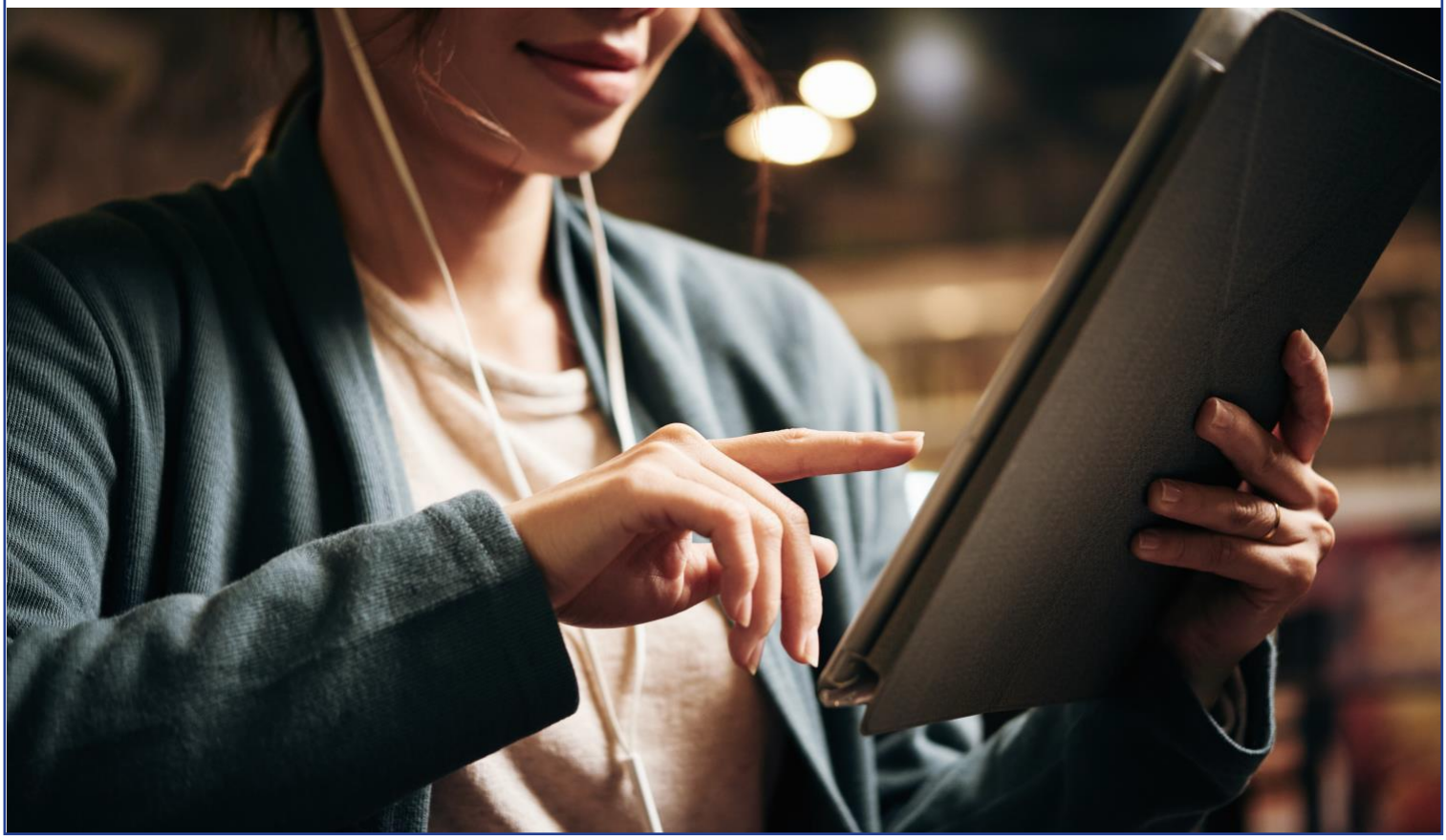
Train.
Prepare.
Recover.

DRI International Glossary for Resilience



Version 2 — July 2018 Rev. 3 (2023)

Maintained by DRI International

For more information, visit www.drii.org, email **driinfo@drii.org**, or **call 866.542.3744**

Legal Disclaimer

These materials are presented solely for informational purposes. DRI International, its officers, directors, staff, licensees, affiliates and volunteers (“DRI International”) are not offering it as legal or other professional services advice. While best efforts have been used in preparing these materials, DRI International makes no representations or warranties of any kind and assumes no liabilities of any kind with respect to the accuracy or completeness of the contents and specifically disclaims any implied warranties of merchantability or fitness of use for a particular purpose. DRI International shall not be held liable or responsible to any person or entity with respect to any loss or incidental or consequential damages caused, or alleged to have been caused, directly or indirectly, by the information contained herein. Every organization is different and the definitions contained herein may not be suitable for your situation. You should seek the services of a competent professional before beginning any improvement program.

Committee Members

Permanent Committee Members

Chair: Dean C. Gallup, MBCP CHEP
Coordinator: Kathy Acevedo, ABCP

Lyndon Bird
Mary Crea, MBCP
John Franchy, CBCP
Jim Kinsman, MBCP
Peter McEvoy
James Price, MBCP, CBCV
Gary Villeneuve, MBCP, CBCLA, CPSCP, ARMP, CBCV
Bobby Williams, MBCP
Mark Wilson, MBCP
Rob Zegarra, MBCP, CCRP

Acknowledgments

Al Berman, MBCP
Buffy Rojas Leach

And to all the attendees of the Annual DRI Conference and members of DRI International who attended the plenary sessions and contributed insight, suggestions and updates to the DRI Glossary for Resilience.

Introduction

Clear communication is essential, yet we all have had experiences in which the same terms are used to describe different situations. For example, which term do you use to describe a fire? Is it an emergency, an incident, an event, a disaster, or all of the above? Sometimes the discrepancies are subtle, sometimes not. In everyday situations, ambiguity can be comical, confusing, or at worst, annoying. In a crisis, unclear definitions can be dangerous.

As the oldest and largest nonprofit organization of its kind, DRI International is the industry thought leader and service is our mission. Our Certified Professionals and the greater resilience community look to us for guidance. When we were asked to offer a DRI glossary, we accepted the challenge. The question we posed was quite simple: What can we create to best serve the profession? We soon realized that the industry already has many glossaries and terms. These various documents offer much insight and are already widely used in various parts of the world. Rather than add to the abundant number of existing glossaries, we felt that DRI should act as an arbiter of existing definitions. For this reason, the DRI glossary limits the number of new definitions we create. Instead, we select and present the best-in-class definitions already in use in the English language.

In keeping with the makeup of our Certified Professionals, the process had to be international, inclusive, and apolitical, so we established a volunteer committee of industry leaders to review and vote on the terms and definitions that would ultimately appear in this document. The initial version was the result of nearly two years of effort to build a standard set of terms. We always expected that this would be a living document, subject to revisions and changes. There have been numerous additions and edits over the years as well as the introduction of versions in Arabic, Chinese, Portuguese, and Spanish, but this is the first major revision. We are eager for your feedback, as well as the participation of representatives from each of the source documents.

In conclusion, we hope you find our work useful. It is with great pride that we present this document in the hope that it will further advance the profession.

Notes from the Chair:

"Boy, those French: They have a different word for everything!" – Steve Martin
Welcome to the DRI International Glossary, which is celebrating its 10th Anniversary in 2024! I remember participating in the DRI2013 terms and definitions breakout session in Philadelphia, the birthplace of America, where the idea of the DRI International Glossary was born as well. I was intrigued by the concept of a consolidated glossary of resilience terms, not only at a professional level, but personally as terms I helped define for NIST were included in the session. Getting on the Glossary Committee was a thrill, and I was honored to become the new Chair in 2017, succeeding the great work of Bobby Williams, our inaugural Chair.

In 2018, the Glossary had major updates to both format and content. Our intent then was and continues to be to make the glossary more readable, easier to access, and more usable to those in the resilience community. Format changes included grouping related terms together, allowing the reader to see alternatives or similar types of terms in one place. The source of the term was clearly indicated, and our source references section is expanded, with an explanation of the standard or organization, and a link to access their full glossaries or pages. We included a list of changes to the glossary to assist those needing to compare versions.

Standards and glossaries, like everything else, change, as our industry has changed. Specialties such as Cybersecurity and Cyber Resilience were in their infancy in 2014. References either were updated or rescinded, and major updates to terms and references were required. Each year, the Glossary Committee has reviewed terms and references for their continued inclusion in the glossary, and if changes were required. Additionally, we took input from DRI Conference participants on terms they would like to see, and areas they thought we may have missed the mark.

DRI International became a reference source in 2018. The Committee felt some terms from old or rescinded references were relevant enough to adopt as our own. Additionally, due to changes in our industry, we saw terms that were needed, but could not find sufficient definitions. DRI's inaugural definition to the Glossary was "Cyber Resilience" in 2020. We have since refined that term's definition and are looking at several terms the Committee feels are critical, but do not have a strong definition. The Glossary went through an extensive review with the release of the 2022 DRI Professional Practices update. The Glossary is a key support document to all DRI certifications and classes. Our Director of Education is a Committee member and coordinates with us to make sure key terms discussed in classes are defined in the Glossary.

The Committee is continuing efforts to continue to improve the Glossary, including possible sections for acronyms, and categorizing terms into Resilience, Cyber and Risk. These are not insignificant changes, and we are taking our time to make sure that any major changes are made correctly.

