ISACA®

Trust in, and value from, information systems

CISM® Glossary

Term	Definition
Acceptable interruption window	The maximum period of time that a system can be unavailable before compromising the achievement of the enterprise's business objectives
Acceptable use policy	A policy that establishes an agreement between users and the enterprise and defines for all parties' the ranges of use that are approved before gaining access to a network or the Internet
Access path	The logical route that an end user takes to access computerized information Scope Note: Typically includes a route through the operating system, telecommunications software, selected application software and the access control system
Access rights	The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy
Accountability	The ability to map a given activity or event back to the responsible party
Administrative control	The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies
Adware	A software package that automatically plays, displays or downloads advertising material to a computer after the software is installed on it or while the application is being used Scope Note: In most cases, this is done without any notification to the user or without the user’s consent. The term adware may also refer to software that displays advertisements, whether or not it does so with the user’s consent; such programs display advertisements as an alternative to shareware registration fees. These are classified as adware in the sense of advertising supported software, but not as spyware. Adware in this form does not operate surreptitiously or mislead the user, and it provides the user with a specific service.
Alert situation	The point in an emergency procedure when the elapsed time passes a threshold and the interruption is not resolved. The enterprise entering into an alert situation initiates a series of escalation steps.
Alternate facilities	Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed Scope Note: Includes other buildings, offices or data processing centers
Alternate process	Automatic or manual process designed and established to continue critical business processes from point-of-failure to return-to-normal

Term	Definition
Antivirus software	An application software deployed at multiple points in an IT architecture It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected
Application controls	The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved
Application layer	In the Open Systems Interconnection (OSI) communications model, the application layer provides services for an application program to ensure that effective communication with another application program in a network is possible. Scope Note: The application layer is not the application that is doing the communication; a service layer that provides these services.
Application service provider (ASP)	Also known as managed service provider (MSP), it deploys, hosts and manages access to a packaged application to multiple parties from a centrally managed facility. Scope Note: The applications are delivered over networks on a subscription basis.
Architecture	Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support enterprise objectives
Benchmarking	A systematic approach to comparing enterprise performance against peers and competitors in an effort to learn the best ways of conducting business Scope Note: Examples include benchmarking of quality, logistic efficiency and various other metrics.
Bit-stream image	Bit-stream backups, also referred to as mirror image backups, involve the backup of all areas of a computer hard disk drive or other type of storage media. Scope Note: Such backups exactly replicate all sectors on a given storage device including all files and ambient data storage areas.
Brute force attack	Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found
Business case	Documentation of the rationale for making a business investment, used both to support a business decision on whether to proceed with the investment and as an operational tool to support management of the investment through its full economic life cycle
Business dependency assessment	A process of identifying resources critical to the operation of a business process

Term	Definition
Business impact analysis/assessment (BIA)	Evaluating the criticality and sensitivity of information assets An exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and the supporting system Scope Note: This process also includes addressing: -Income loss -Unexpected expense -Legal issues (regulatory compliance or contractual) -Interdependent processes -Loss of public reputation or public confidence
Chain of custody	A legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law. Scope Note: Includes documentation as to who had access to the evidence and when, as well as the ability to identify evidence as being the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on the ability to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence, so it cannot be changed, and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.
Change management	A holistic and proactive approach to managing the transition from a current to a desired organizational state, focusing specifically on the critical human or "soft" elements of change Scope Note: Includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives), organizational design, stakeholder management, human resources (HR) policies and procedures, executive coaching, change leadership training, team building and communication planning and execution
Chief executive officer (CEO)	The highest ranking individual in an enterprise
Chief financial officer (CFO)	The individual primarily responsible for managing the financial risk of an enterprise
Chief information officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy, aligning IT and business strategies, and planning, resourcing and managing the delivery of IT services, information and the deployment of associated human resources Scope Note: In some cases, the CIO role has been expanded to become the chief knowledge officer (CKO) who deals in knowledge, not just information. Also see chief technology officer (CTO).

Term	Definition
Chief technology officer (CTO)	The individual who focuses on technical issues in an enterprise Scope Note: Often viewed as synonymous with chief information officer (CIO)
Computer emergency response team (CERT)	A group of people integrated at the enterprise with clear lines of reporting and responsibilities for standby support in case of an information systems emergency This group will act as an efficient corrective control, and should also act as a single point of contact for all incidents and issues related to information systems.
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information
Control	The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature. Scope Note: Also used as a synonym for safeguard or countermeasure. See also Internal control.
Countermeasure	Any process that directly reduces a threat or vulnerability
Criticality analysis	An analysis to evaluate resources or business functions to identify their importance to the enterprise, and the impact if a function cannot be completed or a resource is not available
Cybercop	An investigator of activities related to computer crime
Damage evaluation	The determination of the extent of damage that is necessary to provide for an estimation of the recovery time frame and the potential loss to the enterprise
Data classification	The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the enterprise.
Data Encryption Standard (DES)	An algorithm for encoding binary data Scope Note: It is a secret key cryptosystem published by the National Bureau of Standards (NBS), the predecessor of the US National Institute of Standards and Technology (NIST). DES and its variants has been replaced by the Advanced Encryption Standard (AES)
Data leakage	Siphoning out or leaking information by dumping computer files or stealing computer reports and tapes
Data normalization	A structured process for organizing data into tables in such a way that it preserves the relationships among the data
Data warehouse	A generic term for a system that stores, retrieves and manages large volumes of data Scope Note: Data warehouse software often includes sophisticated comparison and hashing techniques for fast searches as well as for advanced filtering.
Decentralization	The process of distributing computer processing to different locations within an enterprise
Decryption key	A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption

