www.drii.org | driinfo@drii.org | 866.542.3744

DRI International Glossary for Resilience

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

Maintained by DRI International

Version 3 — February 2026

Legal Disclaimer

The DRI International Glossary Committee

Chair
Andrea Abrams, MBCP

Coordinator
Kathy Acevedo, ABCP

Doniella McKoy, CBCP
Gayle Anders, CBCP
Gayle Mitcham, MBCP
Kelvin Brim, CBCP
Kyle Shinn, ABCP
Lyndon Bird
Michelle Noah, CBCP
Sarah Gucciardo, CBCP
Sheila Abshere, CBCP
Steven Lei, CBCP
Susan Lounsbury, MBCP
Rachael Elliott
Rob Alaniz, MBCP

With thanks to:

Al Berman, MBCP, CCRP, CBCLA – Treasurer DRI International
Michelle Cross, MBCP, CCRP, President and CEO DRI International
Deal Gallup, MBCP, CISM, CHEP, CCRP
Buffy Rojas Leach, Sr. Director Communications, DRI International
Raymond Seid, MBCP, ARMP, CBCLA, CHPCP, CCRP, Sr. Director of Education, DRI International

Note from the Chair

This 2026 edition of the DRI Glossary for Resilience contains the perspective of a remarkable Glossary Committee drawn from the United Kingdom, Canada, and the United States.

The fourteen of us reflect our dynamic industry from coast to coast within the United States and across multiple nations and continents, yet our perspectives reflect more than geographic variation. We are seasoned veterans and emerging influential newcomers; retired fire chiefs and deep subject matter experts in niches such as information technology, banking and finance, and the global entertainment industry.

Our workgroup personally experienced evacuation from fires and floods this year, and, in fact, this glossary was finalized in the midst of catastrophic flooding in the state of Texas not far from the home of one of our committee members. True to the nature of those called to the resilience industry, this group became stronger in the face of challenges and ran towards what we perceived as need for refreshed language for our rapidly evolving profession, springing into action to ensure this Glossary reached your hands. As our world continues to rapidly change, our workgroup seeks to provide resources to guide and shape the conversations you will have while performing your mission-critical work.

On behalf of each of us on the Glossary Committee, heartfelt thank you to Michelle Cross, Al Berman, Ray Seid, and Buffy Rojas Leach for entrusting us with this exciting mission. Special thanks also to Dean C. Gallup, the prior Chair of the Glossary Committee, for blazing an admirable and motivational trail for our workgroup. And especially thanks to every DRI student who has provided thoughts and insights into the vocabulary of our profession. We hope that you will recognize your voice in the pages that follow and we look forward to your future contributions to reflect our dynamic world.

Yours in resilience,

Andrea L Abrams

Andrea Abrams, MBCP
Glossary Committee Chair

About this document

Overall Changes to DRI Glossary

DRI is the source entity for its Glossary terms

This 2026 edition includes new terms drawn from a workgroup representing the United Kingdom, Canada, and the United States

Definitions are harmonized with the 2022 update of the DRI International Professional Practices and new/updated DRI courses

For ease of use, definitions appear in alphabetical order rather than nested within related terms (multi-word terms are alphabetized by their first word)

Feedback welcome

Input and suggestions for improvement are always accepted at driinfo@drii.org.

Quarterly review

The Glossary Committee reviews this document each quarter based on:

- Comments received
- Significant changes to industry standards
- Significant changes to laws and regulations
- Significant changes to regulatory guidance

Version control

- Hard copies cannot be controlled.
- The “Last updated” date on the first page reflects the most recent changes.
- For the current version, visit www.drii.org.

Annual public review

A public review session is held at the DRI conference each year.

Annual revision:

A formal annual revision is published by the fourth month following the DRI conference and retains the document name with a Rev #.

Major release cycle

A major release occurs every four years, is named with the release year, and has no revision number. A major release may include:

- New or changed terms
- Removal of terms
- Reorganized categories or formatting improvements

A

Acceptable Downtime

Maximum amount of time that a system, service, or business function can be unavailable for use without causing significant harm to the entity.

Acceptable Risk

The level of potential damage, harm, or negative impact that an entity is willing to tolerate. There must be a balance of potential risks against desired outcomes. The acceptable risk level will vary based on context, including regulatory requirements, industry. and the entity's own risk appetite.

Account Manager

An account manager in the context of business continuity is a relationship manager with a crucial role responsible for maintaining strong relationships with clients and ensuring their needs are met even during disruptions.

Accreditation

The formal recognition of an entity's processes and systems that meet recognized standards and best practices against a specific standard.

Activation

Activation refers to the process of initiating plans and procedures to manage an entity during a disruption. For an incident management system (IMS), activation establishes communications and coordination between incident command and the emergency operations center (EOC). Plans for activation should include a predefined threshold and process for initiating the response.

Active Monitoring

Proactively monitoring the performance of an application or service that uses automated regular checks to discover the current status. Also, regularly scheduled checks to discover the current status of services or functions.

Alert

A message or notification to attract attention.

All-Hazards

A resilience approach focused on preparing for, responding to, and recovering from an adverse event, regardless of its cause.

Alternate Locations

A temporary workspace fully equipped with critical infrastructure (including equipment, technology, and connectivity) to support operations during recovery. (See also: Alternate Site)

Alternate Routing

The strategy of rerouting critical data and information traffic over a different, pre-established path when the primary path becomes unavailable or congested.

Alternate Site

A prearranged location, separate from the primary facility, designated to support critical functions and resume operations when the primary site is unavailable. (See also: Alternate Locations, Secondary Site, Work Recovery Area)

Alternate Work Area

A temporary workspace with the basic critical infrastructure (including equipment, technology, and connectivity) to support operations during recovery. (See also: Alternate Site)

Application

A software program designed to perform specific tasks or functions for an end user.

Application Management

The process of overseeing the lifecycle of an application (including its deployment, operation, maintenance, updates, and eventual retirement) to ensure business requirements and performance standards are met.