My sincere thanks to all the members of the DRI Glossary Committee for all their work over the past decade! Your efforts and professionalism continue to make this a world class reference. Thanks to DRI International President and CEO Chloe Demrovsky for her support and guidance, and to Kathy Acevedo for coordinating committee events and working with the manuscript. Thanks also to all those who provided comments and suggestions on improvements and changes; each input was evaluated and discussed thoroughly by the committee. Our only request is that you continue to provide feedback; this is the best way to make the Glossary even better!

Thank you

Dean C Gallup

Dean C. Gallup, MBCP, CHEP
Glossary Committee Chair

How to use this document:

Here are a few points to keep in mind as you reference this document:

- None of the definitions in this document are original. The citations to the original source documents chosen by the committee can be found under the term being defined.
- In some cases, definitions have been modified for consistency, including the removal of examples, capitalization, or internal references.
- If a note or comment from the source document was included, it has been prefaced by "*[Source Name] Editor's Note*".
- Internal to some definitions are multiple points. Letters are used to list the points internal to a single definition (i.e., a., b., c.)
- Some words or terms may have multiple indented terms underneath (in smaller text). The indented definitions are those deemed by the committee to be similar or a type of the main definition
- Names of organizations, associations, and certifications are not included.
- All sources are included in the section entitled "Cited References" along with a description of the organization or document. Whenever possible, the description is quoted from the document or website of the organization it describes. A link (current as of 06/2018) is included to access the organization's full glossary or web page.

For more information about the process or if you have any questions, please contact DRI at +1-866-542-3744 or email at driinfo@drii.org.

How this document is maintained:

Here are a few points about how this document is maintained:

- Input and suggestions for improvement will ALWAYS be accepted.
  - » Inputs and suggestions can be sent to driinfo@drii.org
- The committee will review this document quarterly.
  - » The review will be based on:
    - Comments received
    - Significant changes to industry standards
    - Significant changes to laws and regulations
    - Significant changes to regulatory guidance
- Hard copies cannot be controlled. This document was last updated as of the date on the first page. For a current version of this document visit www.drii.org
- An annual public review session will occur at the DRI conference.
- A formal annual revision to the document will be made public by the fourth month following the DRI conference.
  - » The annual revision will maintain the name of the document with a "Rev #"
- Major releases to this document will occur on a four (4) year cycle.
  - » This scheduled release will be named with the release year and no revision number.
  - » The major release could include:
    - New or changed terms
    - Removal of terms
    - New, removed or changed reference sources
    - A "Glossary Changes" document
    - Major releases

Table of Contents

A 1
B 5
C 10
D 14
E 17
F 21
G 21
H 22
I 23
J 25
L 26
M 26
N 28
O 28
P 29
R 30
S 34
T 37
U 38
V 38
W 39
Cited References 41
Glossary Changes 46
1. Overall Changes to DRI Glossary 46
2. Terms Added 46
3. Terms Changed 47
4. Terms Moved 48
5. Terms Removed 49
6. Other Changes 49

A

Acceptable Downtime
ASIS

Maximum elapsed time between a disruption and restoration of needed operational capacity or capability.

Acceptable Risk
UNDRR

The level of potential losses that a society or community considers acceptable given existing social, economic, political, cultural, technical and environmental conditions. UNDRR Editor's Note: In engineering terms, acceptable risk is also used to assess and define the structural and non-structural measures that are needed in order to reduce possible harm to people, property, services and systems to a chosen tolerated level, according to codes or "accepted practice" which are based on known probabilities of hazards and other factors.

Account Manager
ITIL

A role that is very similar to business relationship manager, but includes more commercial aspects. Most commonly used when dealing with external customers.

Accreditation
CNSSI-4009

Formal declaration by a Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Activation
BCI/DRJ

The implementation of business continuity procedures, activities and plans in response to a serious incident, emergency, event or crisis.

Active Monitoring
ITIL

Monitoring of a configuration item or an IT service that uses automated regular checks to discover the current status.

Alert
DRJ

Notification that a potential disaster situation is imminent exists or has occurred; usually includes a directive for personnel to stand by for possible activation.

All-Hazards
NFPA 1600

An approach for prevention, mitigation, preparedness, response, continuity, and recovery that addresses a full range of threats and hazards, including natural, human-caused, and technology-caused.

Alternate Routing

BCI/DRJ

The routing of information via an alternate cable or other medium (i.e. using different networks should the normal network be rendered unavailable). A site held in readiness for use during a business continuity invocation to continue the urgent and important processes of an organization. The term applies equally to office or technology requirements. BCI Editor's Note: Alternate sites may be known as 'cold', 'warm' or 'hot'. They might also be called simply a recovery or backup site. In the UK the more traditional term is "alternative site".

Alternate Site

DRJ

An alternate operating location to be used by business functions when the primary facilities are inaccessible.

a. Another location, computer center or work area designated for recovery.
b. Location, other than the main facility, that can be used to conduct business functions.
c. A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster.

Similar Terms

Note: There may be other variations not noted here (such as Alternate Facility) that refer generically to a designated alternate workspace and/or data center.

Alternate Locations (FCD 1) - Fixed, mobile, or transportable locations, other than the headquarters facility, where D/A leadership and continuity personnel relocate in order to perform essential functions following activation of the continuity plan. These include locations to which agency leadership may devolve. These locations refer to not only locations sites but also work arrangements such as telework and mobile work.

Alternate Work Area (DRJ) Recovery environment complete with necessary infrastructure (desk, telephone, workstation, and associated hardware and equipment, communications, etc.).

Fallback (BCI/DRJ) A fallback facility is another site/building that can be used when the original site/building is unusable or unavailable.

Secondary Site (DRI) A location other than the primary site which can be used for the resumption of business operations and other functions in the event of a disaster, a major system or infrastructure malfunction or an inability to access the primary site. A secondary site can be used:
a. in the narrower sense for the replication of programs and data in order to safeguard data integrity, with the replicated data being stored externally to ensure the resumption of business operations following the destruction or loss of data; or
b. in the broader sense for the maintenance of a comprehensive alternative system (i.e. a fallback system comprising hardware, software and data) to cater for the possibility of the production system not being available. In the event that the fallback system is located in the vicinity of the production system and a third system in another location is reserved for emergencies and disasters, the latter is referred to as the "disaster system".

Work Area Recovery (BCI/DRJ) The component of recovery and continuity that deals specifically with the relocation of a key function or department in the event of a disaster, including personnel, essential records, equipment supplies, work space, communication facilities, work station computer processing capability, fax, copy machines, mail services, etc. Office recovery environment complete with necessary office infrastructure (desk, telephone, workstation, hardware, communications).

Application
DRI

Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

Application Management
ITIL

The function responsible for managing applications throughout their lifecycle.

Application Portfolio
ITIL

A database or structured document used to manage applications throughout their lifecycle. The application portfolio contains key attributes of all applications. The application portfolio is sometimes implemented as part of the service portfolio, or as part of the configuration management system.

Application Recovery
BCI/DRJ

The component of disaster recovery that deals specifically with the restoration of business system software and data after the processing platform has been restored or replaced.

Architecture
ITIL

The structure of a system or IT service, including the relationships of components to each other and to the environment they are in. Architecture also includes the standards and guidelines, which guide the design and evolution of the system.

Assessment
ITIL

Inspection and analysis to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.

Asset
BCI/DRJ

Anything that has value to the organization. BCI Editor's Note: This can include physical assets such as premises, plant and equipment as well as HR resources, intellectual property, goodwill and reputation.

Asset Management
ITIL

Asset management is the process responsible for tracking and reporting the value and ownership of financial assets throughout their lifecycle. Asset management is part of an overall service asset and configuration management process.

Audit
ISACA

Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met. Scope Note: May be carried out by internal or external groups.

Audit Trail
CNSSI-4009

1. A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.
2. A record showing who has accessed an information technology (IT) system and what operations the user has performed during a given period.

Auditor
ASIS

Person with competence to conduct an audit. [ISO 9001 2000]

Authentication
DRI

The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. NIST SP 800-53: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authority Having Jurisdiction
NFPA 1600

An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

Authorization
CNSSI-4009

Access privileges granted to a user, program, or process or the act of granting those privileges.

Automatic Call Distribution (ACD)
ITIL

Use of information technology to direct an incoming telephone call to the most appropriate person in the shortest possible time. ACD is sometimes called Automated Call Distribution.

Availability
HIPAA

The property that data or information is accessible and useable upon demand by an authorized person.

Awareness
BCI/DRJ

To create understanding of basic BCM issues and limitations. This will enable staff to recognize threats and respond accordingly. Examples of creating such awareness include distribution of posters and flyers targeted at company-wide audience or conducting specific business continuity briefings for executive management of the organization. Awareness is less formal than training and is generally targeted at all staff.

B

Backup
BCI/DRJ

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.

Basel Accord (Basel III)
BCI/DRJ

An agreement by international financial institutions on the financial risk assessment and ratios between capital and risk.

Benchmark
ITIL

The recorded state of something at a specific point in time.

Benchmarking
ITIL

Comparing a benchmark with a baseline or with best practice. The term benchmarking is also used to mean creating a series of benchmarks over time, and comparing the results to measure progress or improvement.

Best Practice
ITIL

Proven activities or processes that have been successfully used by multiple organizations.

Biological Hazard
UNDRR

Process or phenomenon of organic origin or conveyed by biological vectors, including exposure to pathogenic micro-organisms, toxins and bioactive substances that may cause loss of life, injury, illness or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage. UNDRR Editor's Note: Examples of biological hazards include outbreaks of epidemic diseases, plant or animal contagion, insect or other animal plagues and infestations.

Black Swan
BCI/DRJ

A term popular in BCM, based upon a book of the same name in which the author defines a black swan as an event that could not be predicted by normal scientific or probability methods. BCM professionals need to prepare for "black swan" events.

