Important Terminology's for Aspirants.

1. **access control:** The control of persons, vehicles, and materials through the implementation of security measures for a protected area.
2. **alarm system:** Combination of sensors, controls, and annunciators (devices that announce an alarm via sound, light, or other means) arranged to detect and report an intrusion or other emergency.
3. **asset:** Any tangible or intangible value (people, property, information) to the organization.
4. **barrier:** A natural or man-made obstacle to the movement/direction of persons, animals, vehicles, or materials.
5. **building envelope:** The separation between the interior and the exterior environments of a building. It serves as the outer shell to protect the indoor environment as well as to facilitate its climate control. Building envelope design is a specialized area of architectural and engineering practice that draws from all areas of building science and indoor climate control.
6. **camera:** Device for capturing visual images, whether still or moving; in security, part of a video surveillance.
7. **CCT rating:** *Corrected Color Temperature (CCT)* is a measure of the warmth or coolness of a light. It is measured in degrees Kelvin which is the Centigrade (Celsius) absolute temperature scale where 0°K is approximately 272°C.
8. **closed-circuit television (CCTV):** See video surveillance.
9. **contract security service:** A business that provides security services, typically the services of security officers, to another entity for compensation.
10. **crime prevention through environmental design (CPTED):** [pronounced *sep-ted*] An approach to reducing crime or security incidents through the strategic design of the built environment, typically

employing organizational, mechanical, and natural methods to control access, enhance natural surveillance and territoriality, and support legitimate activity.

11. **crime:** An act or omission which is in violation of a law forbidding or commanding it, for which the possible penalties for an adult upon conviction include incarceration, for which a corporation can be penalized by a fine or forfeit, or for which a juvenile can be adjudged delinquent or transferred to criminal court for prosecution. The basic legal definition of crime is all punishable acts, whatever the nature of the penalty.
12. **denial:** Frustration of an adversary's attempt to engage in behavior that would constitute a security incident (see *security incident*).
13. **detection:** The act of discovering an attempt (successful or unsuccessful) to breach a secured perimeter (such as scaling a fence, opening a locked window, or entering an area without authorization).
14. **event:** A noteworthy happening; typically, a security incident (see *security incident*), alarm, medical emergency, or similar occurrence.
15. **facility:** One or more buildings or structures that are related by function and location, and form an operating entity.
16. **lighting:** Degree of illumination; also, equipment, used indoors and outdoors, for increasing illumination (usually measured in lux or foot-candle units).
17. **intrusion detection system:** A system that uses a sensor(s) to detect an impending or actual security breach and to initiate an alarm or notification of the event.
18. **lock:** A piece of equipment used to prevent undesired opening, typically of an aperture (gate, window, building door, vault door, etc.), while still allowing opening by authorized users.
19. **perimeter protection:** Safeguarding of a boundary or limit.
20. **physical security:** That part of security concerned with physical measures designed to safeguard people; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against a security incident (see *security incident*).
21. **physical security measure:** A device, system, or practice of a tangible nature designed to protect people and prevent damage to, loss of, or unauthorized access to assets (see *assets*).
22. **policy:** A general statement of a principle according to which an organization performs business functions.
23. **private security:** The nongovernmental, private-sector practice of protecting people, property, and information; conducting investigations; and otherwise safeguarding an organization's assets. These functions may be performed for an organization by an internal department (usually called *proprietary security*) or by an external, hired firm (usually called *contract security*).
24. **private security officer:** An individual, in uniform or plain clothes, employed by an organization to protect assets (see *assets*). Also known as a "guard".
25. **procedure:** Detailed implementation instructions for carrying out security policies; often presented as forms or as lists of steps to be taken prior to or during a security incident (see *security incident*).