Term	Definition
Defense in depth	The practice of layering defenses to provide added protection Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an enterprise's computing and information resources.
Degauss	The application of variable levels of alternating current for the purpose of demagnetizing magnetic recording media Scope Note: The process involves increasing the alternating current field gradually from zero to some maximum value and back to zero, leaving a very low residue of magnetic induction on the media. Degauss loosely means to erase.
Digital code signing	The process of digitally signing computer code to ensure its integrity
Disaster recovery plan (DRP) desk checking	Typically a read-through of a disaster recovery plan (DRP) without any real actions taking place Scope Note: Generally involves a reading of the plan, discussion of the action items and definition of any gaps that might be identified
Disaster recovery plan (DRP)	A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster
Disaster recovery plan (DRP) walk-through	Generally a robust test of the recovery plan requiring that some recovery activities take place and are tested A disaster scenario is often given and the recovery teams talk through the steps that they would need to take to recover. As many aspects of the plan as possible should be tested
Discretionary access control (DAC)	A means of restricting access to objects based on the identity of subjects and/or groups to which they belong Scope Note: The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
Disk mirroring	The practice of duplicating data in separate volumes on two hard disks to make storage more fault tolerant. Mirroring provides data protection in the case of disk failure because data are constantly updated to both disks.
Dual control	A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource so that no single entity acting alone can access that resource
Due care	The level of care expected from a reasonable person of similar competency under similar conditions
Due diligence	The performance of those actions that are generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review and/or analysis
Enterprise governance	A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly
Exposure	The potential loss to an area due to the occurrence of an adverse event
Fall-through logic	An optimized code based on a branch prediction that predicts which way a program will branch when an application is presented
Firewall	A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet

Term	Definition
Forensic examination	The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise
Guideline	A description of a particular way of accomplishing something that is less prescriptive than a procedure
Honeypot	A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems Scope Note: Also known as "decoy server"
Hot site	A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster
Hypertext Transfer Protocol (HTTP)	A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit hypertext markup language (HTML), extensible markup language (XML) or other pages to client browsers
Impact analysis	A study to prioritize the criticality of information resources for the enterprise based on costs (or consequences) of adverse events In an impact analysis, threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames. This analysis is the basis for establishing the recovery strategy.
Incident	Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service
Incident response	The response of an enterprise to a disaster or other significant event that may significantly affect the enterprise, its people, or its ability to function productively An incident response may include evacuation of a facility, initiating a disaster recovery plan (DRP), performing damage assessment, and any other measures necessary to bring an enterprise to a more stable status.
Information security	Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)
Information security governance	The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly
Information security program	The overall combination of technical, operational and procedural measures and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis
Information systems (IS)	The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies Scope Note: Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.

Term	Definition
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
Internet service provider (ISP)	A third party that provides individuals and enterprises with access to the Internet and a variety of other Internet-related services
Interruption window	The time that the company can wait from the point of failure to the restoration of the minimum and critical services or applications After this time, the progressive losses caused by the interruption are excessive for the enterprise.
Intrusion detection	The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack
Intrusion detection system (IDS)	Inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack
IT governance	The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise’s IT sustains and extends the enterprise's strategies and objectives
IT steering committee	An executive-management-level committee that assists in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects, and focuses on implementation aspects
IT strategic plan	A long-term plan (i.e., three- to five-year horizon) in which business and IT management cooperatively describe how IT resources will contribute to the enterprise’s strategic objectives (goals)
IT strategy committee	A committee at the level of the board of directors to ensure that the board is involved in major IT matters and decisions Scope Note: The committee is primarily accountable for managing the portfolios of IT-enabled investments, IT services and other IT resources. The committee is the owner of the portfolio.
Key goal indicator (KGI)	A measure that tells management, after the fact, whether an IT process has achieved its business requirements; usually expressed in terms of information criteria
Key performance indicator (KPI)	A measure that determines how well the process is performing in enabling the goal to be reached Scope Note: A lead indicator of whether a goal will likely be reached, and a good indicator of capabilities, practices and skills. It measures an activity goal, which is an action that the process owner must take to achieve effective process performance.
Key risk indicator (KRI)	A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk Scope Note: See also Risk Indicator.
Mail relay server	An electronic mail (e-mail) server that relays messages so that neither the sender nor the recipient is a local user
Mandatory access control (MAC)	A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf
Maximum tolerable outages (MTO)	Maximum time that an enterprise can support processing in alternate mode