Application Recovery

The process of restoring a software application as well as its associated data, configurations, and dependencies to a functional state following a disruption. Recovery efforts are guided by the application's defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) to ensure timely availability and minimal data loss in support of business operations. (See also: Disaster Recovery)

Architecture

The design and structure of systems, processes, and infrastructure.

Artificial Intelligence (AI)

The simulation of human intelligence processes in machines, allowing them to perform tasks that usually require human intelligence/intervention. An example of uses in business continuity and resilience is datamining of large fields of data (e.g. near misses).

Assessment

Assessment generally refers to the process of evaluating something.

In resilience, specific types of assessments include:

Risk Assessment: The process of identifying threats and hazards to life, property, operations, the environment, information, and entities, as well as the analysis of probabilities, vulnerabilities, and impacts. (See also: Risk Assessment)

Business Impact Analysis (BIA): An analysis that identifies, quantifies, and qualifies the impacts resulting from interruptions or disruptions of an entity's resources. It identifies time-critical functions, recovery priorities, dependencies, and interdependencies, and helps establish Recovery Time Objectives (RTOs). It also assesses how a disruption could affect an entity's operations, reputation, market share, ability to do business, or relationships with key stakeholders. (See also: Business Impact Analysis)

Resource Needs Assessment: Determines the resources needed to maintain operations based on identified hazards and the business impact analysis.

Damage Assessment: A determination of the effects of an incident on people, assets, operations, information, economic characteristics, and/or the environment.

Asset

Anything with value, including tangible value (land, buildings, and equipment), intangible value (intellectual property, goodwill, and reputation), and strategic value (employees, customer lists).

Asset Management

The process of identifying, protecting, and administering resources.

Audit

A systematic and documented evaluation of process against regulations to measure compliance.

Audit Trail

A chronological record of events and actions. (See also: Audit). In business continuity/ resilience the records are related to the recovery process after a disruption.

Auditor

An individual or team that independently assesses the effectiveness and compliance of processes, controls, or systems to assess compliance with standards, measure effectiveness, and identify opportunities for improvement.

Authentication

The process of verifying the identity of a user, device, or system, typically by validating credentials or tokens to confirm the user is who they claim to be before granting access to resources or services.

Authority Having Jurisdiction

An entity, office, or individual within a defined geographic or functional area responsible for enforcing codes, standards, and regulations.

Authorization

The process of defining, granting, and managing access rights or permissions for users, devices, systems, or resources based on established roles, policies, or criteria.

Automated Monitoring

Real-time observation of systems, processes, or external threats (e.g. flooding, fire, or earthquakes). Can alert decision makers to critical events as they occur, as well as streamline analytics (often using AI) to determine abnormal content on systems (e.g. a DDoS attack).

Automatic Call Distribution (ACD)

A telephony system feature that automatically routes incoming calls based on predefined rules (including availability, skill set, or call priority) to ensure efficient response, balanced workload, and continuity of critical communications during disruptions.

Availability

The readiness of systems, resources and services.

Awareness

The knowledge and understanding of a subject or situation.

B

Backup

A process by which data, electronic, or paper-based information is copied and stored separately from the primary data or system. The purpose of backups is to restore information if the primary data is corrupted or destroyed.

Basel Accord (Basel III)

A set of international banking standards issued by the Basel Committee on Banking Supervision that require banks to maintain minimum capital, liquidity, and leverage levels to strengthen resilience and reduce systemic risk.

Benchmark

A recorded baseline measurement or condition used as a reference point for evaluating performance, risk, or compliance over time.

Benchmarking

The practice of comparing processes, systems, or performance metrics against established baseline measurement, standard, or recognized best practice to evaluate effectiveness and identify areas for improvement.

Best Practice

Proven activities, processes, or methods that have standardized and widespread adoption across industry groups, and entities.

Biological Hazard

A biological substance that poses a threat to the health of people, animals, or the environment.

Black Swan

A rare and unpredictable event with extreme consequences that cannot be anticipated using conventional forecasting or probability methods.

Brute Force Attack

A type of hacking incident which uses trial and error to ascertain passwords, login credentials, encryption keys, and access to data.

Business Continuity (BC)

An ongoing process to ensure an entity's ability to maintain critical functions and resume normal operations quickly following a disruption. This includes developing all necessary procedures to mitigate such a situation and the training for personnel to carry them out.

Business Continuity Coordinator

A professional responsible for ensuring an entity has and can execute its business continuity program to ensure that critical business processes will continue during and after a disruption.

Business Continuity Management (BCM)

A holistic management program that provides processes for an entity to maintain its required business operations during a disruption.

Business Continuity Management Lifecycle

A process that is used by an entity to prepare for, respond to, and recover from disruptions.

Business Continuity Management Program

A holistic and continuous process that ensures an entity can maintain necessary business processes and operations during and after a disruption. This includes documented plans and strategies as well as the education to ensure they can be carried out.

Business Continuity Management System (BCMS)

A comprehensive framework that helps entities maintain critical business processes and operations.

Business Continuity Management Team

A group of professionals within an entity responsible for developing, implementing, testing, and maintaining the entity's business continuity plans.

Business Continuity Maturity Model (BCMM)

A framework to assess and categorize an entity's business continuity program comprehensiveness, providing a roadmap for improvement and increased resilience.

Business Continuity Plan (BCP)

A document that outlines the strategies and steps for an entity to maintain critical business functions and recover from disruptions to its operations. (See also: Continuity Plan)

Business Continuity Plan Administrator

The individual designated to develop, maintain, update, and distribute the business continuity plan. Also called the Business Continuity Manager.

Business Continuity Planning

The process of identifying risks and impacts to an entity's operations, as well as developing strategies, plans, and procedures to facilitate the ability to continue the necessary processes during a disruption.

Business Continuity Policy Statement

A declaration of an entity's goals, principles, and approach to business continuity management.

Business Continuity Program

A management and governance program designated to develop, implement, and maintain business continuity plans.