26. **progressive collapse:** Occurs when the failure of a primary structural element results in the failure of adjoining structural elements, which in turn causes further structural failure. The resulting damage progresses to other parts of the structure, resulting in a partial or total collapse of the building.
27. **proprietary information:** Valuable information, owned by a company or entrusted to it, which has not been disclosed publicly; specifically, information that is not readily accessible to others, that was created or collected by the owner at considerable cost, and that the owner seeks to keep confidential.
28. **proprietary security organization:** Typically, a department within a company that provides security services for that company.
29. **protection-in-depth:** The strategy of forming layers of protection for an asset (see *assets*).
30. **risk:** The likelihood of loss resulting from a threat, security incident, or event.
31. **risk assessment:** The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.
32. **risk management:** A business discipline consisting of three major functions: loss prevention, loss control, and loss indemnification.
33. **security incident:** An occurrence or action likely to impact assets.
34. **security manager:** An employee or contractor with management-level responsibility for the security program of an organization or facility.
35. **security measure:** A practice or device designed to protect people and prevent damage to, loss of, or unauthorized access to equipment, facilities, material, and information.
36. **security officer:** An individual, in uniform or plain clothes, employed to protect assets.
37. **security survey:** A thorough physical examination of a facility and its systems and procedures, conducted to assess the current level of security, locate deficiencies, and gauge the degree of protection needed.
38. **security vulnerability:** An exploitable security weakness.
39. **site hardening:** Implementation of enhancement measures to make a site more difficult to penetrate.
40. **stand-off distance/set-back:** The distance between the asset and the threat, typically regarding an explosive threat.
41. **surveillance:** Observation of a location, activity, or person.
42. **tailgating:** To follow closely. In access control, the attempt by more than one individual to enter a controlled area by immediately following an individual with proper access. Also called *piggybacking*.
43. **threat:** An action or event that could result in a loss; an indication that such an action or event might take place.
44. **throughput:** The average rate of flow of people or vehicles through an access point.
45. **token:** An electronically encoded device (i.e., a card, key-fob, etc.) that contains information capable of being read by electronic devices placed within or at the entry and exit points of a protected facility.
46. **uninterruptible power supply (UPS):** A system that provides continuous power to an alternating current (AC) line within prescribed tolerances; protects against over-voltage conditions, loss of primary power, and intermittent brownouts. Usually utilized in conjunction with an emergency generator.
47. **video surveillance:** A surveillance system in which a signal is transmitted to monitors/recording, and control equipment. Includes closed-circuit television (CCTV) and network- based video systems.

Important Terms, Definitions &Terminology (BSK-W Solutions)

- Assets

  Any real or personal property, tangible or intangible, that a company or individual owns that can be given or assigned a monetary value. Intangible property includes things such as goodwill, proprietary information, and related property. For purposes of this guideline, people are included as assets.

- Consequential

  A secondary result ensuing from an action or decision. From an insurance or security standpoint, costs, loss, or damage beyond the market value of the asset lost or damaged, including other indirect costs.

- Cost/Benefit Analysis

  A process in planning, related to the decision to commit funds or assets. This is a systematic attempt to measure or analyze the value of all the benefits that accrue from a particular expenditure. Usually, this process involves three steps:

  - Identification of all direct and indirect consequences of the expenditure.
  - Assignment of a monetary value to all costs and benefits resulting from the expenditure.
  - Discounting expected future costs and revenues accruing from the expenditure to express those costs and revenues in current monetary values.

- Criticality

  The impact of a loss event, typically calculated as the net cost of that event. Impact can range from *fatal*, resulting in a total recapitalization, abandonment, or long-term discontinuance of the enterprise, to *relatively unimportant.*

- Events

  Something that happens; a noteworthy happening. In the security context, this usually represents an occurrence such as a security incident, alarm, medical emergency, or related episode or experience.

- Goodwill

  The value of a business that has been built up through the reputation of the business concern and its owners.

- Loss Event

  An occurrence that actually produces a financial loss or negative impact on assets. Examples include security incidents, crimes, war, natural hazards, or disasters.

- Natural Disaster

  A naturally occurring calamitous event bringing great damage, loss, or destruction such as tornadoes, hurricanes, earthquakes, and related occurrences.

- Probability

  The chance, or in some cases, the mathematical certainty that a given event will occur; the ratio of the number of outcomes in an exhaustive set of equally likely outcomes that produce a given event to the total number of possible outcomes.

Important Terms, Definitions &Terminology (BSK-W Solutions)

- Qualitative
  Relating to that which is characteristic of something and which makes it what it is.
- Quantitative
  Relating to, concerning, or based on the amount or number of something, capable of being measured or expressed in numerical terms.

- Risk
  The possibility of loss resulting from a threat, security incident, or event.

- Risk Analysis

  A detailed examination including risk assessment, risk evaluation, and risk management alternatives, performed to understand the nature of unwanted, negative consequences to human life, health, property, or the environment; an analytical process to provide information regarding undesirable events; the process of quantification of the probabilities and expected consequences for identified risks.
- Risk Assessment
  The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.
- Security Incident
  A security-related occurrence or action likely to lead to death, injury, or monetary loss. An assault against an employee, customer, or supplier on company property would be one example of a security incident.
- Security Vulnerability
  An exploitable capability; an exploitable security weakness or deficiency at a facility, entity, venue, or of a person.
- Site
  A spatial location that can be designated by longitude and latitude.
- State-of-the-Art
  The most advanced level of knowledge and technology currently achieved in any field at any given time.