Business Continuity
NFPA 1600

An ongoing process to ensure that the necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.

Business Continuity Coordinator
DRJ

A role within the BCM program that coordinates planning and implementation for overall recovery of an organization or unit(s).

Business Continuity Management (BCM)
ISO 22301

Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Business Continuity Management Lifecycle
BCI/DRJ

A series of business continuity activities which collectively cover all aspects and phases of the BCM program.

Business Continuity Management Program
BCI/DRJ

Ongoing management and governance process supported by top management and appropriately 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 and services through training, exercising, maintenance and review.

Business Continuity Management System (BCMS)
ISO 22301

Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity. ISO Editor's Note: The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes and resources.

Business Continuity Management Team
BCI/DRJ

A group of individuals functionally responsible for directing the development and execution of the business continuity plan, as well as responsible for declaring a disaster and providing direction during the recovery process, both pre-disaster and post-disaster.

Business Continuity Maturity Model (BCMM)
BCI/DRJ

A tool to measure the level and degree to which BCM activities have become standard and assured business practices within an organization.

Business Continuity Plan (BCP)
BCI/DRJ

A documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical products and services at an acceptable predefined level.

Similar Term

Continuity Plan *(*FCD 1) A documented plan that details how an individual organization will ensure it can continue to perform its essential functions during a wide range of events that impact normal operations.

Business Continuity Plan Administrator
BCI/DRJ

The designated individual responsible for plan documentation, maintenance, and distribution.

Business Continuity Planning
BCI/DRJ

The process of developing prior arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions can continue within planned levels of disruption. The end result of the planning process is the BC Plan.

Business Continuity Policy Statement
BCI/DRJ

A BCM policy sets out an organization'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 Program
ISO 22301

Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.

Business Continuity Program Board
BCI/DRJ

A management group to give advice, guidance and management authorization to the BC Manager.

Business Continuity Steering Committee
BCI/DRJ

A top management group to give direction, advice, guidance and financial approval for the BCM programs undertaken by the BCM manager and various BC coordinators.

Business Continuity Strategy
BCI/DRJ

A strategic approach by an organization to ensure its recovery and continuity in the face of a disaster or other major incidents or business disruptions.

Business Continuity Team
BCI/DRJ

The strategic, tactical and operational teams that would respond to an incident, and who should contribute significantly to the writing and testing of the BC plans.

Business Function
BCI/DRJ

A description of work that is performed to accomplish the specific requirements of the organization. Examples of business function include delivering raw materials, paying bills, receiving cash and inventory control.

Business Impact Analysis (BIA)
FCD 1

A method of identifying the effects of failing to perform a function or requirement.

Business Interruption
BCI/DRJ

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.

Business Interruption Costs
BCI/DRJ

The impact to the business caused by different types of outages, normally measured by revenue lost.

Business Objective
ITIL

The objective of a business process, or of the business as a whole.

Business Operations ITIL	The day-to-day execution, monitoring and management of business processes.
Business Process ITIL	A process that is owned and carried out by the business. A business process contributes to the delivery of a product or service to a business customer.
Business Recovery BCI/DRJ	Steps taken to resume the business within an acceptable timeframe following a disruption.
Business Recovery Coordinator BCI/DRJ	An individual or group designated to coordinate or control designated processes or testing.
Business Recovery Team BCI/DRJ	A group responsible for: relocation and recovery of business unit operations at an alternate site following a business disruption; and subsequent resumption and restoration of those operations at an appropriate site.
Business Recovery Timeline BCI/DRJ	The approved sequence of activities required to achieve stable operations following a business interruption. This timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.
Business Resumption Singapore MAS	The condition of a function, following its recovery, when it is ready to take on tasks and activities to meet new business obligations.
Business Unit BCI/DRJ	A business unit within an organization e.g. branch/ division.
Business Unit Coordinator BCI/DRJ	A staff member appointed by a business unit to serve as the liaison person responsible for all BCM direction and activities within the unit.

C

Call Tree
BCI/DRJ

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

Capacity
UNDRR

The combination of all the strengths, attributes and resources available within a community, society or organization that can be used to achieve agreed goals. UNDRR Editor's Note: Capacity may include infrastructure and physical means, institutions, societal coping abilities, as well as human knowledge, skills and collective attributes such as social relationships, leadership and management. Capacity also may be described as capability. Capacity assessment is a term for the process by which the capacity of a group is reviewed against desired goals, and the capacity gaps are identified for further action.

Change management
FFIEC

Change management refers to the broad processes for managing organizational change. Change management encompasses planning, oversight or governance, project management, testing, and implementation.

Checklist
BCI/DRJ

a. Tool to remind and /or validate that tasks have been completed and resources are available, to report on the status of recovery.
b. A list of items (names or tasks etc.) to be checked or consulted.

Chief Information Officer (CIO)
CNSSI-4009

Agency official responsible for:
a. Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information systems are acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;
b. Developing, maintaining, and facilitating the implementation of a sound and integrated information system architecture for the agency; and
c. Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. CNSSI Editor's Note: Organizations subordinate to federal agencies may use the term Chief Information Officer to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.

Civil Emergency
BCI/DRJ

Event or situation which threatens serious damage to human welfare in a place, environment or a place or the security of that place.

Cloud Computing
CNSSI-4009

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cold Site
BCI/DRJ

An alternate facility that already has in place the environmental infrastructure required to recover critical business functions or information systems, but does not have any pre-installed computer hardware, telecommunications equipment, communication lines, etc. These must be provisioned at time of disaster.

Command Center
BCI/DRJ

The location, local to the event but outside the immediate affected area, where tactical response, recovery and restoration activities are managed. There could be more than one command center for each event reporting to a single emergency operations center.

Confidentiality
HIPAA

The property that data or information is not made available or disclosed to unauthorized persons or processes.

Contingency Plan
BCI/DRJ

A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations.

Contingency Planning
BCI/DRJ

Process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively impacts the organization.

Continual Improvement
NFPA 1600

Recurring process of enhancing the management program in order to achieve improvements in overall performance consistent with the entity's policy, goals, and objectives.

Continuity
ASIS

Strategic and tactical capability, pre-approved by management, of an organization to plan for and respond to conditions, situations, and events in order to continue operations at an acceptable predefined level. ASIS Editor's Note: Continuity, as used in this Standard, is the more general term for operational and business continuity to ensure an organization's ability to continue operating outside of normal operating conditions. It applies not only to for profit companies, but organizations of all natures, such as non-governmental, public interest, and governmental organizations.

Continuity Manager
FCD 1

The Senior Continuity Planner responsible for managing day-to-day continuity programs, representing his/her D/A on the Continuity Advisory Group and working groups, as appropriate, and reporting to the Continuity Coordinator on all continuity program activities.

Continuity of Government (COG)
FCD 1

A coordinated effort within each branch of government (e.g., the Federal Government's executive branch) to ensure that National Essential Functions (NEFs) continue to be performed during a catastrophic (COG) emergency. FCD Editor's Note: this term may also be applied to non-Federal governments.

Continuity of Operations (COOP) Plan
NIST SP 800-34

A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.

Continuous Availability
ITIL

A continuously available IT service.

Continuous Operations
ITIL

1. The ability of an organization to perform its processes without interruption.
2. A means of managing a risk, ensuring that a business objective is achieved, or ensuring that a process is followed.

Control
ISACA

The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature. Example controls include policies, procedures, roles, RAID, door-locks etc. A control is sometimes called a countermeasure or safeguard. Control also means to manage the utilization or behavior of a configuration item, system or IT service.

Corporate Governance
BCI/DRJ

The system/process by which the directors and officers of an organization are required to carry out and discharge their legal, moral and regulatory accountabilities and responsibilities.

Corrective Action
ISO 22301

Action to eliminate the cause of nonconformity and to prevent recurrence.

Cost Benefit Analysis
BCI/DRJ

A process (after a BIA and risk assessment) that facilitates the financial of different strategic BCM options and balances the cost of each option against the perceived savings.

Crisis
BCI/DRJ

A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate. Or, an occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an organization.

Crisis Management
BCI/DRJ

The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, and ability to operate.

Crisis Management Team (CMT)
BCI/DRJ

A group of individuals responsible for developing and implementing a comprehensive plan for responding to a disruptive incident. The team consists of a core group of decision-makers trained in incident management and prepared to respond to any situation. BCI Editor's Note: In most countries crisis and incident are used interchangeably but in the UK the term crisis has traditionally been used for wide area incidents involving emergency services. However, the recent UK Government sponsored PAS200 document seeks to extent the use of this term beyond the public sector.

Critical Infrastructure
BCI/DRJ

Physical assets whose incapacity or destruction would have a debilitating impact on the economic or physical security of an organization, community, nation, etc.

Similar Term

Critical Asset (FCD 1) An asset of such strategic importance to the performance of essential functions that its incapacitation or destruction would have a very serious or debilitating effect on an organization's ability to perform the function(s).

Cyber Attack
FFIEC

An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network; An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Resilience
DRI

An entity's ability to continuously deliver their products and services despite any adverse cyber events by actively preparing, planning, reacting, responding, and recovering the entity from cyberattacks. In addition, adapting to changing threat landscapes; effectively training personnel; and ensuring that response and recovery plans are maintained and exercised.

Cybersecurity
CNSSI 4009

The prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

D

Damage Assessment
NFPA 1600

An appraisal or determination of the effects of the incident on humans, on physical, operational, economic characteristics, and on the environment.