Term	Definition
Message authentication code	An American National Standards Institute (ANSI) standard checksum that is computed using Data Encryption Standard (DES)
Metric	A quantifiable entity that allows the measurement of the achievement of a process goal Scope Note: Metrics should be SMART--specific, measurable, actionable, relevant and timely. Complete metric guidance defines the unit used, measurement frequency, ideal target value (if appropriate) and also the procedure to carry out the measurement and the procedure for the interpretation of the assessment.
Mirrored site	An alternate site that contains the same information as the original Scope Note: Mirrored sites are set up for backup and disaster recovery and to balance the traffic load for numerous download requests. Such download mirrors are often placed in different locations throughout the Internet.
Mobile site	The use of a mobile/temporary facility to serve as a business resumption location The facility can usually be delivered to any site and can house information technology and staff.
Monitoring policy	Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted
Nonintrusive monitoring	The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities
Nonrepudiation	The assurance that a party cannot later deny originating data; provision of proof of the integrity and origin of the data and that can be verified by a third party Scope Note: A digital signature can provide non-repudiation.
Outcome measure	Represents the consequences of actions previously taken; often referred to as a lag indicator Scope Note: Outcome measure frequently focuses on results at the end of a time period and characterize historic performance. They are also referred to as a key goal indicator (KGI) and used to indicate whether goals have been met. These can be measured only after the fact and, therefore, are called "lag indicators."
Packet filtering	Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them, based on a list of rules
Passive response	A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action
Password cracker	A tool that tests the strength of user passwords by searching for passwords that are easy to guess It repeatedly tries words from specially crafted dictionaries and often also generates thousands (and in some cases, even millions) of permutations of characters, numbers and symbols.
Penetration testing	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers

Term	Definition
Policy	1. Generally, a document that records a high-level principle or course of action that has been decided on The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise’s management teams. Scope Note: In addition to policy content, policies need to describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured. 2. Overall intention and direction as formally expressed by management Scope Note: COBIT 5 perspective
Privacy	Freedom from unauthorized intrusion or disclosure of information about an individual
Procedure	A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.
Proxy server	A server that acts on behalf of a user Scope Note: Typical proxies accept a connection from a user, make a decision as to whether the user or client IP address is permitted to use the proxy, perhaps perform additional authentication, and complete a connection to a remote destination on behalf of the user.
Reciprocal agreement	Emergency processing agreement between two or more enterprises with similar equipment or applications Scope Note: Typically, participants of a reciprocal agreement promise to provide processing time to each other when an emergency arises.
Recovery action	Execution of a response or task according to a written procedure
Recovery point objective (RPO)	Determined based on the acceptable data loss in case of a disruption of operations It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.
Recovery time objective (RTO)	The amount of time allowed for the recovery of a business function or resource after a disaster occurs
Redundant site	A recovery strategy involving the duplication of key IT components, including data or other key business processes, whereby fast recovery can take place
Resilience	The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect
Return on investment (ROI)	A measure of operating performance and efficiency, computed in its simplest form by dividing net income by the total investment over the period being considered

Term	Definition
Risk assessment	A process used to identify and evaluate risk and its potential effects Scope Note: Includes assessing the critical functions necessary for an enterprise to continue business operations, defining the controls in place to reduce enterprise exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.
Risk avoidance	The process for systematically avoiding risk, constituting one approach to managing risk
Risk mitigation	The management of risk through the use of countermeasures and controls
Risk tolerance	The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives
Risk transfer	The process of assigning risk to another enterprise, usually through the purchase of an insurance policy or by outsourcing the service
Risk treatment	The process of selection and implementation of measures to modify risk (ISO/IEC Guide 73:2002)
Root cause analysis	A process of diagnosis to establish the origins of events, which can be used for learning from consequences, typically from errors and problems
Security metrics	A standard of measurement used in management of security-related activities
Sensitivity	A measure of the impact that improper disclosure of information may have on an enterprise
Service delivery objective (SDO)	Directly related to the business needs, SDO is the level of services to be reached during the alternate process mode until the normal situation is restored
Service level agreement (SLA)	An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured
Sniffing	The process by which data traversing a network are captured or monitored
Social engineering	An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information
Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system
Threat	Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm Scope Note: A potential cause of an unwanted incident (ISO/IEC 13335)
Threat event	Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm
Two-factor authentication	The use of two independent mechanisms for authentication, (e.g., requiring a smart card and a password) typically the combination of something you know, are or have
Virtual private network (VPN)	A secure private network that uses the public telecommunications infrastructure to transmit data Scope Note: In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.
Virus signature file	The file of virus patterns that are compared with existing files to determine whether they are infected with a virus or worm

Term	Definition
Vulnerability	A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events
Vulnerability analysis	A process of identifying and classifying vulnerabilities
Warm site	Similar to a hot site but not fully equipped with all of the necessary hardware needed for recovery
Web hosting	The business of providing the equipment and services required to host and maintain files for one or more web sites and provide fast Internet connections to those sites Scope Note: Most hosting is "shared," which means that web sites of multiple companies are on the same server to share/reduce costs.
Web server	Using the client-server model and the World Wide Web's HyperText Transfer Protocol (HTTP), Web Server is a software program that serves web pages to users.
Worm	A programmed network attack in which a self-replicating program does not attach itself to programs, but rather spreads independently of users’ action