Business Continuity Program Board

A governance body that provides strategic oversight, direction and support for an entity's business continuity program.

Business Continuity Steering Committee

A committee, responsible for providing strategic direction, oversight, guidance, and approval for the entity's business continuity management program.

Business Continuity Strategy

The resources and processes to enable entities to meet their business continuity objectives.

Business Continuity Team

A designated group of individuals responsible for developing, maintaining, executing, and testing an entity's business continuity strategies and plans. The team ensures that critical operations can continue or be restored in the required timeframe following a disruption.

Business Function

A defined set of related activities or tasks that deliver a specific outcome for the entity.

Business Impact Analysis (BIA)

The process by which an entity determines the effects of a disruption to the entity and its assets.

Business Interruption

An interruption to an entity's ability to operate in its usual manner.

Business Interruption Costs

Financial impact associated with a disruption of an entity's ability to operate in its usual manner.

Business Interruption Insurance

Insurance that compensates an entity for income lost as a result of a covered event that prevents a business from operating due to direct physical loss or damage.

Business Objective

A specific, measurable result the entity intends to achieve within a defined timeframe to advance its strategy and mission.

Business Operations

The day-to-day activities and processes performed by an entity to deliver products or services.

Business Process

A structured set of functions designed to achieve a specific organizational goal, including delivery of a product or service to a customer.

Business Recovery

The process of restoring operations and critical functions to an acceptable level following a business disruption to ensure minimal operational impact and alignment with predefined recovery objectives.

Business Recovery Coordinator

An individual designated to coordinate, control, and oversee designated recovery processes or testing within an entity's business continuity program to ensure effective resumption of operations following disruptions.

Business Recovery Team

A group of individuals responsible for maintaining business recovery procedures, coordinating the recovery of business functions and processes, and facilitating the resumption of operations following a disruption.

Business Recovery Timeline

A defined chronological sequence for the restoration of organizational capabilities following operational disruption.

Business Resumption

The process or condition of restoring and resuming an entity's processes and operations to a defined state following a disruption, ensuring continuity and alignment with recovery objectives.

Business Unit

A department, division, or functional group within an entity that performs specific process(es).

Business Unit Coordinator

A designated representative within each business unit responsible for implementing business continuity specific to their unit's functions and requirements.

C

Call Tree

A structured communication method, that defines the sequence, and procedures for notifying contacts during emergencies, crises, or business continuity plan activations to ensure timely notification.

Capacity

An entity's ability to maintain its operations and deliver products and/or services.

Change Management

The process of managing organizational transitions encompasses planning, oversight or governance, project management, testing, and implementation. In the context of technology change management, this is the systematic control and documentation of modifications to IT systems, infrastructure configurations, and technical procedures. This process may encompass version control, configuration management, rollback procedures, and technical change approval workflows that ensure system integrity while enabling rapid adaptation to disruption scenarios and recovery requirements.

Checklist

A list that documents specific tasks, items, actions, or requirements to be performed during preparedness, response, recovery, or continuity activities.

Chief Information Officer (CIO)

The executive leader responsible for organizational technology strategy and digital infrastructure management.

Chief Resilience Officer

The executive leader responsible for strategies that reduce an entity's vulnerability to disruptions.

Civil Emergency

Incident posing an immediate threat to public safety, health or welfare that requires immediate action by authorities.

Climate Risk

The negative impacts on humans and ecological systems as a result of climate change.

Cloud Computing

A computing model in which shared, provider-managed resources (including servers, storage, networking, platforms, and applications) are delivered over networks on demand. Capacity is pooled and elastic, allowing rapid provisioning and release with minimal administration and supporting resilience through geographic distribution, redundancy, and rapid recovery.

Cold Site

A facility used for recovery that requires resources, such as equipment, technical infrastructure, and raw materials to become operational.

Command Center

A physical or virtual location established near, but outside, the affected area to direct and coordinate tactical response, recovery, and restoration activities. Multiple command centers may operate simultaneously during an event and typically report to the emergency operations center.

Confidentiality
The ethical and legal duty to refrain from sharing sensitive, private, personal, or proprietary information from unauthorized disclosure.

Contingency Plan
A formal, documented strategy developed by an entity or business unit to prepare for and respond to specific operational disruptions or system failures, ensuring an effective and timely recovery of critical functions.

Contingency Planning
The process of creating strategies and procedures that enable an entity to effectively respond to disruptions that could negatively impact its ability to deliver goods and services.

Contingent Business Interruption Insurance
A form of business income insurance covering an insured against loss of income as a result of a disruption to its inbound supply chain or the inability of a recipient to receive goods from the entity's outbound delivery system.

Continual Improvement
An ongoing process aimed at enhancing an entity's management system and overall performance to better meet its objectives.

Continuity
A state of continuous and uninterrupted operation.

Continuity of Government (COG)
A coordinated effort within government branches to ensure that critical national functions continue during catastrophic emergencies, maintaining authority and operational capabilities.

Continuity of Operations (COOP) Plan
A documented set of instructions and procedures that enables an entity to sustain its mission-critical functions following a disaster.

Continuity Plan
A document that defines the strategies and activities for an entity to recover and maintain critical functions.

Continuous Availability
The delivery of technology (application, system, service) without interruption.

Continuous Operations
The ability of an entity to perform its business processes without interruption, ensuring ongoing delivery of products and services despite adverse events.

Control
A physical or procedural restriction to prevent an undesired action. Control also means managing the utilization or behavior of a configuration item, system, or IT service.

Corporate Governance
Policies, rules, processes, practices, and controls which direct corporate behavior.

Corrective Action

Action taken to resolve non-conformity issues.

Cost Benefit Analysis

A process used to assess the advantages and disadvantages (costs) of a particular course of action.

Crisis

A severe and/or widespread event that threatens or disrupts an entity, group, or society.

Crisis Communications

The practice of managing and sharing information during a disruption.