- Statistics
  A branch of mathematics dealing with the collection, analysis, interpretation, and presentation of masses of numerical data. In security, this could represent a collection of quantitative data such as

  security incidents, crime reports, and related information that, together with other like information, serves as security-related statistics used for a number of applications including risk and vulnerability evaluations.
- Threat
  An intent of damage or injury; an indication of something impending.

Important Terms, Definitions &Terminology (BSK-W Solutions)

Background Screening: An inquiry into the history and behaviors of an individual under consideration for employment, credit, access to sensitive assets (such as national defense information), and other reasons.

Bankruptcy: A statutory procedure by which a debtor obtains financial relief and undergoes a judicially supervised reorganization or liquidation of the debtor's assets for the benefit of creditors.

Civil Records: Official records related to civil cases—i.e., when one party sues another.

Conviction: The act or process of judicially finding someone guilty of a crime; the state of having been proved guilty.

Credit Bureau: A Consumer Reporting Agency specifically involved in creating a consumer credit report. See also *Consumer Reporting Agency*.

Credit Report: A detailed report of an individual's credit history prepared by a credit bureau including: (1) personal data (current and previous addresses, Social Security Number, employment history); (2) summary of credit history (number and type of accounts that are past-due or in good standing); (3) detailed account information; (4) inquires into applicant's credit history (number and type of inquiries into applicant's credit report); (5) details of any accounts turned over to credit agency (such as information about liens or wages garnishments via federal, state, or county records); and (6) information on how to dispute any of the above information.

Criminal Records: Official records related to criminal cases. A crime is an act or omission that is prosecuted in a criminal court by a government prosecutor and can be punished by confinement, fine, restitution, and/or forfeiture of certain civil rights.

DD Form 214: DD Form 214, Certificate of Release or Discharge from Active Duty. The term "DD-214" is often used generically to mean "separation papers" or "discharge papers." The DD Form 214 documents the primary occupational specialties, decorations, education, and the characterization of service. The DD Form 214 was issued to separate service members beginning in the 1950's. Prior to that time, a variety of service specific forms were issued to separating service members.

Decision-Making: The process of evaluating and judging information gathered and relating it to the specific requirements of the position for which the applicant is applying.

Due Diligence: The attention and care that a reasonable person exercises under the circumstances to avoid foreseeable harm to other persons or their property. Failure to make this effort may be considered negligence.

Employment Verification: The process of contacting an applicant's past employers to confirm items such as dates of employment, title, salary, and eligibility for rehire.

Felony: A serious crime typically punishable by imprisonment for more than one year or by death. Examples include burglary, arson, rape, and murder.

Important Terms, Definitions &Terminology (BSK-W Solutions)

- **Incarceration:** The act or process of confining someone; imprisonment.In other words, another official name for a special type of preemployment background screen which normally involves communicating with others that know the applicant and reporting back the details of those inquiries. If information is obtained that is adverse to the interest of the consumer, then Section 606 of the FCRA sets forth additional requirements.

- **Jail:** A local government's detention center where persons awaiting trial or those convicted of misdemeanors are confined.

- **Judgment:** A court's final determination of the rights and obligations of the parties in a case.

- **Lien:** A legal right or interest that a creditor has in another's property, lasting usually until a debt or duty that it secures is satisfied.

- **Misdemeanor:** A crime that is less serious than a felony and is typically punishable by fine, penalty, forfeiture, or confinement (usually for up to one year) in a place other than prison (such as county jail).