Data Integrity
FFIEC

The property that data has not been destroyed or corrupted in an unauthorized manner; Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Data Mirroring
BCI/DRJ

A process whereby critical data is replicated to another device.

Data Recovery
BCI/DRJ

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

Declaration
BCI/DRJ

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

Delegation of Authority FCD 1	Identification, by position, of the authorities for making policy determinations and decisions at HQ, field levels, and all other organizational locations. Generally, pre-determined delegations of authority will take effect when normal channels of direction have been disrupted and will lapse when these channels have been reestablished.
Denial of Service (DoS) CNSSI-4009	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)
Dependency BCI/DRJ	The reliance or interaction of one activity or process upon another.
Devolution FCD-1	The transfer of statutory authority and responsibility from an organization's primary operating staff and facilities to other staff and alternate locations to sustain essential functions when necessary.
Devolution Emergency Response Group (DERG) FCD-1	Personnel stationed at a geographically dispersed location, other than the primary location, who are identified to continue performance of essential functions.
Disaster BCI/DRJ	A sudden, unplanned catastrophic event causing unacceptable damage or loss. a. An event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time b. An event where an organization's management invokes their recovery plans.
Disaster Recovery (DR) BCI/DRJ	The technical aspect of business continuity. The collection of resources and activities to re-establish information technology services (including components such as infrastructure, telecommunications, systems, applications and data) at an alternate site following a disruption of IT services. Disaster recovery includes subsequent resumption and restoration of those operations at a more permanent site.
Disaster Recovery Plan NIST SP 800-34	A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Disaster Recovery Planning
BCI/DRJ

The activities associated with the continuing availability and restoration Planning of the IT infrastructure.

Disaster Risk Reduction
UNDRR

The concept and practice of reducing disaster risks through systematic efforts to analyze and manage the causal factors of disasters, including through reduced exposure to hazards, lessened vulnerability of people and property, wise management of land and the environment, and improved preparedness for adverse events. Comment: A comprehensive approach to reduce disaster risks is set out in the United Nations-endorsed Hyogo Framework for Action, adopted in 2005, whose expected outcome is "The substantial reduction of disaster losses, in lives and the social, economic and environmental assets of communities and countries." The International Strategy for Disaster Reduction (ISDR) system provides a vehicle for cooperation among Governments, organizations and civil society actors to assist in the implementation of the Framework. Note that while the term "disaster reduction" is sometimes used, the term "disaster risk reduction" provides a better recognition of the ongoing nature of disaster risks and the ongoing potential to reduce these risks.

Disaster/Emergency Management
NFPA 1600/BCI/DRJ

1. An ongoing process to prevent, mitigate, prepare for, respond to, maintain continuity during, and recover from an incident that threatens life, property, operations, or the environment. (NFPA 1600)
2. A program that implements the mission, vision, strategic goals, objectives and management framework of the program and organization. (BCI/DRJ)

Disruption
ASIS

An event that interrupts normal business, functions, operations, or processes, whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a blackout, terror attack, technology failure, or earthquake). ASIS Editor's Note: A disruption can be caused by either positive or negative factors that will disrupt normal functions, operations, or processes.

Distributed Denial of Service (DDoS)
CNSSI-4009

A denial of service technique that uses numerous hosts to perform the attack.

Document
BCI/DRJ

Information and its supporting medium such as paper, magnetic, electronic or optical computer disc or image.

Downtime
BCI/DRJ

A period in time when something is not in operation. BCI Editor's Note: This is often called outage when referring to IT services and systems.

Duty of Care
BCI/DRJ

A corporate governance requirement to take care of the assets of the organization – a duty incumbent on officers of an enterprise.

E

Emergency
ASIS

1. An unexpected or impending situation that may cause injury, loss of life, destruction of property, or cause the interference, loss, or disruption of an organization's normal business operations to such an extent that it poses a threat.
2. Sudden, urgent, usually unexpected occurrence or event requiring immediate action. [ISO/PAS 22399 2007] ASIS Editor's Note: An emergency is usually a disruptive event or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

Emergency Management
BCI/DRJ

Emergency management is the responsibility of governments and public authorities, complying with appropriate laws that relate to emergency response. BCI Editor's Note: An Emergency Management Plan (EMP) is usually managed by one or more Emergency Management Teams (EMT). Different structures exist in different countries.

Emergency Operations Center
BCI/DRJ

The physical and/or virtual location from which strategic decisions are made and all activities of an event/incident/crisis are directed, coordinated and monitored. DRJ Editor's Note: EOC is different from Command Center.

Emergency Operations Center
BCI/DRJ

The physical and/or virtual location from which strategic decisions are made and all activities of an event/incident/crisis are directed, coordinated and monitored. DRJ Editor's Note: EOC is different from Command Center.

Emergency Preparedness
BCI/DRJ

The capability that enables an organization or community to respond to an emergency in a coordinated, timely, and effective manner to prevent the loss of life and minimize injury and property damage.

Emergency Relocation Group (ERG)
FCD-1

Staff assigned to continue performance of essential functions at an alternate location in the event that their primary operating facility or facilities are impacted or incapacitated by an incident.

Emergency Response
BCI/DRJ

The immediate reaction and response to an emergency situation commonly focusing on ensuring life safety and reducing the severity of the incident.

Emergency Response Plan
BCI/DRJ

A documented plan usually addressing the immediate reaction and response to an emergency situation.

Similar Terms

Emergency Plan (FCD 1) Documented procedures that direct coordinated actions to be undertaken in response to threats that are typically of limited duration, and do not require an organization to activate its continuity plan. Also referred to as Occupant Emergency Plan or Building Closure Plan.

Occupant Emergency Plan (OEP) (FCD 1) A short-term emergency response plan which establishes procedures for evacuating buildings or sheltering-in-place to safeguard lives and property. Organizations may refer to this plan as the Emergency Plan or Building Closure Plan. Common scenarios that would lead to the activation of these plans include inclement weather, fire, localized power outages, and localized communications outages. These types of events are generally short-term in nature.

Emergency Response Team (ERT)
BCI/DRJ

Qualified and authorized personnel who have been trained to provide immediate assistance.

Enterprise
CNSSI-4009

An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management.

Enterprise Risk Management (ERM)
BCI/DRJ

ERM includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

Escalation
BCI/DRJ

The process by which event related information is communicated upwards through an organization's established chain of command.

Essential Functions
FCD 1

The critical activities performed by organizations, especially after a disruption of normal activities.

Essential Services
BCI/DRJ

Infrastructure services without which a building or area would be considered disabled and unable to provide normal operating services; typically includes utilities (water, gas, electricity, telecommunications), and may also include standby power systems or environmental control systems.

Evacuation
ASIS

Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas. [ASIS International Business Continuity Guideline: 2005].

Event
ISO 31000

Occurrence or change of a particular set of circumstances.

Executive / Management Succession Plan
BCI/DRJ

A predetermined plan for ensuring the continuity of authority, decision making, and communication in the event that key members of executive management unexpectedly become incapacitated.

Exercise
NFPA 1600

Activity in which the entity's plan(s) is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result when put into effect.

Types of Exercises

Desk Top Exercise (BCI/DRJ) Technique for rehearsing emergency teams in which participants review and discuss the actions they would take according to their plans, but do not perform any of these actions; can be conducted with a single team, or multiple teams, typically under the guidance of exercise facilitators.

Call Tree Test (BCI/DRJ) A test designed to validate the currency of contact lists and the processes by which they are maintained.

Disaster Recovery Exercise (FFIEC) A test of an institution's disaster recovery or BCP.

Full-Scale Exercise (DRI) A full-scale exercise is a multi-agency, multi-jurisdictional, multidiscipline exercise involving functional (e.g., joint field office, emergency operations centers) and "boots on the ground" response (e.g., continuity staff relocating to their alternate sites to conduct scenario driven essential functions).

Functional Exercise (DRI) A functional exercise examines and/or validates the coordination, command, and control between various multi-agency coordination centers (e.g., emergency operations centers, joint field office). A functional exercise does not involve any "boots on the ground" (i.e., first responders or emergency officials responding to an incident in real time).

Life Safety (DRI) A functional or discussion-based exercise to familiarize staff with policies and procedures that provide its occupants a reasonable level of safety during fires and other emergencies. Examples of life safety exercises include evacuation drills, identification shelter-in-place locations, and active shooter training.

Notification (DRI) A functional exercise that implements a plan's stakeholder notification process of plan activation.

Plan Walkthrough (DRI) A discussion-based training exercise to review and discuss each portion of a resilience plan to familiarize key stakeholders of the plan's scope, contents, policies, and procedures.

Tabletop or Table Top Exercise (NIST SP800-84) A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. Note: This may also be called a "Scenario Based Tabletop."

Scenario Based Tabletop (see note above)

Exercise Plan
BCI/DRJ

A plan designed to periodically evaluate tasks, teams, and procedures that are documented in business continuity plans to ensure the plan's viability. This can include all or part of the BC plan, but should include mission critical components.

F

Facility
BCI/DRJ

Plant, machinery, equipment, property, buildings, vehicles, information systems, transportation facilities, and other items of infrastructure or plant and related systems that have a distinct and quantifiable function or service. BCI Editor's Note: Also see Infrastructure.

Failover
CNSSI-4009

The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

Failure
ITIL

Loss of ability to operate to specification, or to deliver the required output. The term failure may be used when referring to IT services, processes, activities, configuration items etc. A failure often causes an incident.

First Responder
BCI/DRJ

A member of an emergency service who is first on the scene at a disruptive incident. This would normally be police, fire or ambulance personnel.