Crisis Management

A strategic process entities use to prepare for, respond to, and recover from unexpected events or disruptions to operations, damage to reputation, or harm to stakeholders.

Crisis Management Team (CMT)

A group within an entity who are tasked with preparing for, responding to, and mitigating the impact of crises.

Crisis Fatigue

A psychological and physical state of exhaustion or desensitization that occurs when individuals or entities are subjected to prolonged, repeated, or high-intensity crises or disruptions.

Critical Infrastructure

Assets of such strategic importance to the performance of critical functions that their incapacitation or destruction would have a very serious or debilitating effect on an entity's ability to maintain operations.

Critical Operations

The services, products, or functions of an entity which, if disrupted, could put the continued viability of the entity at risk.

Critical Third Parties

Organizations in the supply chain that are required for the entity to be able to fulfill its mission.

Cyber Attack

A malicious attempt to disrupt, damage or disable computer systems, networks or digital devices.

Cyber Insurance/Cyber Liability Insurance

A type of insurance designed to mitigate the effects of a variety of technology-related threats, including malware and ransomware attacks, data breaches, etc.

Cyber Resilience

An entity's ability to anticipate, withstand, recover from, and adapt to adverse cyber events.

Cybersecurity

The protection of networks, systems, and data against unauthorized access, use, disclosure, disruption, modification, or destruction to preserve confidentiality, integrity, and availability.

D

Damage Assessment

A determination of the effects of the incident on people; on physical, operational, economic characteristics; or on the environment.

Data Integrity

The accuracy, consistency, and reliability of data.

Data Mirroring

The real-time or near real-time replication of data from a primary system to one or more secondary location(s) to maintain an up-to-date copy for availability, failover, or recovery.

Data Recovery

The process of restoring data, applications, and configurations from backups or replicas to a known, usable state after loss, corruption, or disruption.

Data Risk

Data risk addresses the impact that can result from the management of data including its collection, storage, processing, use, sharing, or disposal.

Declaration

A formal announcement made by authorized personnel that a disaster, emergency, or disruption has occurred or is imminent, triggering pre-established response and recovery actions.

Deepfake Technology

Deepfake technology is used to create realistic (but fake) images, videos, and sound recordings of a person.

Delegation of Authority

A formal preapproved assignment of specific responsibilities to a designated alternate.

Denial of Service (DoS) Attack

A cyberattack that aims to make technology resources (application, computer, or network) unavailable to its intended users. (See also: Distributed Denial of Service Attacks)

Dependency

Reliance upon another entity, action, or tool for completion of a function, operation, process, or activity. (See also: Interdependencies)

Devolution

The transfer of statutory or operational authority, responsibility, or critical functions from an entity's primary operating staff and facilities to other staff and alternate locations to sustain critical functions when necessary.

Devolution Emergency Response Group (DERG)

A pre-identified team, located at an alternate location(s) equipped with delegated decision-making authority to maintain critical organizational functions during leadership succession scenarios.

Digital Twin Testing

A dynamic, virtual representation of an entity's physical assets, systems, or operations that enables simulation, analysis, and testing of continuity and recovery strategies in real time.

Disaster

A sudden event causing unacceptable damage or loss; an event that compromises an entity's ability to provide critical functions, processes, or services for some unacceptable period of time; or an event where an entity's management invokes recovery plans.

Disaster Recovery

The coordinated process of restoring and resuming technology systems, applications, data, and infrastructure following a disruption.

Disaster Recovery Plan

A documented set of procedures and information developed to restore technology systems, applications, and data in the event of a disruption. The plan includes recovery strategies, recovery time objective (RTO), recovery point objective (RPO), roles and responsibilities, and required resources.

Disaster Recovery Planning

The ongoing process of developing, implementing, maintaining, and testing strategies and procedures to restore technology services after a disruption. This ensures critical technology capabilities can meet defined recovery objectives during and after adverse events.

Disaster Risk

Risk to an entity, group, or community which arises from an event.

Disaster Risk Reduction

A comprehensive methodology for minimizing organizational vulnerability to disruptive events through proactive identification, assessment, and mitigation of potential threats.

Disaster Management

The process of preparing for, responding to, and recovering from a large event that exceeds the resources of the local community.

Disruption

An event that interrupts normal functions, operations, or processes.

Distributed Denial of Service (DDoS) Attack

A widespread cyberattack using multiple machines to overload a system with the purpose of making technology resources (application, computer, or network) unavailable to its intended users. (See also: Denial of Service Attack)

DORA (Digital Operational Resilience Act)

A regulation in the European Union (EU) to strengthen the digital resilience of financial entities.

Document

Information and its supporting medium (including paper, magnetic, electronic or optical computer disc, or image) or the recording of such information that can be used as a record.

Downtime

The period when a system, service, facility, or process is unavailable or unable to perform its intended function.

Duty of Care

The legal and ethical obligation that requires an individual or entity to act toward others with the caution and prudence that a reasonable person would use to avoid foreseeable harm.

E

Emergency

An event or situation that poses a significant threat to operations, people, property, or environment, and that potentially requires immediate response to minimize harm and restore normal function.

Emergency Management

A program that includes mitigation, preparedness, response, and recovery activities as related to natural or man-made hazards.

Emergency Operations Center (EOC)

A designated physical or virtual facility where organizational leadership directs, coordinates, and monitors strategic response actions during an incident, ensuring unified decision-making and resource management.

Emergency Plan

A documented set of procedures that directs coordinated, short-term actions to address localized threats or incidents that do not necessitate activating the entity's continuity plan. Commonly referred to as an occupant emergency plan or building closure plan.

Emergency Preparedness

A state of organizational readiness achieved through planning, training, and resource alignment that enables a timely, coordinated, and effective response to an emergency, protecting life, property, and mission-critical operations.

Emergency Relocation Group (ERG)

Designated personnel who relocate to a pre-identified alternate location to sustain the entity's critical functions when the primary facility is unavailable.