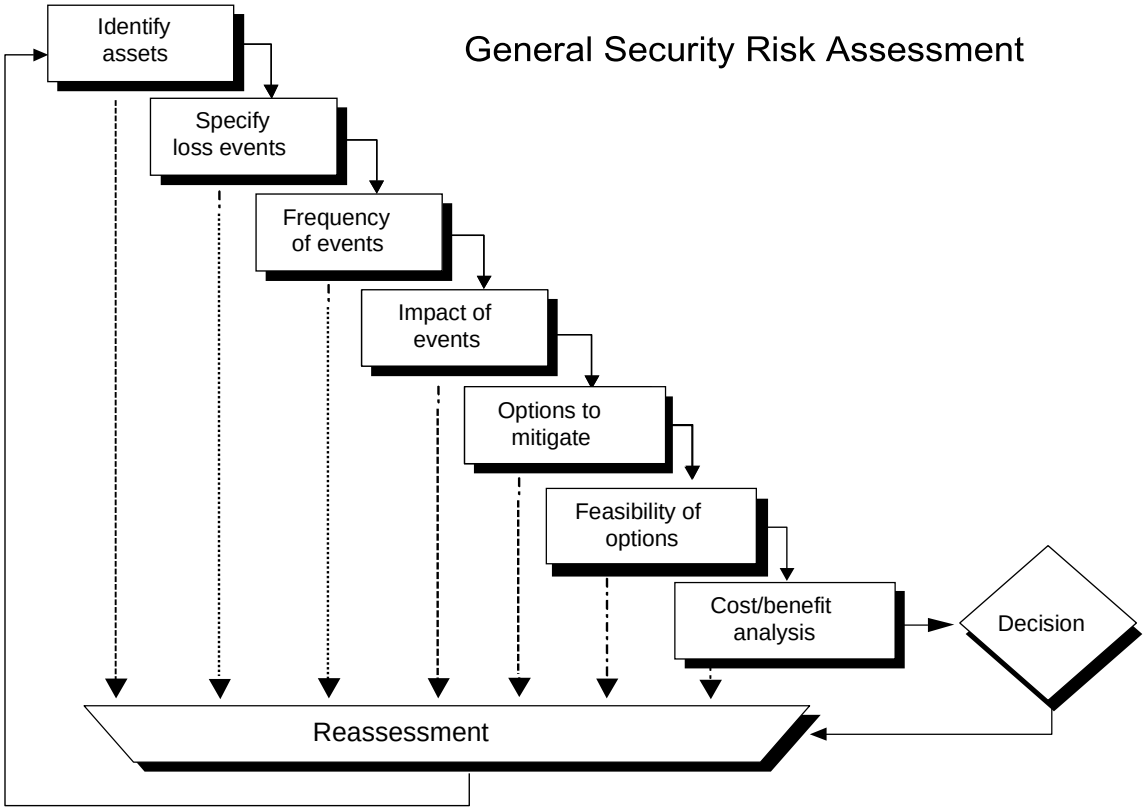
- **Negligent Hiring:** The failure to use reasonable care in the employee selection process, resulting in harm caused to others. Employers have a legal duty not to hire people who could pose a threat of harm to others, which can include everything from slight to fatal bodily injury, theft, arson, or property damage. The definition of ''reasonable care'' depends on the degree of the risk of harm to others. The greater the risk, the higher the standard of care required.
  Prison: A state or federal facility of confinement for convicted criminals, especially felons.

- **Employee Assistance Program (EAP):** An employee benefit involving mental health counseling offered by some employers, typically in conjunction with a health insurance plan. EAPs are intended to help employees deal with personal problems that might adversely affect their work performance, health, and well-being. EAPs generally provide short-term counseling and referral services for employees and their household members. As a general matter, communications are confidential as between the employee and EAP, with two exceptions: (i) mental health providers have a "duty to warn" if the employee poses a credible risk of violence; or (ii) the employee authorizes the release of clinical information.
- **Fitness for Duty Examination:** Distinct from a *Violence Risk Assessment* (see definition for *Violence Risk Assessment*). A process at times imposed by an employer when an employee exhibits behavior that does *not* generate a concern for safety from violence but that impedes job functioning and could be related to a physical, mental, or emotional disorder. The process is conducted by a licensed mental health professional specifically trained and qualified to evaluate the impact of clinical conditions on job-related functioning and to assess whether the employee is fit to perform the essential functions of his or her job, with or without a reasonable accommodation by the employer.

- **Incident Management:** Synonymous with *Case Management* and *Threat Management.* The process and practice of responding to reports, made to or coming to the attention of management, regarding problematic behavior that has generated concerns under the organization's workplace violence prevention policy.