Function
ITIL

A team or group of people and the tools they use to carry out one or more processes or activities - for example, the service desk. The term function also has two other meanings: An intended purpose of a configuration item, person, team, process, or IT service. For example, one function of an email service may be to store and forward outgoing mails, one function of a business process may be to dispatch goods to customers; to perform the intended purpose correctly, the computer is "functioning ".

G

Gap Analysis
FFIEC

A comparison that identifies the difference between actual and desired outcomes.

Geographic Dispersion
FCD 1

The distribution of personnel, functions, facilities, and other resources in physically different locations from one another.

Governance
ITIL

Ensuring that policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

Governance, Risk and Compliance (GRC)
BCI/DRJ

GRC is the umbrella term covering an organization's approach across these three areas. Being closely related concerns, governance, risk and compliance activities are increasingly being integrated and aligned to some extent in order to avoid conflicts, wasteful overlaps and gaps. While interpreted differently in various organizations, GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations.

H

Hacker
CNSSI-4009
Unauthorized user who attempts to or gains access to an information system.

Hazard
UNDRR
A dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage. UNDRR Editor's Note: The hazards of concern to disaster risk reduction as stated in footnote 3 of the Hyogo Framework are "… hazards of natural origin and related environmental and technological hazards and risks." Such hazards arise from a variety of geological, meteorological, hydrological, oceanic, biological, and technological sources, sometimes acting in combination. In technical settings, hazards are described quantitatively by the likely frequency of occurrence of different intensities for different areas, as determined from historical data or scientific analysis.

High Availability
ITIL
An approach or design that minimizes or hides the effects of configuration item failure on the users of an IT service. High availability solutions are designed to achieve an agreed level of availability and make use of techniques such as fault tolerance, resilience and fast recovery to reduce the number of incidents, and the impact of incidents.

Hot Site
BCI/DRJ
An alternate facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems.

Human Threats
BCI/DRJ
Possible disruptions in operations resulting from human actions as identified during the risk assessment. (i.e. disgruntled employee, terrorism, blackmail, job actions, riots, etc.)

I

Impact
BCI/DRJ

The effect, acceptable or unacceptable, of an event on an organization. The types of business impact are usually described as financial and non-financial and are further divided into specific types of impact.

Impact Analysis
ASIS

Process of analyzing all operational functions and the effect that an operational interruption might have upon them. ASIS Editor's Note: Impact analysis includes business impact analysis – the identification of critical business assets, functions, processes, and resources as well as an evaluation of the potential damage or loss that may be caused to the organization resulting from a disruption (or a change in the business or operating environment). Impact analysis identifies:
a. how the loss or damage will manifest itself
b. how that degree for potential escalation of damage or loss with time following an incident;
c. the minimum services and resources (human, physical, and financial) needed to enable business processes to continue to operate at a minimum acceptable level; and
d. the timeframe and extent within which activities, functions, and services of the organization should be recovered.

Incident
NFPA 1600

An event that has the potential to cause interruption, disruption, loss, emergency, crisis, disaster, or catastrophe.

Incident Command System
BCI/DRJ

Combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure with responsibility for the command, control, and coordination of assigned resources to effectively direct and control the response and recovery to an incident. The flexible design of the ICS allows its span of control to expand or contract as the scope of the situation changes.

Incident Management
BCI/DRJ

The process by which an organization responds to and controls an incident using emergency response procedures or plans.

Incident Management Plan (IMP)
BCI/DRJ

A clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process.

Incident Management System (IMS)
NFPA 1600

The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents.

Incident Management Team
BCI/DRJ

A group of individuals responsible for developing and implementing a comprehensive plan for responding to a disruptive incident. The team consists of a core group of decision-makers trained in incident management and prepared to respond to any situation.

Incident Manager
BCI/DRJ

Commands the local Emergency Operations Center (EOC) reporting up to senior management on the recovery progress. Has the authority to invoke the recovery plan.

Incident Response
BCI/DRJ

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

Incident Response Plan
NIST SP800-34

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT systems(s).

Information Technology (IT)
ITIL

The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, applications and other software. The information may include business data, voice, images, video, etc. Information technology is often used to support business processes through IT services.

Insurance
BCI/DRJ

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.

Type of Insurance

Business Interruption Insurance (BCI/DRJ) Business Interruption (BI) insurance coverage is a term used widely within the insurance industry, relating to the requirement for calculation of adequate insurance, covering financial loss due to temporary business cessation.

DRI International

Contingent Business Interruption Insurance - A form of business income insurance covering an insured against loss of income and continuing a major supplier, a major customer, or a major location where the insured is a satellite and will lose business if the major shuts down, or (for sales representatives) a manufacturing supplier.

DRI International

Extra Expense Insurance - Insurance covering the additional cost to maintain operations or get back in operation more quickly, following property loss; it can be written alone or in conjunction with business income insurance.

Interagency Agreement (IAA)
FCD 1

A written agreement entered into between two Federal agencies, or major organizational units within an agency, which specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other (the requesting agency).

Interdependencies
FFIEC

Where two or more departments, processes, functions, and/or third parties support one another in some fashion.

Internal Audit
ISO 22301

Audit conducted by, or on behalf of, the organization itself for management review and other internal purposes, and which might form the basis for an organization's self-declaration of conformity.

IT Service Continuity Management (ITSCM)
ITIL

The process responsible for managing risks that could seriously impact IT services. ITSCM ensures that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services. ITSCM should be designed to support business continuity management.

J

Just-in-Time (JIT)
BCI/DRJ

System whereby dependencies for critical business processes are provided exactly when required, without requiring intermediate inventory.

L

Likelihood
BCI

Chance of something happening, whether defined, measured or estimated objectively or subjectively. It can use general descriptors (such as rare, unlikely, likely, almost certain), frequencies or mathematical probabilities. It can be expressed qualitatively or quantitatively. BCI Editor's Note: The vagueness of this term makes its use in BCM of very limited value.

Loss
BCI/DRJ

Unrecoverable resources that are redirected or removed as a result of a business continuity event. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.

M

Malicious Code (Malware)
NIST SP 800-83

A program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Types of Malware
SANS Institute

Ransomware - A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.

CNSSI-4009

Spyware - Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

CNSSI-4009

Virus - A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

NIST SP 800-47

Worm - A computer program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Managed Services
ITIL

A perspective on IT services which emphasizes the fact that they are managed. The term managed services is also used as a synonym for outsourced IT services.

Management System
ISO 22301

Set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives. ISO Editor's Note: 1) A management system can address a single discipline or several disciplines. 2) The system elements include the organization's structure, roles and responsibilities, planning, operation, etc. 3) The scope of a management system can include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

Manual procedures
BCI/DRJ

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 fallback to manual alternatives lessens. However, temporary measures and methods of working can help mitigate the impact of the event for a short period.

Manual Workaround
ITIL

A workaround that requires manual intervention. Manual workaround is also used as the name of a recovery option in which the business process operates without the use of IT services. This is a temporary measure and is usually combined with another recovery option.

Maximum Tolerable Downtime (MTD)
NIST SP 800-34

The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission.

Metric
ITIL

Something that is measured and reported to help manage a process, IT service or activity.

Mission Essential Functions (MEFs)
FCD 1

The limited set of agency-level Government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities.

Mission Statement
ITIL

A short but complete description of the overall purpose and intentions of that organization. It states what is to be achieved but not how this should be done.

Mitigation
NFPA 1600

Activities taken to reduce the impacts from hazards.

Mobilization
BCI/DRJ

The activation of the recovery organization in response to a disaster declaration.

Mutual Aid
AS/NZS 5050

Formalized and documented reciprocal arrangements between two or more organizations providing for unilateral, bilateral or multilateral assistance in specified circumstances.

Mutual Aid Agreement
ASIS

Pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement. [ISO/PAS 22399 2007]

N

Natural Hazard
UNDRR

Natural process or phenomenon that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage. UNDRR Editor's Note: Natural hazards are a sub-set of all hazards. The term is used to describe actual hazard events as well as the latent hazard conditions that may give rise to future events. Natural hazard events can be characterized by their magnitude or intensity, speed of onset, duration, and area of extent. For example, earthquakes have short durations and usually affect a relatively small region, whereas droughts are slow to develop and fade away and often affect large regions. In some cases hazards may be coupled, as in the flood caused by a hurricane or the tsunami that is created by an earthquake.

O

Offsite Location
BCI/DRJ

A site at a safe distance from the primary site where critical data (computerized or paper) and/or equipment is stored from where it can be recovered and used at the time of a disruptive incident if original data, material or equipment is lost or unavailable.

Off-Site Storage
BCI/DRJ

Any place physically located a significant distance away from the primary site, where duplicated and vital records (hard copy or electronic and/or equipment) may be stored for use during recovery.

Operational
ITIL

The lowest of three levels of Planning and delivery (Strategic, Tactical, Operational). Operational Activities include the day-to-day or short-term Planning or delivery of a Business Process or IT Service Management Process. The term Operational is also a synonym for Live.

Organization Head
FCD 1

The highest-ranking official of an organization, or a successor or designee who has been selected by that official in orders of succession.

Outage
DRI

Period of time after disruption that a service, system, process or business function is expected to be unusable or inaccessible.

Outsourcing
BCI/DRJ

The transfer of business functions to an independent (internal and/or external) third party supplier.

P

Pandemic
FFIEC

An epidemic or infectious disease that can have a worldwide impact.

Plan Maintenance
BCI/DRJ

The management process of keeping an organization's BCM competence and capability up-to-date, fit-for-purpose and effective.

Preparedness
BCI/DRJ

Activities implemented prior to an incident that may be used to support and enhance mitigation of, response to, and recovery from disruptions.