Emergency Response

The immediate, coordinated actions taken at the onset of an emergency to safeguard life, protect property, and limit escalation in order to ensure the situation is stabilized and critical impacts are minimized.

Emergency Response Plan

A documented set of procedures that details an entity's rapid, coordinated actions to protect life, property, and critical operations during the initial phase of an emergency.

Emergency Response Team (ERT)

A designated group of trained and authorized personnel that mobilizes immediately to implement the entity's emergency response procedures, protect life and property, and stabilize the situation during an incident.

Enterprise

A public or private sector entity or business.

Enterprise Risk Management (ERM)

The methods and processes used by entities to manage risks and seize opportunities related to the achievement of their objectives. Provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the entity's objectives (risks and opportunities), assessing risks 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

Increase in severity of an incident or notifying a higher level of command.

Essential Functions

The operations within an organization, deemed necessary for the survival of the organization.

Essential Services

Activities not involving a physical product that are necessary for the survival of the organization.

Evacuation

The orderly movement of people from a hazardous area to a safe location.

Event

An occurrence; in the context of business continuity, an event often refers to an undesired situation requiring a response.

Executive/Management Succession Plan

A predetermined plan for the continuity of authority, knowledge, and decision making of critical roles in the event the person in the role is unable or unwilling to remain in the role.

Exercise

An activity designed to test, evaluate, and improve an entity's response or reaction to a situation. In the context of resilience, an exercise involves performing and assessing recovery and response actions in a simulated, controlled environment to ensure the business continuity, disaster recovery, crisis management or emergency response plans will work as intended in an actual disaster.

Types of Exercises include:

Call Tree Test: A structured verification exercise used to validate the accuracy and effectiveness of an entity's emergency communication system, specifically the ability to reach all employees and key interested parties during an emergency.

Disaster Recovery Exercise: A process designed to validate an entity's disaster recovery (DR) capabilities.

Full-Scale Exercise: A test involving all processes of an organization.

Functional Exercise: An exercise that assesses the actions of a specific function of an entity.

Life Safety Test: A test of the capabilities to reduce the effects of an incident on people.

Notification Test: An exercise that tests a plan ability to communicate during an incident.

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

Tabletop Exercise: A discussion-based exercise in which participants are given a fictitious scenario and are asked to describe how they would respond to it. Also known as a scenario-based tabletop.

Exercise Plan

A documented framework that outlines the objectives, scope, scenario, participants, roles, logistics, and evaluation criteria for conducting a business continuity, disaster recovery, and/or crisis management exercise. The plan can serve as a roadmap to ensure that the exercise is structured, consistent, and aligned with the organizational goals.

Extra Expense Insurance

Insurance covering the additional cost to maintain operations or get back in operation more quickly following property loss.

F

Facility

A physical location that supports an entity's administration, processes, systems, and/or operations.

Failover

The automated or manual process of switching from a primary system, component, or site to a redundant or standby system to maintain operations following a failure or disruption.

Failure

The inability of an operational or technology system, component, process, service, or function to perform its intended purpose within defined parameters. A failure often causes an incident.

Fallback Site

A substitute facility used when the primary site is unavailable or unusable, providing a temporary base for critical operations. (See also: Alternate Site)

Financial Risk

The possibility of monetary reduction or loss of economic gain as a result of an action or inaction.

First Responder

An individual trained to provide immediate assistance at the scene of an emergency. Typically, they are first to arrive and are responsible for protecting life, property, and environment during the initial stages of an incident.

Function

Task(s) completed by a person, team, or technology.

G

Gap Analysis

The process of identifying differences between current capabilities, resources and/or information, and desired outcomes to highlight areas that require improvement or remediation.

Geographic Dispersion

A strategy to intentionally distribute critical organizational assets, personnel, and operations across multiple physical locations to minimize single-point-of-failure risks. This strategy reduces exposure to localized geographical threats.

Governance

The organizational framework that defines decision-making authority, accountability structures, and oversight mechanisms for managing enterprise operations and risk. This may encompass the policies, procedures, and control systems that guide organizational behavior and ensure responsible management of resources and capabilities.

Governance, Risk and Compliance (GRC)

A unified management approach that aligns organizational governance structures with risk management activities and regulatory compliance requirements. This integrated framework ensures decision-making processes consider risk implications while meeting legal and regulatory obligations across all operational areas. While interpreted differently in various entities, GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM), and corporate compliance with applicable laws and regulations.

H

Hacker

An individual who uses technical skills to gain unauthorized access to systems, networks, or data.

Hazard

A potential source of harm or adverse impact to people, operations, property, the environment, or organizational objectives.

High Availability

A characteristic of a system or a service that aims to minimize downtime and ensure continuous operation for an extended period.

Hot Site

An alternate facility that is fully redundant and equipped with infrastructure, equipment, and resources to provide immediate business recovery in the event the primary location is unavailable.

Human Threats

Intentional or unintentional actions caused by individuals; have the potential to disrupt operations, cause harm to personnel, damage assets, or compromise information and infrastructure.

I

Impact
The effect or consequence of a disruptive event on the entity's operations, assets, finances, reputation, or personnel. Impacts may be quantitative or qualitative and are used to assess severity and prioritize recovery efforts.

Impact Analysis
The process of evaluating the financial and personnel effects of a disruption.

Impact Tolerance
The amount of operational downtime an entity can withstand. A term commonly used in operational resilience regulations.

Important Business Services (IBS)
The services an entity provides which, if disrupted, could create a risk to for the viability of the entity. IBSs are the specific products or services an entity provides to its customers.

Incident
An event or occurrence.

Incident Command System
A site (virtual or real) to manage and coordinate responses to incidents, emergencies, or disruptions.

Incident Management
The coordinated process an entity uses to respond to an incident, applying established emergency procedures to limit impact, protect people and assets, and restore acceptable operations as quickly as possible.

Incident Management Plan (IMP)
A documented guide that defines the personnel, resources, services, and step-by-step actions needed to execute the incident management process when an event occurs.

