis management (CM)	The process of trying to resolve a serious adverse event with minimal impact on an organization and its stakeholders. One of the four main business continuity areas.
crisis management core team	The primary members of an organization's crisis management team, made up of representatives of the departments that routinely play a role in CM.
crisis management extended team	The crisis management core team plus individuals from peripheral departments brought in on an as-needed basis.
crisis management plan	Document setting forth the steps the organization will take in responding to a crisis.
crisis management program	Collectively, the team, leadership, documentation, training, and exercises that are established to enable an organization to emerge from a severe adverse event with minimal impact to life safety, property, and the organization's business operations.
crisis management team (CMT)	The people formally assigned to the team that handles emergency situations.
critical business process	A business process whose interruption has the potential to seriously impact the organization and its stakeholders.
critical business unit	A business unit that is essential to the organization's ability to carry out its mission.
critical dependency	A resource that must be in place for a given process to function.

Term	Definition
critical supplier	A vendor that provides a product or service essential to the organization's ability to carry out its key operations.
critical vendor	See critical supplier.
culture of continuity	The adoption throughout an organization of concepts, considerations, and practices tending to promote recoverability and resilience.
current state assessment (CSA)	Analysis to determine the strengths and weaknesses of an organization's business continuity program.
cyber plan	Document outlining how an organization will respond to an occurrence that threatens to erase, encrypt, corrupt, or steal data from its information systems.
data backup	Safety copies of data files made to the cloud or to tape.
data center (DC)	Facility containing computers where critical data and applications are stored.
data protection	The process of ensuring that the critical information of an organization remains correct, uncorrupted, and secure from theft.
data protection policy	Organizational statement explaining the rules and procedures employees are expected to follow in order to protect the organization's data.
data validation	The activity of verifying information that has been gathered for use in a process.
declaration of recovery	Following an event, an internal statement made by pre-authorized personnel that the organization will undertake a specified type of recovery.
dependency	A resource that must be in place before a given process will work.

Term	Definition
disaster	A severe adverse occurrence negatively affecting the organization's ability to carry out its mission-critical operations. Often encountered in the context of a natural disaster or the task of IT disaster recovery.
disaster declaration	Formal statement by an organization that a negative event rising to the severity of a disaster has occurred.
disaster exercise scenario	Fictional emergency presented for participants to cope with as part of mock disaster training.
Disaster Recovery as a Service (DRaaS)	The use of third-party vendors to provide cloud-based backup and recovery of organizational servers and data.
disaster recovery plan	Document giving the procedures for recovering IT data and applications.
disruption	An interruption in an organization's ability to carry out its everyday processes and activities.
emergency operations center (EOC)	The real, virtual, or hybrid space where the crisis management team meets to manage a crisis.
enterprise risk management (ERM)	The activity of identifying and mitigating the hazards that threaten an organization.
event	An adverse occurrence that interferes with an organization's ability to carry out its activities.
exercise	See mock disaster exercise.
facilitator	Person who presents and conducts a mock disaster exercise.
failover	Shifting to the use of a backup computer resource following an outage of the primary resource.

Term	Definition
FFIEC	Business continuity standard published by the Federal Financial Institutions Examination Council, a government agency. Sometimes referred to as the FFIEC IT Examination Handbook. A highly stringent standard developed for use in the financial sector.
fourth-party vendors	Companies that supply goods and services to an organization's suppliers.
full-scale exercise	An extended, highly realistic mock disaster exercise.
fusion center	High-level center at an organization devoted to the collection and analysis of real-time information pertaining to the organization's security, technology, and operations. Coordinates the overall response to a situation of simultaneous emergencies. Modeled on the government fusion centers established after 9/11.
gap analysis	Assessment to identify weaknesses in an organization's BCM program.
governance	The oversight structure and policies establishing how a BCM program will be administered.
governance, risk, and compliance (GRC)	The activities of governing an organization, managing risk, and ensuring compliance with applicable regulations and standards approached as an integrated endeavor.
human threat	A threat posed to an organization by human actors, e.g., an active shooter. One of the three types of business continuity threat.
hybrid emergency operations center	A space for coordinating an organization's response to a crisis that incorporates both physical and remote components.
impact	The negative consequences of an event.

Term	Definition
impact categories	The different types of damage an event can cause an organization, e.g., loss of revenue; damage to brand, image, and reputation. Used in conducting business impact analyses to help organizations prioritize their business processes.
incident	Negative occurrence that impedes an organization's ability to carry out its normal activities.
Incident Command System (ICS)	Widely used method for organizing emergency response teams that includes a management hierarchy and procedures for managing incidents.
incident stabilization	The process of stopping the damage actively being caused by a disruption. One of the four crisis management priorities.
inherent risk	The danger that resides in an activity before the application of mitigation controls.
interdependencies	Relationships in which resources depend on each other in order to function.
ISO 22301	Business continuity standard issued by the International Organization for Standardization, the global organization made up of national standards bodies. A brief, high-level standard that some users find too vague for their needs. Was recently supplemented by a new risk management standard, ISO 22332.
IT process	A function executed at the level of computer technology.
IT stack	Set of information technologies an organization depends on to carry out its operations.
IT disaster recovery (IT/DR)	The aspect of business continuity dealing with the protection and recovery of IT data and applications. One of the four main business continuity areas.
IT/DR recovery plan	Document outlining procedure for restoring computing systems and recovering data following an event.