Preventative Measures
BCI/DRJ

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

Prevention
ASIS

Measures that enable an organization to avoid, preclude, or limit the impact of a disruption. [ISO/PAS 22399 2007]

Primary Operating Facility
FCD 1

The facility where an organization's leadership and staff operate on a day-to-day basis.

Priority
ITIL

A category used to identify the relative importance of an incident, problem or change. Priority is based on impact and urgency, and is used to identify required times for actions to be taken. For example, the SLA may state that priority incidents must be resolved within 12 hours.

Program
FCD 1

A group of related initiatives managed in a coordinated way, so as to obtain a level of control and benefits that would not be possible from the individual management of the initiatives. Programs may include elements of related work outside the scope of the discrete initiatives in the program.

R

Readiness
BCI/DRJ

Activities implemented prior to an incident that may be used to support and enhance mitigation of, response to, and recovery from disruptions. It is also often called preparedness.

Reciprocal Agreement
BCI/DRJ

Agreement between two organizations (or two internal business groups) similar equipment/environment that allows each one to recover at the other's location.

Reconstitution
FCD 1

The process by which surviving and/or replacement organization personnel resume normal operations.

Recovery
NFPA 1600

Activities and programs designed to return conditions to a level that is acceptable to the entity.

Recovery Point Capability
BCI/DRJ

The point in time to which data was restored and/or systems were recovered (at the designated recovery/alternate location) after an outage or during a disaster recovery exercise.

Recovery Point Objective (RPO)
ISO 22301

Point to which information used by an activity must be restored to enable the activity to operate on resumption. ISO Editor's Note: Can also be referred to as "maximum data loss".

Recovery Time Capability
BCI/DRJ

The demonstrated amount of time in which systems, applications and/or functions have been recovered, during an exercise or actual event, at the designated recovery/alternate location (Physical or virtual).

Recovery Procedures
CNSSI-4009

Actions necessary to restore data files of an information system and computational capability after a system failure.

Recovery Strategies
Singapore MAS

Defined, management-approved and tested course of action in response to operational disruptions.

Recovery Time Estimate (RTE)
AS/NZS 5050

Estimated period of time required to restore a particular level of functionality after taking into account any uncertainties.

Recovery Time Objective (RTO)
ASIS

Time goal for the restoration and recovery of functions or resources based on the acceptable down time and acceptable level of performance in case of a disruption of operations.

Recovery Timeline
BCI/DRJ

The sequence of recovery activities, or critical path, which must be followed to resume an acceptable level of operation following a business interruption. The timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.

Redundancy
FCD 1

The state of having duplicate capabilities, such as systems, equipment, or resources.

Regulation
ISACA

Rules or laws defined and enforced by an authority to regulate conduct.

Remediation
CNSSI-4009

The act of mitigating a vulnerability or a threat.

Residual Risk
BCI/DRJ

The level of risk remaining after all cost-effective actions have been taken to lessen the impact, probability and consequences of a specific risk or group of risks, subject to an organization's risk appetite.

Resilience
FCD 1

The ability to prepare for and adapt to changing conditions and recover rapidly from operational disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Resource Management
NFPA 1600

A system for identifying available resources to enable timely access needed to prevent, mitigate, prepare for, respond to, maintain continuity during, or recover from an incident.

Response
UNDRR

1. Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment.
2. The provision of emergency services and public assistance during or immediately after a disaster in order to save lives, reduce health impacts, ensure public safety and meet the basic subsistence needs of the people affected. UNDRR Editor's Note: Disaster response is predominantly focused on immediate and short-term needs and is sometimes called "disaster relief". The division between this response stage and the subsequent recovery stage is not clear-cut. Some response actions, such as the supply of temporary housing and water supplies, may extend well into the recovery stage.

Response Plan
ASIS

Documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident.

Response Time
ITIL

A measure of the time taken to complete an operation or transaction. (ITIL)

Restoration
BCI/DRJ

Process of planning for and/or implementing procedures for the repair of hardware, relocation of the primary site and its contents, and returning to normal operations at the permanent operational location.

Resumption
BCI/DRJ

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.

Return on Investment (ROI)
ITIL

A measurement of the expected benefit of an investment. In the simplest sense it is the net profit of an investment divided by the net worth of the assets invested.

Risk
ITIL

A possible event that could cause harm or loss, or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.

Types of Risk

Business Risk (BCI/DRJ) Risk that internal and external factors, such as inability to provide a service or product, or a fall in demand for an organization's products or services will result in an unexpected loss.

Disaster Risk (UNDRR) The potential disaster losses, in lives, health status, livelihoods, assets and services, which could occur to a particular community or a society over some specified future time period. Comment: The definition of disaster risk reflects the concept of disasters as the outcome of continuously present conditions of risk. Disaster risk comprises different types of potential losses which are often difficult to quantify. Nevertheless, with knowledge of the prevailing hazards and the patterns of population and socio-economic development, disaster risks can be assessed and mapped, in broad terms at least.

Operational Risk (BCI/DRJ) The risk of loss resulting from inadequate or failed procedures and controls. This includes loss from events related to technology and infrastructure, failure, business interruptions, staff related problems, and from external events such as regulatory changes.

Risk Acceptance
BCI/DRJ

A management decision to take no action to mitigate the impact of a particular risk.

Risk Analysis
BCI/DRJ

The quantification of threats to an organization and the probability of them being realized.

Risk Appetite
BCI/DRJ

Total amount of risk that an organization is prepared to accept, tolerate, or be exposed to at any point in time.

Risk Assessment / Analysis
BCI/DRJ

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 Avoidance
BCI/DRJ

An informed decision to not become involved in or to withdraw from a risk situation.

Risk Categories
BCI/DRJ

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 Criteria
ISO 31000

Terms of reference against which the significance of a risk is evaluated.

Risk Evaluation
AS/NZS 5050

Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk Management
UAE NCEMA

Structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analyzing, evaluating, controlling and responding to risk.

Risk Mitigation
CNSSI-4009

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Risk Reduction
BCI/DRJ

A selective application of appropriate techniques and management principles to reduce either probability of an occurrence or its impact, or both.

Risk Tolerance
ASIS

Organization's readiness to bear the risk after risk treatments in order to achieve its objectives [ISO/IEC Guide 73]. ASIS Editor's Note: Risk tolerance can be limited by legal or regulatory requirements.

Risk Transfer
BCI/DRJ

A common technique used by risk managers to address or mitigate potential exposures of the organization. A series of techniques describing the various means of addressing risk through insurance and similar products.

Root Cause
ITIL

The underlying or original cause of an incident or problem.

Root Cause Analysis (RCA)
ITIL

An activity that identifies the root cause of an incident or problem. RCA typically concentrates on IT infrastructure failures.

S

Salvage
BCI/DRJ

The recovery of personal effects, documentation, office, and computer equipment.

Scenario
BCI/DRJ

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. DRJ Editor's Note: Scenarios are neither predictions nor forecasts.

Scope
ITIL

The boundary, or extent, to which a process, procedure, certification, contract etc. applies.

Security
CNSSI-4009

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Controls
NIST SP 800-34

The management, operational, and technical controls (i.e., FIPS 199) safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Service Level Agreement (SLA)
BCI/DRJ

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.

Service Provider
ITIL

An organization supplying services to one or more internal customers or external customers.

Single Point of Failure (SPOF)
ITIL

Any Configuration Item that can cause an Incident when it fails, and for which a Countermeasure has not been implemented. A SPOF may be a person, or a step in a Process or Activity, as well as a Component of the IT Infrastructure. See Failure.

Situational Awareness
CNSSI-4009

Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.

Stakeholder
BCI/DRJ

Individual or group having an interest in the performance or success of an organization e.g., customers, partners, employees, shareholders, owners, the local community, first responders, government, and regulators.

Standard
NFPA1600/ITIL

1. A document, the main text of which contains only mandatory provisions using the word "shall" to indicate requirements and which is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Non-mandatory provisions shall be located in an appendix or annex, footnote, or fine-print note and are not to be considered a part of the requirements of a standard. (NFPA 1600)
2. A mandatory requirement. Examples include ISOIIEC 20000 (an international standard), an internal security standard for Unix configuration, or a government standard for how financial records should be maintained. The term standard is also used to refer to a code of practice or specification published by a standards organization such as ISO or BSI. (ITIL)

Strategic
ITIL

(Service Strategy) The highest of three levels of Planning and delivery (Strategic, Tactical, Operational). Strategic Activities include Objective setting and long term Planning to achieve the overall Vision.

Succession
FCD 1

A formal, sequential assumption of a position's authorities and responsibilities, to the extent not otherwise limited by law, by the holder of another specified position as identified in statute, executive order, or other presidential directive, or by relevant D/A policy, order, or regulation if there is no applicable executive order, other presidential directive, or statute in the event of a vacancy in office or a position holder dies, resigns, or is otherwise unable to perform the functions and duties of that pertinent position.

Supplier
ITIL

A third party responsible for supplying goods or services.

Supply Chain
BCI/DRJ

The linked processes that begins with the acquisition of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include suppliers, vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, and other entities that lead to the end user.

T

Tactical
ITIL
The middle of three levels of planning and delivery (strategic, tactical, operational). Tactical activities include the medium-term plans required to achieve specific objectives, typically over a period of weeks to months.

Technological Hazard
UNDRR
A hazard originating from technological or industrial conditions, including accidents, dangerous procedures, infrastructure failures or specific human activities, that may cause loss of life, injury, illness or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage. UNDRR Editor's Note: Examples of technological hazards include industrial pollution, nuclear radiation, toxic wastes, dam failures, transport accidents, factory explosions, fires, and chemical spills. Technological hazards also may arise directly as a result of the impacts of a natural hazard event.