Important Terms, Definitions &Terminology (BSK-W Solutions)

- **Intimate Partner Violence:** Synonymous with *domestic violence*, *domestic abuse*, *spousal abuse*, and *family violence.* Can be broadly defined as a pattern of abusive behaviors in an intimate relationship (whether heterosexual or homosexual), including marriage, cohabitation, dating, family, or friendship. Intimate partner violence can consist of physical aggression, threats, stalking, sexual abuse, psychological abuse, neglect, economic deprivation, and any form of threatening, injurious, and violent acts.
- **Threat**: Any verbal or physical conduct that conveys an intent or is reasonably perceived to convey an intent to cause physical harm or to place someone in fear of physical harm.
- **Threat Management Team:** Synonymous with *Incident Management Team* and *Case Management Team*. A multi-disciplinary group of personnel selected by an organization to receive, respond to, and resolve reports of problematic behavior made under the organization's workplace violence prevention policy. For clarity and consistency, this Standard will employ the term "Threat Management Team," even though it is acknowledged that the Team will assemble to address some reports made under an organization's workplace violence prevention policy that do not ultimately involve an actual threat.
- **Violence Risk Assessment:** Also termed a *Threat Assessment* and *Risk Assessment*. A Violence Risk Assessment refers to the investigative and analytical process followed by a professional qualified by education, training, or experience to determine the nature and level of risk of violence presented by a person and the steps that could be taken to respond to, manage, and mitigate the risk. A violence risk assessment remains distinct from a *fitness for duty examination* (above) and a *violence risk screening* (below).
- **Violence Risk Screening**: A Violence Risk Screening refers to the investigative and analytic process followed by a Threat Management Team to make a gross and general determination of whether particular behavior should be viewed as generating a concern for possible violence and thereby should be treated under an organization's Threat Management protocols. A violence risk screening remains distinct from a *violence risk assessment* (above) which requires specifically-trained and qualified personnel.
- **Workplace Violence:** A spectrum of behaviors – including overt acts of violence, threats, and other conduct – that generates a reasonable concern for safety from violence, where a nexus exists between the behavior and the physical safety of employees and others (such as customers, clients, and business associates) on-site, or off-site when related to the organization.
- **Workplace Violence Prevention Policy:** A written policy adopted by an organization that strictly prohibits violence and threats affecting the workplace, as well as other behavior deemed inappropriate by the organization from a violence-prevention standpoint.
- **Workplace Violence Prevention and Intervention Program:** Synonymous with *Workplace Violence Program.* A coordinated collection of policies, procedures, and practices adopted by an organization to help prevent workplace violence and to assist the organization in effectively responding to reports of problematic behavior made under the organization's workplace violence prevention policy.


General Security Risk Assessment
Identify assets
Specify loss events
Frequency of events
Impact of events
Options to mitigate
Feasibility of options
Cost/benefit analysis
Decision
Reassessment

Important Terms, Definitions &Terminology (BSK-W Solutions)

Term	Definition
acceptable downtime	Maximum elapsed time between a disruption and restoration of needed operational capacity or capability.
activity	Process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products or services. NOTE: Examples of such processes include accounting, call center, information services, manufacturing, distribution, and other services.
alternate worksite	A work location, other than the primary location, to be used when the primary location is not accessible. [ASIS International Business Continuity Guideline: 2004]
auditor	A person with the competence to conduct an audit.
business continuity	Ability of an organization to operate at predefined levels following a disruptive event.
business continuity management (BCM)	Proactive set of planning, preparedness and related activities which are intended to restore an organization's critical business functions to pre- determined levels enabling the organization to operate despite serious disruptive events and recover to an operational state expeditiously.
business continuity plan (BCP)	A collection of procedures and information which is developed, tested and maintained in preparation for use in a disruptive event to continue operations at predefined levels following the event.
continual improvement	Recurring process of enhancing the security, preparedness, and continuity (SPC) management system in order to achieve improvements in overall SPC management performance consistent with the organization's SPC management policy NOTE: The process need not take place in all areas of activity simultaneously.
conformity	Fulfillment of a requirement.
crisis	An unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.

Important Terms, Definitions &Terminology (BSK-W Solutions)

Term	Definition
crisis management	Holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value- creating activities -- as well as effectively restoring operational capabilities. NOTE: Crisis management also involves the management of preparedness, mitigation response, continuity or recovery in the event of an incident -- as well as management of the overall program through training, rehearsals, and reviews to ensure the preparedness, response, and continuity plans stays current and up-to-date.
crisis management team	Group of individuals functionally responsible for directing the development and execution of the response and operational continuity plan, declaring an operational disruption or emergency/crisis situation and providing direction during the recovery process, both pre-and post-disruptive incident. NOTE: The crisis management team may include individuals from the organization as well as immediate and first responders, stakeholders, and other interested parties.
disaster	Event that causes significant damage to assets or loss of life.
disruption	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). NOTE: A disruption can be caused by either positive or negative factors that will disrupt normal functions, operations or processes.
downtime	Period of time when something is not in operation. NOTE: The allowable period of downtime is determined by the organizations obligations (e.g., customer and regulatory requirements).
emergency	Serious, unexpected, and precarious situation requiring immediate action.
evacuation	Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas. [ASIS International Business Continuity Guideline: 2004]