Incident Management System (IMS)
An integrated framework encompassing facilities, personnel, policies, procedures, equipment, and communications that establishes a standard organizational structure for directing and coordinating resources effectively during an incident.

Incident Management Team
An authorized group responsible for developing, leading, and managing the response plan during a disruptive incident, ensuring resources are coordinated and actions are executed effectively.

Incident Manager
The designated official in command of incident management response.

Incident Response
The actions taken after an event to safeguard life, limit damage, prevent escalation, and restore operational stability.

Incident Response Plan
A documented set of instructions, procedures, and actions to respond to, mitigate, and minimize the impact of disruptive incidents.

Information Technology (IT)
The computers, software, networks, and data to manage, process, store, and transmit information which support organizational operations.

Inherent Risk

The level of risk that exists without application of any mitigation or controls.

Insider Threat

The risk posed by individuals who have authorized access to an entity's systems and/or data and who may cause intentional or accidental damage.

Insurance

A contractual arrangement in which another party, usually an insurance company, agrees to compensate a person or entity for losses caused by a covered occurrence, in exchange for a premium (payment). This arrangement transfers the person's or entity's exposure.

Interagency Agreement (IAA)

A formal cooperative arrangement between entities that establishes protocols for mutual support, resource sharing, and coordinated response during disruptive events.

Interdependencies

The relationship between two or more processes, technologies, or entities where the operation, recovery and/or success of one relies on the mutual successful operation, recovery and/or success of the other(s).

Internal Audit

An independent, objective assessment within an entity to evaluate and improve the effectiveness of a process, control, and/or governance processes. In the context of business continuity and resilience, internal audits assess the design, implementation, and performance of continuity programs, ensuring compliance with policies, regulatory requirements, and best practices. Findings from internal audits help identify gaps, recommend corrective actions, and support continuous improvement.

IT Service Continuity Management (ITSCM)

The management process that keeps critical IT services available during and after a disruption.

J

Jamming

A type of denial-of-service attack, where wireless networks are disrupted or disabled through electronic interference signals.

Just-in-Case Supply Chain

A strategy in which goods are stored in inventory to ensure that they are available when needed.

Just-in-Time (JIT)

A strategy in which goods arrive exactly when needed which minimizes the need to store goods.

K

Key Logger

A key logger is a type of malicious hardware or malware that records key strokes on a computer keyboard or other device (such as a cash machine) without a user's knowledge. The data is then sent back to hackers who can use the information to access data such as password/PIN-protected records/files, networks, or building access controls.

Key Risk Indicators (KRIs)

Metrics used to identify, assess, and monitor the main drivers of risk.

L

Legal Risk

The possibility of civil and/or criminal penalties resulting from non-compliance with laws or regulations.

Likelihood

The possibility or chance of occurrence.

Loss

The adverse effect on an entity resulting from a disruption, hazard, or event. Loss may be direct (the event happened directly to the entity or its assets) or indirect (the event happened outside the entity or its assets) and can include harm to people or the environment (including damage to assets, loss of data/information, service degradation, regulatory penalties, and reputational impact); all of which can result in impact to financial impact (including increased costs, reduced revenue, additional expenses) as well as, reputational impact.

M

Machine Learning

A subfield of artificial intelligence which involves the development of statistical algorithms that can learn from very large datasets (big data) to identify patterns and make predictions or decisions. Over time, the artificial intelligence learns in order to improve accuracy in performance.

Malicious Code (Malware)

Software or code that is designed to infiltrate a computer, network, or application with the intent to cause harm or disruption. Also called Malware.

Managed Services

The practice of outsourcing the responsibility for a specific set of functions or processes to a third party known as a managed service provider (MSP). Managed services are based on a proactive, ongoing, and often subscription-based model.

Management System

An organized framework of policies, roles, processes, and resources an entity uses to plan, operate, monitor, and continually improve in order to meet its objectives.

Manual Workaround

The use of non-automated processes when automated systems are not available.

Maximum Tolerable Downtime (MTD)

The maximum duration an entity can tolerate a disruption to critical processes, systems, or functions before suffering unacceptable consequences, such as severe financial loss, reputational damage, or threats to viability. Also called Maximum Tolerable Period of Disruption (MTPD)

Metric

A quantifiable measure used to monitor performance, risk, or progress against a defined objective or standard.

Microsimulation

An automated analytical tool that measures interaction of individual things or people.

Mission Essential Functions (MEFs)

Functions that directly support an entity's mission and must have the highest availability support.

Mission Statement

A statement outlining an entity's overall purpose, intentions, and objectives.

Mitigation

Actions taken to reduce the probability, severity, and duration of adverse events.

Mobilization

The activation and deployment of personnel, resources, and information during a disruptive event or plan activation.

Multifactor Authentication (MFA)

A security process where users are required to provide two or more forms of identification or credentials in order to access an account or application.

Mutual Agreement

Prearranged support between two or more entities to share people, equipment, facilities, or services when needs exceed local capacity. Assistance can be reciprocal or one-way under agreed terms. Also referred to as reciprocity.

Mutual Aid Agreement

A prearranged agreement between entities to provide assistance during an emergency.

N

Natural Hazards

Threats that result from natural occurrences.

O

Occupant Emergency Plan

A document of procedures that outline the steps to protect the occupants either by evacuation or shelter-in-place following an emergency or crisis.

Offsite Location

An alternate, geographically separate location, used to maintain or restore operations following an event.

Off-Site Storage

A secure facility (geographically separated from the primary site) where records, backups, and critical spare resources are kept for recovery.

Operational

Relating to and about an entity or an entity's processes. The term operational can also refer to aspects related to the functioning or performance of an entity's activities, systems, or processes.

Operational Capability

The ability to execute operations.

Operational Continuity
Maintaining business activities following a disruptive event.

Operational Experience
The knowledge gained by direct involvement in performing or managing an entity's processes.

Operational Procedures
Defined processes to complete a task.