Telework Site
FCD 1
An approved worksite where an employee performs his or her duties other than the location from which the employee would otherwise work.

Test
BCI/DRJ
A pass/fail evaluation of infrastructure (example-computers, cabling, devices, hardware) and\or physical plant infrastructure (example- building systems, generators, utilities) to demonstrate the anticipated operation of the components and system. Tests are often performed as part of normal operations and maintenance. Tests are often included within exercises.

Test Plan
FFIEC
A document that is based on the institution's test scope and objectives and includes various testing methods.

Testing
ASIS
Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties, and to reveal weaknesses in the preparedness and response/continuity/recovery plans. [ASIS International Business Continuity Guideline 2005]

Threat
ASIS
Potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community.

Threat Assessment
CNSSI-4009
Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Threat Monitoring
CNSSI-4009

Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.

Training
BCI/DRJ

Training is more formal than awareness. It aims to build knowledge and skills to enhance competency in job performance. Whereas awareness is generally targeted at all staff, training is directed at staff with specific duties and responsibilities. For example, staff involved in the recovery should be equipped and adequately prepared with the necessary knowledge and skill to undertake recovery activities. Training forms part of the awareness, training and education learning continuum.

Trigger
BCI/DRJ

An event that causes a system to initiate a response.

U

Unified Command
NIMS

An [Incident Command System] ICS application used when more than one agency has incident jurisdiction or when incidents cross political jurisdictions.

V

Vital Records
BCI/DRJ

Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the legal and financial rights of that organization and of the individuals directly affected by its activities.

Similar Terms

Essential Records (FCD 1) Information systems and applications, electronic and hardcopy documents, references, and records needed to support essential functions during a continuity event. The two basic categories of essential records are emergency operating records and rights and interest records. Emergency operating records are essential to the continued functioning or reconstitution of an organization. Rights and interest records are critical to carrying out an organization's essential legal and financial functions and vital to the protection of the legal and financial rights of individuals who are directly affected by that organization's activities. The term "vital records" refers to a specific sub-set of essential records relating to birth, death, and marriage documents.

Legal and Financial Rights Records (FCD 1) Vital records essential to protect the legal and financial rights of the government and the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as ‘‘rights-and-interests’’ records.

Vulnerability
BCI/DRJ

The degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of a risk, event or other occurrence.

Vulnerability Assessment
CNSSI-4009

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

W

Walk-Through
ISACA

A thorough demonstration or explanation that details each step of a process.

Wallet Card
FFIEC

Portable information cards that provide emergency communications information for customers and employees.

Warm Site
BCI/DRJ

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

Cited References

AS NZS 5050 (2010)	**Australia AS NZS 5050**	Australia AS/NZS 5050:2010 explains how to apply AS/NZS IS 31000:2009 [Risk management -- Principles and guidelines] to disruption related risks. It includes detailed guidance particular to the features of these risks and to the risk management framework through which they are managed.
	Link (as of 06/2018):	https://www.standards.org.au/standards-catalogue/sa-snz/publicsafety/ob-007/as-slash-nzs--5050-2010
ASIS (2009)	**ASIS International**	Founded in 1955, ASIS International is a global community of security practitioners, each of whom has a role in the protection of assets - people, property, and/or information. The glossary terms used are contained in Security and Resilience in Organizations and Their Supply Chains (ORM.1)[ASIS_SPC.1-2009_Item_No._1842]
	Link (as of 06/2018):	https://www.asisonline.org/publications--resources/standards--guidelines/
BCI/DRJ (2018)	**Business Continuity Institute / Disaster Recovery Journal**	These two international trade publications combined their glossaries into a single glossary. While some terms in their glossary may have different definitions, all references in the DRI Glossary for Resilience indicate a joint BCI/DRJ definition
	Link (as of 06/2018):	https://drj.com/resources/drj-glossary-of-business-continuity-terms/
CNSSI-4009 (2015)	**Committee on National Security Systems (CNSS) Glossary**	This instruction applies to all U.S. Government Departments, Agencies, Bureaus and Offices; supporting contractors and agents; that collect, generate process, store, display, transmit or receive classified or controlled unclassified information or that operate, use, or connect to National Security Systems (NSS), as defined herein.
	Link (as of 06/2018):	https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

DRI (2018)	**Disaster Recovery Institute International**	Disaster Recovery Institute (DRI) International first published its Glossary for Resiliency in 2014. In its second major release, DRI International maintained several terms from the first version that were no longer supported by reference documents. The Committee determined these terms to be important and relevant to the resilience community, and now maintain these terms as DRI International terms.
	Link (as of 06/2018):	https://drii.org/resources/viewglossary
FCD-1 (2017)	**U.S. Department of Homeland Security - Federal Emergency Management Agency Federal Continuity Directive 1**	Federal Continuity Directive 1 (FCD-1) implements Federal requirements for establishing the framework, requirements, and processes to support the development of Federal departments and agencies continuity programs and by specifying and defining elements of a continuity plan.
	Link (as of 06/2018):	https://www.gpo.gov/docs/default-source/accessibility-privacy-coop-files/January2017FCD1-2.pdf
FFIEC (2015)	**Federal Financial Institutions Examination Council**	The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions.
	Link (as of 06/2018):	https://www.ffiec.gov/
HIPAA (2001)	**Health Insurance Portability and Accountability Act of 1996**	HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by Congress in 1996. HIPAA does the following: Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs; Reduces health care fraud and abuse; Mandates industry-wide standards for health care information on electronic billing and other processes; and Requires the protection and confidential handling of protected health information. HIPAA no longer provides an official Glossary. Several other healthcare organizations have compiled definitions from HIPAA. One such compilation is from the West Virginia Department of Health and Human Resources.

	Links (as of 08/2023):	http://www.wvdhhr.org/hipaa/glossary_final.asp https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf
ISACA (2018)	**ISACA Glossary**	ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide. The COBIT framework and the CISA, CISM, CGEIT and CRISC certifications are ISACA brands respected and used by these professionals for the benefit of their enterprises.
	Link (as of 06/2018):	https://www.isaca.org/Pages/Glossary.aspx
ISO 22301 (2012)	**International Standard ISO 22301 - Societal security - Business continuity management systems – Requirements**	ISO 22301 is an International Standard for business continuity management, that specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
	Link (as of 08/2023):	https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1bsmknus1_306856.pdf
ISO 31000 (2009)	**International Standard ISO 31000 - Risk management - Principles and guidelines**	This International Standard provides principles and generic guidelines on risk management. This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.
	Link (as of 08/2023):	https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf
ITIL (2011)	**ITIL Practices**	ITIL (formerly an acronym for Information Technology Infrastructure Library) is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.
	Link (as of 06/2018):	https://www.alaska.edu/files/oit/ITIL_2011_English_glossary_v1.0.pdf

NFPA 1600 (2013)	**National Fire Protection Association Publication 1600 - Standard on Disaster/ Emergency Management and Business Continuity Programs**	The NFPA Standards Council established the Disaster Management Committee in January 1991. The committee was given the responsibility for developing documents relating to preparedness for, response to, and recovery from disasters resulting from natural, human, or technological events. The first document that the committee focused on was NFPA 1600, Recommended Practice for Disaster Management
	Link (as of 06/2018):	https://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf
NIMS (2008)	**National Incident Management System**	NIMS uses the Federal Emergency Management Administration (FEMA) Incident Command System (ICS) Training Glossary
	Link (as of 06/2018):	https://training.fema.gov/emiweb/is/icsresource/assets/icsglossary.pdf
NIST SP 800-34 (2010)	**National Institute on Standards and Technology (NIST) Special Publication (SP) 800-34 Revision 1 - Contingency Planning Guide for Federal Information Systems**	NIST SP 800-34 Rev 1 assists organizations in understanding the purpose, process, and format of information system contingency planning development through practical, real-world guidelines. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle. This document provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities.
	Link (as of 06/2018):	https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final
SANS (2020)	SANS Institute	The SANS Institute was established in 1989 as a cooperative research and education organization. SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.
	Link (as of 07/2020)	https://www.sans.org/security-resources/glossary-of-terms/

Singapore MAS (2004)	**Monetary Authority of Singapore**	As Singapore's central bank, the Monetary Authority of Singapore (MAS) promotes sustained, non-inflationary economic growth through appropriate monetary policy formulation and close macroeconomic surveillance of emerging trends and potential vulnerabilities. It manages Singapore's exchange rate, foreign reserves and liquidity in the banking sector. MAS is also an integrated supervisor overseeing all financial institutions in Singapore -- banks, insurers, capital market intermediaries, financial advisors, and the stock exchange.
	Link (as of 06/2018):	http://www.mas.gov.sg/
UAE NCEMA (2011)	**United Arab Emirates National Emergency Crisis and Disasters Management Authority**	The mission of NCEMA is to enhance the UAE's capabilities in managing emergency, crisis and disaster by: setting the requirements of business continuity, enabling quick recovery through joint planning, and coordinating communication both at the national and local level.
	Link (as of 06/2018):	https://www.ncema.gov.ae/en/home.aspx
UNDRR Glossary (2016)	**United Nations Office for Disaster Risk Reduction (UNDRR) Terminology**	By its resolution 69/284 of 3 June 2015, the General Assembly established an open-ended intergovernmental expert working group comprising experts nominated by States and supported by the United Nations Office for Disaster Risk Reduction, with the involvement of relevant stakeholders, for the development of a set of possible indicators to measure global progress in the implementation of the Sendai Framework for Disaster Risk Reduction 2015-2030, coherent with the work of the Inter-Agency and Expert Group on Sustainable Development Goal Indicators.
	Link (as of 06/2018):	https://www.undrr.org/terminology

Glossary Changes

The following are changes to terms and references made from the 2014 version of the DRI Glossary for Resiliency.