Important Terms, Definitions &Terminology (BSK-W Solutions)

Term	Definition
exercises	Evaluating management programs, rehearsing the roles of team members and staff, and testing the recovery or continuity of an organization's systems (e.g., technology, telephony, administration) to demonstrate management competence and capability. NOTE 1: Exercises include activities performed for the purpose of training and conditioning team members and personnel in appropriate responses with the goal of achieving maximum performance. NOTE 2: An exercise can involve invoking response and operational continuity procedures, but is more likely to involve the simulation of a response and/or operational continuity incident, announced or unannounced, in which participants role-play in order to assess what issues might arise, prior to a real invocation.
facility (infrastructure)	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.
first responder	A member of an emergency service who is first on the scene at a disruptive incident NOTE 1: Emergency services include any public or private service that deals with disruptions, such as the initial responding law enforcement officers, other public safety officials, emergency medical personnel, rescuers and/or other emergency response service providers.
hazard	Possible source of danger or conditions (physical or operational) that have a capacity to produce a particular type of adverse effect.
internal audit	Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the management system audit criteria set by the organization are fulfilled. NOTE: In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.
key performance indicator (KPI)	Metric used to evaluate factors that are crucial to the success of an organization or of a particular activity in which it engages. NOTE: A KPI is a metric which indicates how an organization is performing against its objectives.
loss	Being deprived of someone or something, of value.
management plan	Clearly defined and documented plan of action, typically covering the key personnel, resources, services, and actions needed to implement the incident management process.

Important Terms, Definitions &Terminology (BSK-W Solutions)

Term	Definition
mitigation	Limitation of any negative consequence of a particular incident.
mutual aid agreement	Written agreement between agencies, organizations, or jurisdictions to lend assistance across jurisdictional boundaries.
ORMS	Organizational resilience management system - Coordinated activities to direct and control an organization with regard to managing risk to enhance resilience and security in the organization and its supply chain. NOTE: Direction and control with regard to ORMS generally includes establishment of the policy, planning, and objectives directing operational processes and continual improvement.
ORMS objective	Something sought, or aimed for, related to managing risk to enhance resilience and security in the organization and its supply chain. NOTE 1: Quality objectives are generally based on the organization's quality policy. NOTE 2: Quality objectives are generally specified for relevant functions and levels in the organization.
ORMS policy	Overall intentions and direction of an organization related to managing risk to enhance resilience and security in the organization and its supply chain as formally expressed by top management. NOTE 1: Generally, the security and resilience policy is consistent with the overall policy of the organization, and provides a framework for the setting of security and resilience objectives. NOTE 2: ORMS principles presented in this Standard can form a basis for the establishment of a quality policy.
policy	Overall intentions and direction of an organization, as formally expressed by top management.
preparedness (readiness)	Activities, programs, and systems developed and implemented prior to an incident that may be used to support and enhance mitigation of, response to, and recovery from disruptions, disasters, or emergencies.
probability	A number between zero and one that shows how likely a certain event is.
procedure	An established or specified way to conduct an activity or a process.
process	Actions, changes or steps taken in order to achieve a particular end.
product	Goods and services that are the result of a process. NOTE: Typically, a product is an item or service that is produced to create value.

Term	Definition
recovery point objective	Point in time to which data or capacity of a process is in a known and valid or integral state can be restored from. This should be less than the maximum amount of loss tolerance and may be defined in hours or days.
recovery time objective (RTO)	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.
resilience	Absorptive and adaptive capacity in a complex and changing environment.
resources	Any asset (human, physical, information, or intangible), facilities, equipment, materials, products, or waste that has potential value and can be used.
response plan	Documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident.
response team	Group of individuals responsible for developing, executing, rehearsing, and maintaining the response plan, including the processes and procedures.
safety	Freedom from danger, risk, or injury.
security	The condition of being protected against risks, hazards, threats, or loss. NOTE 1: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside. NOTE 2: The term security means that something not only is secure, but that it has been secured.
target	Something you are trying to do or achieve with defined metrics.
testing	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: 2004]
threat	Potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community.