Operational Resilience
The ability of an entity to continue operations throughout a business disruption. It includes planning, response, recovery, training, and exercising.

Operational Risk
The possibility of adverse impact or loss to operational processes.

Operational Risk Profile
A summary of the types and levels of operational risks to which an entity may be vulnerable. It details the likelihood and potential impact of failures in internal processes, people, systems, or from external events. It serves as a crucial tool for senior management to analyze current exposure, make strategic decisions, allocate resources, and monitor the effectiveness of risk controls.

Operations Centers
Facilities established to manage response, continuity, and recovery operations (See also: Emergency Operations Center)

Organizational Resilience
An entity's ability to anticipate, prepare for, respond to, and recover from incidents, while maintaining values and integrity.

Outage
The temporary loss of a resource.

Outsourcing
An arrangement where work is transferred to an external entity.

P

Pandemic

A widespread outbreak of a communicable disease impacting global or regional populations.

Penetration testing

Penetration testing (sometimes referred to as ethical hacking) is an assessment tool using a simulated cyber-attack to test vulnerabilities in a system or network.

Phishing

Phishing is a fraudulent communication where the sender misrepresents themselves in order to obtain personal information. Types of phishing include:

Spear phishing: A sophisticated, targeted phishing attack using personalized information to convince someone that the email is genuine.

Voice phishing: An act where attackers make automated phone calls to a large number of people, often using text-to-speech synthesizers, to trick them into entering in personal information on keypads. Also referred to as vishing.

SMS phishing: An act where SMS messages are sent to multiple people encouraging them to enter personal information by clicking a link, calling a phone number, or contacting an email address. Also referred to as smishing.

Plan Maintenance

The systematic process of keeping documentation current. For business continuity planning, it is the process of ensuring the business continuity plan (BCP) is up to date.

Platform Outage

A situation where a service or application becomes temporarily or permanently unavailable due to technical problems.

Preparedness

Maintaining a level of readiness to mitigate the impact of an incident.

Preventative Measures

Preemptive controls to mitigate or prevent undesirable impacts.

Prevention

Activities implemented to stop a destructive activity from occurring.

Primary Operating Facility

The principal location where an entity conducts standard business operations and maintains core operational capabilities.

Priority

The designation that ranks activities and resources in order of importance.

Program

The overall framework and plan of action for a specific initiative.

R

Ransomware
A type of malware that prevents access to a set of data or applications until a payment is made to restore access.

Readiness
The state of being prepared.

Reciprocal Agreement
An agreement between two entities to provide predefined assistance (including facilities, equipment, resources, and processes) to facilitate continuity.

Reconstitution
Refers to the process of restoring and resuming normal business operations.

Recovery
The process of restoring and resuming operations, functions, or systems following a disruption.

Recovery Point Capability
The demonstrated ability of an entity to recover data to a defined point in time.

Recovery Point Objective (RPO)
The maximum acceptable amount of data loss measured over time before a disruption occurs.

Recovery Time Capability
The demonstrated ability of an entity to recover a function, process, or system within a specific time frame.

Recovery Procedures
Documented steps to restore and resume systems, applications, infrastructure, or business processes following a disruption.

Recovery Strategies
Predefined and documented actions for restoring operations, systems, or business functions following a disruption. Strategies are often selected based on risk, impact, resource requirements, and recovery objectives.

Recovery Time Estimate (RTE)
The estimated time needed to recover a specific process, system, or application after a disruption.

Recovery Time Objective (RTO)
The maximum acceptable time that a process, application, or system can be unavailable before significant impact occurs.

Recovery Timeline
An ordered sequence of actions required to restore operations, systems, or functions following a disruption.

Redundancy
Duplicate systems, processes, or resources to facilitate recovery.

Regulation
A rule or requirement established by an authoritative body mandating compliance in order to avoid penalty.

Regulatory Risk
The possibility of financial loss and civil or criminal penalties resulting from non-compliance with regulatory requirements.

Remediation
Actions taken to correct or eliminate an identified vulnerability, hazard, or deficiency.

Reputational Risk
The possibility of negative perception or a worsening of public opinion toward a person or entity.

Residual Risk
The level of risk that remains after mitigations and controls are applied.

Resilience
The ability to adapt, withstand, and overcome negative situations or disrupting events.

Resilience Heat Map
A visual tool used to illustrate and assess risk exposure and/or the level of resilience across key business areas, processes, systems, or locations.

Resource Management
The coordinated planning, acquisition, allocation, and tracking of personnel, equipment, facilities, and funds to support organizational objectives and sustain operations.

Response
Actions taken in reacting to a disruptive or emergency incident.

Response Plan
A documented set of procedures guiding coordinated actions to manage and control the reaction to an incident.

Response Time
The elapsed time from detection or first notification to the time of reaction.

Restoration
The process of returning systems, facilities, or processes to normal operation after a disruption.

Resumption
Restoring activities after a disruption.

Return on Investment (ROI)
A measure of the benefits gained from taking an action measured against the cost of implementing the action.

Risk
The possibility of adverse impact. (See also: Operational Risk, Financial Risk, Legal Risk, Regulatory Risk, Reputational Risk)

Risk Acceptance
Willingness of risk owners and/or senior leadership to tolerate a level of uncertainty or potential loss. (See also: Risk Tolerance)

Risk Analysis

A step in the risk assessment process that assesses the likelihood of a threat occurring and impact if the threat occurs.

Risk Appetite

The overall level of uncertainty or potential loss an entity is willing to accept order to achieve its strategic objectives.

Risk Assessment

The process of identifying potential threats; completing a risk analysis; prioritizing risks and developing mitigation strategies.

Risk Avoidance

The process of avoiding potential risks by eliminating the potential risks.

Risk Categories

Groupings of risks based on shared characteristics (including origin, type, or potential impact) to support structured analysis and management.

Risk and Control Assessments

A tool to assess operational risks, exposure, or impact levels and the design/effectiveness of mitigating controls.

Risk Criteria

Defined thresholds and benchmarks used to assess and prioritize potential loss.