1. Overall Changes to DRI Glossary

a. Name changed to the **DRI Glossary for Resilience**
b. **DRI International (DRI)** added as a reference standard. The DRI Glossary Committee determined some terms from old or removed standards were still the most appropriate definitions for those terms. The Committee adopted these definitions as DRI definitions.
c. Several new terms added from DRI courses with input from the DRI community in the form of a survey at DRI2020.
d. Changes and updates made to correspond to the release of the 2022 DRI International Professional Practices, and new/updated DRI courses.

2. Terms Added

a. **Contingent Business Interruption Insurance** as a Type of Insurance, using the old Adjusters International glossary definition, which will become a DRI definition
b. **Continuity Manager** added with new definition from FCD-1
c. **Continuity Plan**, a new term in FCD-1, is added as a similar term to **Business Continuity Plan**
d. **Critical Asset**, a new term in FCD-1, is added as a similar term to **Critical Infrastructure**
e. **Cyber Resilience** added with definition from DRI
f. **Data Mirroring** added with definition from BCI/DRJ
g. **Devolution Emergency Response Group (DERG)** added with definition from FCD-1
h. **Distribution Denial of Service (DDoS)** added with definition from CNSSI-4009
i. **Emergency Plan**, a new term in FCD-1, is added as a similar term to **Emergency Response Plan**
j. **Emergency Relocation Group (ERG)** added with definition from FCD-1
k. **Essential Records**, a new term in FCD-1, is added as a similar term to **Vital Records**
l. **Extra Expense Insurance** was added as a type of Insurance, using the old Adjusters International glossary definition, which will become a DRI definition
m. **Full Scale Exercise**, a term from FCD-1, is moved as a similar term to **Exercise**, using the old FCD-1 definition, which will become a DRI definition
n. **Functional Exercise**, a term from FCD-1, is moved as a similar term to **Exercise**, using the old FCD-1 definition, which becomes a DRI definition
o. **Geographic Dispersion** added with new definition from FCD-1
p. **Hacker** added with definition from CNSSI-4009
q. **Incident Management System** added with definition from NFPA 1600
r. **Interagency Agreement (IAA)** added with new definition from FCD-1

s. **Legal and Financial Rights Records**, a new term in FCD-1, is added as a similar term to **Vital Records**
t. **Life Safety** added under ***Types of Exercises*** with definition from DRI
u. **Malicious Code (Malware)** added with definition from NIST SP 800-83
v. **Notification** added under ***Types of Exercises*** with definition from DRI
w. **Operational** is added using ITIL definition to correspond to **Tactical**
x. **Organization Head** added with new definition from FCD-1
y. **Plan Walkthrough** added under ***Types of Exercises*** with definition from DRI
z. **Primary Operating Facility** added with new definition from FCD-1
aa. **Ransomware**, with definition from SANS Institute, was added as a type of **Malicious Code**
bb. **Recovery Point Capability** added with definition from BCI/DRJ
cc. **Recovery Time Capability** added with definition from BCI/DRJ
dd. **Regulation** added with definition from ISACA
ee. **Scenario Based Tabletop** added under ***Types of Exercises***
ff. **Spyware,** with definition from CNSSI-4009, was added as a type of **Malicious Code**
gg. **Strategic** is added using ITIL definition to correspond to **Tactical**
hh. **Succession** added with new definition from FCD-1
ii. **Telework Site** added with new definition from FCD-1
jj. **Unified Command** added with definition from NIMS
kk. **Virus,** with definition from CNSSI-4009, was added as a type of **Malicious Code**
ll. **Worm**, with definition from NIST SP 800-47, was added as a type of **Malicious Code**

3. Terms Changed

a. **Alternate Facilities** is changed to **Alternate Locations** and an updated FCD-1 definition incorporated and is merged as a similar term under **Alternate Site;** updated to include a note that Alternate Facility and Alternate Location are similar terms.
b. **Application** reference changed to **DRI**, maintaining old term from CNSSI-4009 (2009)
c. **Audit** definition changed to **ISACA** definition, replacing old definition from BS-25999
d. **Audit Trail** updated with new **CNSSI-4009 (2015)** definition, retaining its reference
e. **Authentication** reference changed to **DRI**, maintaining old term from CNSSI-4009 (2009)
f. **Business Unit** definition changed to **BCI/DRJ** definition, replacing old definition from Singapore SS540.
g. **Cloud Computing** updated with new **CNSSI-4009 (2015)** definition, retaining its reference
h. **Continuity of Operations Plan (COOP)** is changed to **Continuity of Operations (COOP) Plan**, maintaining definition and reference from **NIST SP800-34**
i. **Cyber Attack** definition changed to **FFIEC** definition, replacing old definition from CNSSI- 4009 (2009)
j. **Cyber Resilience** updated with new **DRI** definition, retaining its reference
k. Cybersecurity, with a definition from ISACA, was removed as a type of Security in 2020. Cybersecurity was then added as a term with a definition from CNSSI-4009
l. **Data Integrity** definition changed to **FFIEC** definition, replacing old definition from CNSSI- 4009 (2009)

m. **Devolution** definition is updated using new **FCD-1 (2017)** definition, retaining its reference
n. **Internal Audit** definition changed to **ISO 22301** definition, replacing old definition from BS- 25999
o. **Occupant Emergency Plan (OEP)** uses new definition from **FCD-1 (2017)** and moved as a similar term to **Emergency Response Plan**, retaining its reference
p. **Outage** becomes a **DRI** definition, maintaining its old ECB definition
q. **Reconstitution** definition is updated using new **FCD-1 (2017)** definition, retaining its reference
r. **Redundancy** definition is updated using new **FCD-1 (2017)** definition, retaining its reference
s. **Resilience** definition is updated using new **FCD-1 (2017)** definition, retaining its reference
t. **Table Top** is changed to **Tabletop or Table Top** under **Exercises** with definition changed to NIST SP800-84 definition.
u. **Test** changed to **BCI/DRJ** definition, replacing old definition from ECB
v. **Threat** definition changed to **ASIS** definition, replacing old definition from Singapore SS540
w. **Training** definition changed to **BCI/DRJ** definition, replacing old definition from Singapore SS540
x. **Single Point of Failure (SPOF)** definition changed to **ITIL** definition, replacing old definition from ECB
y. **Situational Awareness** updated with new **CNSSI-4009 (2015)** definition, retaining its reference
z. **Vital Records** definition changed to **BCI/DRJ** definition, replacing old definition from Singapore SS540.
aa. **Walk Through** changed to **ISACA** definition (old definition from ECB removed)

4. Terms Moved

a. **Alternate Facilities** is changed to **Alternate Locations** and an updated FCD-1 definition incorporated and is merged as a similar term under **Alternate Site**
b. **Alternate Work Area** is merged as a similar term under **Alternate Site**
c. **Business Interruption Insurance** is merged as a type of **Insurance**
d. **Business Risk** is merged as a type of **Risk**
e. **Call Tree Test** is merged as a type of **Exercise**
f. **Desktop Exercise** is merged as a type of **Exercise**
g. **Disaster Recovery Exercise** is merged as a type of **Exercise**
h. **Disaster Risk** is merged as a type of **Risk**
i. **Fallback** is merged as a similar term under **Alternate Site**
j. **Occupant Emergency Plan (OEP)** uses the new definition from FCD-1 and moved as a similar term to **Emergency Response Plan**
k. **Operational Risk** is merged as a type of **Risk**
l. **Secondary Site** is merged as a similar term under **Alternate Site**
m. **Table Top Exercise** is merged as a type of **Exercise**
n. **Work Area Recovery** is merged as a similar term under **Alternate Site**

5. Terms Removed

a. **Facilities**, a term removed from FCD-1, has been removed
b. **National Incident Management System**, a term removed from FCD-1, has been removed
c. **National Response Framework**, a term removed from FCD-1, has been removed
d. **Orders of Succession,** a term removed from FCD-1, has been removed

6. Other Changes

a. **ISACA** added as a reference organization
b. **National Incident Management System (NIMS)** added as a reference document
c. **International Standards Organization (ISO)** reference changed to **ISO 31000**
d. **Business Continuity Insights (BCI)** and **Disaster Recovery Journal (DRJ)** combined their glossaries; terms from either reference are now referenced to **BCI/DRJ**
e. **BS-25999** removed as a reference standard
f. **European Central Bank (ECB)** removed as a reference standard
g. **Singapore SS540** removed as a reference standard
h. **FCD-1** definitions updated using new 2017 version of standard
i. **CNSSI-4009** definitions updated using new 2015 version of standard
j. **Incident Response Plan** – It was determined in DRI2018 Nashville to hold on any changes to this term, the definition of which differs from DRI's Professional Practices. Reference to the term has been changed to **NIST SP800-34**, but the definition remains the same. A white paper will be developed to determine the most appropriate definition(s) for this term and for **Incident.**
k. **"You Say Incident, I Say Event**", a white paper on defining the term incident, was developed and published in April 2019
l. **SANS Institute** added as a reference organization
m. **Adjusters International,** added as a reference organization in 2020, was removed in 2023 since they no longer have a glossary; terms that referenced Adjusters International definitions will become DRI definitions.
n. **United Nations Office for Disaster Risk Reduction (UNISDR)** reference organization title updated to **United Nations Office for Disaster Risk Reduction**