Term	Definition
life safety	Protection of people's health and welfare during an event. The first of the four crisis management priorities.
loss of facility or region	Losing the use of a building or other site needed to carry out business activities. Alternately, the disruption of facilities throughout a region, e.g., as the result of a power failure. One of the four types of disruption.
loss of human resources	Losing access to personnel needed to carry out business activities. One of the four types of disruption.
loss of technology	Losing the use of a technological resource needed to carry out business activities. One of the four types of disruption.
loss of vendor	Losing a third-party supplier, product, or service needed to carry out business activities. One of the four types of disruption.
manual workaround	A backup method of completing a business process that does not rely on computer technology.
metrics	Methods of quantifying performance aspects of a business continuity program.
micro mock disaster exercise	Brief, informal mock disaster exercise in which participants state how they would respond to a disaster scenario presented by a facilitator. Usually added to a meeting that is being held for another purpose.
mission critical activities	The processes and operations an organization must carry out in order to accomplish its core mission.
mission critical facility	A building or other physical site essential to an organization's ability to accomplish its mission.
mitigation controls	Steps taken and resources created to reduce organizational risk, e.g., business impact analyses, recovery plans, recovery exercises.

Term	Definition
mitigation planning	The process of assessing organizational risk and taking steps to reduce it.
mitigation strategy	A high-level approach adopted in order to reduce risk. The principal mitigation strategies are risk acceptance, risk avoidance, risk limitation, and risk transfer.
mock disaster exercise	Training or assessment activity in which an organization is tasked with coping with a fictional disaster.
NFPA 1600	Business continuity standard issued by the National Fire Protection Association. Industry-agnostic standard covering all levels from strategic to tactical. Very practical and direct.
NIST 800	Business continuity standard published by the National Institute of Standards and Technology, an agency of the U.S. Commerce Dept. Focused on IT.
natural threat	Danger posed to an organization by natural phenomena, e.g., hurricanes, wildfires. One of the three types of business continuity threat.
operational risk management (ORM)	The process of managing the possibility that adverse events might occur internally and externally as an organization is carrying out its mission.
organizational culture	The values, habits, and attitudes of an organization.
organized chaos	Situation in which the confusion brought on by a crisis is prevented from penetrating below the surface by an underlying structure and competence.
outage	An interruption in the provision of a service.
pandemic plan	Document giving procedure for maintaining operations during a pandemic, focused on coping with a loss of human resources.

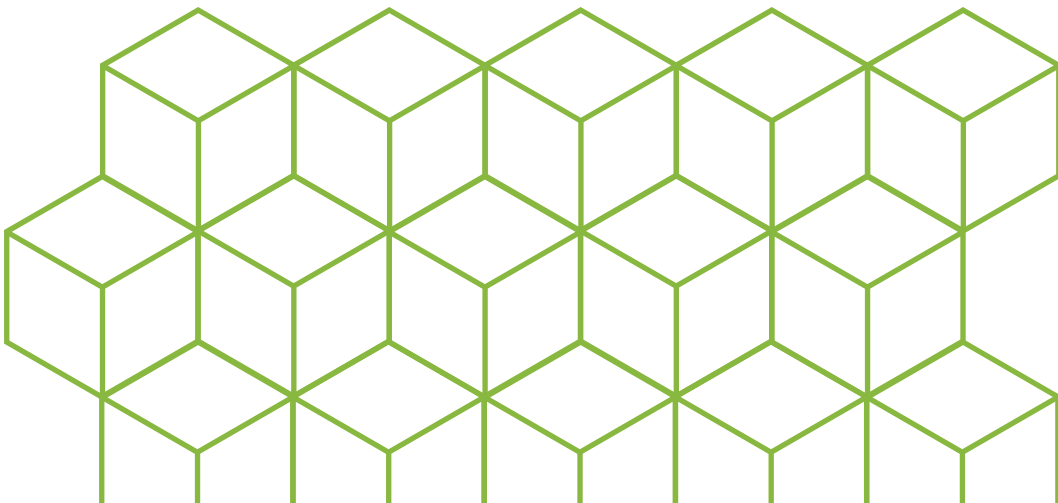
Term	Definition
post-incident analysis (PIA)	Assessment conducted after the resolution of an event to identify the strengths and weaknesses of the organization's response.
Pre-work	See BIA pre-work.
program administration	The administrative aspects of a business continuity management program, including oversight, governance, policy, and standards. One of the four main business continuity areas.
property preservation	The protection of physical assets during a crisis. One of the four crisis management priorities.
qualitative impact	Type of event-related damage that cannot be expressed in numbers, e.g. reputational damage. Used to help an organization prioritize its business processes when conducting a business impact analysis.
quantitative impact	Type of event-related damage that can be expressed in numbers, e.g. loss of revenue. Used to help an organization prioritize its business processes when conducting a business impact analysis.
recoverability	An organization's ability to resume its operations after an impact.
recovery	The return to operation of a business process or IT process after a disruption.
recovery exercise	Training or assessment activity addressing the restoration of critical business processes.
recovery plan	Document outlining procedure to bring a business process or IT process back online following an outage.
recovery plan template	See business continuity template.