Risk Evaluation

The process of assessing risks by measuring them against established criteria.

Risk Management

A profession; or actions to prevent adverse impact to an entity.

Risk Mitigation

The process of implementing measures to reduce the likelihood or impact of identified risks to acceptable levels.

Risk Reduction

Actions taken to decrease the probability or severity of risks through improvements to processes, controls, or systems.

Risk Response Strategies

Actions taken to reduce or manage identified risks to an entity. These include avoidance, transfer, mitigation, and acceptance.

Risk Tolerance

The overall level of impact an entity can accept in order to achieve its strategic objectives. (See also: Risk Acceptance)

Risk Transfer

Sharing the financial impact of a disruptive event.

Root Cause

The primary factor or underlying reason that initiates a problem, failure, or incident.

Root Cause Analysis

A systematic method for investigating and identifying the fundamental causes of a problem or incident in order to prevent recurrence.

S

Salvage

Actions taken to recover items that have been affected by a disaster.

Scenario

A hypothetical situation used to simulate a real event.

Scenario Testing

Presenting a fictitious event and asking participants to respond as if the event was occurring, with the goal of assessing and improving participants' overall response capabilities in a controlled setting.

Secondary Site

A prearranged location, separate from the primary facility, designated to support critical functions and resume operations when the primary site is unavailable. (See also: Alternate Site)

Scope

The boundaries and extent of work, coverage, or applicability.

Security

The protection of assets, systems, and information from threats that could result in harm, disruption, or unauthorized access.

Security Controls

Measures implemented to increase the protection of assets, systems, and information against potential threats.

Service Level Agreement (SLA)

A contractual agreement between a customer and a product/service provider that details the expected performance levels.

Service Provider

An entity providing products and/or services to another organization.

Single Source

A provider selected to be the only vendor to supply a specific product or service.

Single Point of Failure

A resource (person, place, or thing) that when unavailable will result in the failure of the system.

Situational Awareness

A compilation of information pertaining to the current state of the threat landscape.

Sole Source

The only existing or available supplier. A disruption or failure in this source would cause a significant impact to operations.

Spyware

A type of malware designed to gather information about a user or entity without their knowledge, often to monitor activity or steal sensitive data.

Stakeholder

An interested party and/or someone directly involved or impacted by something.

Standard

An established set of criteria, guidelines, or requirements developed by recognized bodies to ensure consistency, quality, and effectiveness in processes, products, or services.

Strategic

The identification of long-term goals and the means by which they can be accomplished.

Succession

Designating a predetermined replacement for an orderly transfer of authority.

Supplier

A person or entity that provides goods or services.

Supply Chain

A connected system of entities, people, activities, and resources involved in creating, delivering, and receiving products or services.

Supply Chain Mapping

The process of identifying and documenting all entities, activities, and relationships involved in the production, delivery, and receipt of products or services to understand dependencies, risks, and potential points of failure.

T

Tactical

Actions planned to achieve a particular goal or objective.

Technological Hazard

A potential source of harm or adverse impact arising from technology, infrastructure, or industrial processes, including equipment failures, hazardous material releases, infrastructure outages, or cyber incidents. Such hazards may occur on their own or be triggered by a natural event.

Telework Site

A remote location used to conduct business.

Test

A means of measuring the capabilities and/or knowledge of a particular person or entity.

Test Plan

A document that details the scope, methodology, objectives, and success criteria of a test or exercise.

Testing

Performing a structured evaluation of the effectiveness or capabilities relative to specified objectives or measurement criteria.

Threat

A potential undesirable event, action, or circumstance that may cause harm if it were to come to fruition.

Threat Assessment

The systematic process of identifying, analyzing, and evaluating the likelihood and severity of hazards.

Threat Monitoring

Continuous analysis, observation, and review of indicators to detect potential hazards that may affect people, assets, operations, objectives, or the environment.

Third-Party/Third- Party Service Provider

Any external organization that provides goods, services, or support to an entity.

Tolerance for Disruption

The amount of acceptable interruption or downtime of a process.

Training

Training is a structured process to educate and transfer knowledge and skills in order to enhance competency in a subject.

Trigger

A predefined condition, threshold, or event that initiates a response.

Trojan Horse

Malware disguised as legitimate software or a file that, once executed, allows unauthorized access or damage to a system.

U

Unified Command

A component of an incident command system that determines hierarchical authority when multiple agencies or jurisdictions work together to manage an incident.

V

Value Stream Mapping

A visual tool and analytical method used to document, analyze, and improve the flow of information and activities required to deliver a product or service. Identifies both value-adding and non-value-adding steps, enabling entities to enhance efficiency, reduce waste, and strengthen process resilience.

Vendor

An individual or company that provides products or services to another person or organization.

Virus

Malicious code that attaches itself to legitimate programs or files and spreads by infecting other files or systems, often causing damage or disruption.

Vital Records

Documents or information required for the continued functioning, operational reconstitution, or protection of legal or financial interests.

Vulnerability

A weakness or gap in a system, process, or control that could be exploited by a threat to increase risk to people, assets, operations, or objectives.

Vulnerability Assessment

The process of identifying, quantifying, and prioritizing vulnerabilities in systems, processes, or controls to inform and guide mitigation strategies.

W

Walk-Through

A step-by-step review process in which participants systematically examine a plan, process, procedure, or system to verify its completeness, accuracy, and usability.

Warm Site

An alternate site that requires some level of resources such as equipment, technical infrastructure, and raw materials to become operational. It cannot be used immediately but can be used more quickly than a cold site.

Work Area Recovery

A prepared site separate from the primary facility, designated to support critical functions and resume operations when the primary site is unavailable. (See also: Alternate Site)

Worm

A standalone, rapidly spreading malware that replicates itself across networks without needing to attach to other files or programs. (See also: Malware)

Z

Zero Day Attack

A type of cyberattack where malware is released to exploit a vulnerability in a technology system before a patch can be applied.