Term	Definition
recovery point objective (RPO)	The maximum amount of data that can be permanently lost after an outage before a process is materially impacted, measured in terms of time. The RPO helps in determining an appropriate data protection strategy for the underlying application.
recovery strategy	The overall approach that will be used to restore a business process or IT process.
recovery time objective (RTO)	The time window within which a business process and its associated applications must be restored after an outage in order to prevent serious impact to the organization.
remote work model	A method of workplace organization in which employees work at a location away from company facilities.
reputational impact	Damage to an organization's image or standing caused by an event.
residual risk	The risk that remains in an organization or process after the implementation of mitigation controls.
resilience	A highly desirable state in which an organization, through sound business continuity management, has obtained the ability to continue its critical operations even during disruptions.
return on investment (ROI)	Financial benefi s accruing to an organization as a result of spending on business continuity initiatives.
risk	The possibility that an activity will result in harm.
risk acceptance	A mitigation strategy involving a conscious decision to remain vulnerable to a potential harm, usually based on a cost-benefit nalysis.
risk appetite	The theoretical amount of risk management is willing to accept as the organization carries out its activities.

Term	Definition
risk avoidance	A mitigation strategy centered on altering organizational behavior to eliminate a given risk.
risk limitation	A mitigation strategy in which measures are taken to reduce risk, short of completely eliminating it. Incorporates a combination of the strategies of risk avoidance and risk acceptance.
risk management	The process of assessing and mitigating the danger to which an organization is exposed as it carries out its activities.
risk mitigation controls	See mitigation controls.
risk mitigation planning	The activity of assessing organizational risk and taking steps to reduce it.
risk score	A metric indicating the level of residual risk in a business process, derived from consideration of such factors as the threats facing it and its RTO.
risk tolerance	The amount of deviation from the organization's risk appetite that management is willing to incur in a real-world situation.
risk transfer	A mitigation strategy in which a risk is passed on to another organization, such as by hiring a third-party vendor to perform the associated function.
roadmap	A plan for closing gaps in an organization's business continuity program that includes remediation activities and timeframes for their completion.
service level agreement (SLA)	Contract between an organization and a vendor specifying the type, amount, and reliability of a service to be provided.
single point of failure (SPOF)	A resource whose loss would interrupt the performance of a critical operation owing to an absence of redundancy. Can be a facility, a piece of equipment, or a person who is the only employee who knows how to perform a critical activity.

Term	Definition
site recovery plan	Plan giving the procedure for temporarily reestablishing a facility's operations in another location.
situational awareness	The state of being attuned to the whole breadth of relevant events taking place during a crisis.
social media policy	Company rules governing what employees are allowed to post about the organization on social media.
Software as a Service (SaaS)	Computing services obtained through a third-party vendor.
stakeholder	Individual or group that contributes to an organization and has a recognized interest in its success.
subject matter expert (SME)	A person with specialized knowledge about a topic under discussion.
supply chain	Network of vendors whose products and services an organization needs to carry out its operations.
supply chain risk management (SCRM)	The process of managing threats to an organization's access to essential goods and services.
supply chain security	The degree to which an organization enjoys certain, reliable, and timely access to the third-party vendors, products, and services it needs to carry out its operations. One of the four main business continuity areas.
tabletop exercise	Discussion-based mock disaster exercise.
technology threat	Threat to an organization caused by technological entities, e.g., malware. One of the three types of business continuity threat.
third-party vendor	Outside provider of a product or service that an organization needs to carry out its mission.
threat and risk assessment (TRA)	A written evaluation of the hazards facing an organization.

Term	Definition
validation	The process of verifying that a recovery plan is functional. Also see data validation.
value on investment (VOI)	A measure of the value of a BC program in terms of people, time, and money. High compliance with business continuity standards and low residual risk equate to high VOI.
vendor agreement	A contract between the organization and a supplier. Can stipulate requirements for the supplier's business continuity program.
vendor site visit	Physical inspection by an organization of a facility belonging to one of its suppliers to assess the supplier's resilience.
vendor threat assessment	Analysis conducted by an organization of the hazards facing one of its suppliers.
virtual command center	A nonphysical space created with collaboration tools for use in managing an event.
weighting (of impact categories)	The process of determining how much importance to give various impact categories when conducting a business impact analysis. Optimal choices vary depending on an organization's industry, mission, and values.
work from home	Workplace model in which employees perform work activities from their residences.



Business continuity consulting for today's leading companies

- A 20+-year proven track record of applying industry standards and best practices across a diverse pedigree of clients.
- A simple mission: Ensure the continuous operations of our clients' critical processes.
- We seek to partner with clients who have a commitment to BCM versus a check the box mentality.
- SaaS Tools: BIA On-Demand, BCM One, Compliance Confidence, Residual Risk.

Contact us for a free consultation at mha-it.com

MHA Consulting