

CISM Glossary 1 June 2008

Term	Definition
Acceptable Interruption Window	The maximum period of time that a system can be unavailable before compromising the achievement of the organization's business objectives.
Acceptable Use Policy	A policy that establishes an agreement between users and the organization and defines for all parties' ranges of use that are approved before gaining access to a network or the Internet.
Access Path	The logical route an end user takes to access computerized information. Scope Note: Typically, an access path includes a route through the operating system, telecommunications software, selected application software and the access control system.
Access Rights	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 Controls	The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies.
Alert Situation	The point in an emergency procedure when the elapsed time passes a threshold and the interruption is not resolved. The organization 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: This includes other buildings, offices or data processing centers.
Alternate Process	Automatic or manual processes designed and established to continue critical business processes from point-of-failure to return-to-normal.
Antivirus Software	An application software deployed at multiple points in an IT architecture and is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected.
Application Control	'Manual or programmed activities intended to ensure the completeness and accuracy of records and the validity of entries made. The objectives of application controls are to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from manual and programmed processing.
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; it is 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.
Backup Center	An alternate facility to continue IT/IS operations when the primary DP center is unavailable.
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.

Term	Definition
Business Dependency Assessment	A process of identifying resources critical to the operation of a business process.
Business Impact Analysis/Assessment (BIA)	<p>Evaluating the criticality and sensitivity of information assets. An exercise that determines the impact of losing the support of any resource to an organization, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting system.</p> <p>Scope Note: This process also includes addressing:</p> <ul style="list-style-type: none"> -Income loss -Unexpected expense -Legal issues (regulatory compliance or contractual) -Interdependent processes -Loss of public reputation or public confidence
Chain of Custody	<p>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.</p> <p>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.</p>
Confidentiality	The protection of sensitive or private information from unauthorized disclosure.
Control Center	Hosts the recovery meetings where disaster recovery operations are managed.
Controls	The policies, procedures, practices and organizational structures designed to provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented or detected.
COSO	Committee of Sponsoring Organizations of the Treadway Commission.
Countermeasure	Scope Note: Its 1992 report "Internal Control--Integrated Framework" is an internationally accepted standard for corporate governance. See www.coso.org .
Criticality Analysis	Any process that directly reduces a threat or vulnerability.
Cybercops	An analysis to evaluate resources or business functions to identify their importance to the organization, and the impact if a function cannot be completed or a resource is not available.
Damage Evaluation	An investigator of computer-crime-related activities.
Data Classification	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 organization.
Data Encryption Standard (DES)	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 organization.
Data Normalization	An algorithm for encoding binary data.
Data Warehouse	Scope Note: It is a private key cryptosystem published by the National Bureau of Standards (NBS), the predecessor of the US National Institute of Standards and Technology (NIST). DES was defined as a Federal Information Processing Standard (FIPS) in 1976 and has been used commonly for data encryption in the forms of software and hardware implementation.
Data Warehouse	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.
Data Warehouse	Scope Note: Data warehouse software often includes sophisticated comparison and hashing techniques for fast searches, as well as advanced filtering.

Term	Definition
Decentralization	The process of distributing computer processing to different locations within an organization.
Decryption Key	A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption.
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 organization'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 Declaration	The communication to appropriate internal and external parties that the disaster recovery plan is being put into operation.
Disaster Notification Fee	The fee the recovery site vendor charges when the customer notifies them that a disaster has occurred and the recovery site is required. Scope Note: The fee is implemented to discourage false disaster notifications.
Disaster Recovery Plan	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 Desk Checking	Typically a read-through of a disaster recovery plan without any real actions taking place. Scope Note: It generally involves a reading of the plan, discussion of the action items and definition of any gaps that might be identified.
Disaster Recovery Plan 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 they would need to take to recover. As many aspects of the plan should be tested as possible.
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.
Domain Name Server (DNS)	A network service based on a hierarchical database system distributed across the Internet that translates the web address to IP addresses and vice versa.
Dual Control	A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such 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.
Exposure	The potential loss to an area due to the occurrence of an adverse event.
External Storage	The location that contains the backup copies to be used in case recovery or restoration is required in the event of a disaster.
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.
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".

Term	Definition
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 HTML, XML or other pages to the client browsers.
Impact Analysis	An impact analysis is a study to prioritize the criticality of information resources for the organization 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.
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 risks are 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.
Integrity	The accuracy, completeness and validity of information.
Internet Service Provider (ISP)	A third party that provides individuals and organizations access to the Internet and a variety of other Internet-related services.
Interruption Window	The time 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 organization.
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)	An IDS inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack.
ISO/IEC 17799	This standard defines information's confidentiality, integrity and availability controls in a comprehensive information security management system. Scope Note: Originally released as part of the British Standard for Information Security in 1999 and then as the Code of Practice for Information Security Management in October 2000, it was elevated by the International Organization for Standardization (ISO) to an international code of practice for information security management. The latest version is ISO/IEC 17799:2005.
IT Steering Committee	An executive management level committee that assists the executive in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects and focuses on implementation aspects.
Mail Relay Server	An 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.
Masqueraders	Attackers that penetrate systems by using the identity of legitimate users and their logon credentials.
Maximum Tolerable Outages (MTO)	Maximum time the organization can support processing in alternate mode.
Message Authentication Code	An ANSI standard checksum that is computed using Data Encryption Standard (DES).
Mirrored Site	An alternate site that contains the same information as the original. Scope note: Mirror sites are set up for backup and disaster recovery as well as 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. They 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 can be verified by a third party. Scope Note: A digital signature can provide non-repudiation.

Term	Definition
Offline Files	Computer file storage media not physically connected to the computer; typically tapes or tape cartridges used for backup purposes.
Open Source Security Testing Methodology	An open and freely available methodology and manual for security testing.
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 searching for passwords that are easy to guess by repeatedly trying words from specially crafted dictionaries and often also by generating 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.
Policies	High-level statements of management intent and direction.
Privacy	Freedom from unauthorized intrusion or disclosure of information about individuals.
Procedures	A detailed description of the steps necessary to perform specific operations in conformance with applicable standards.
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 or not 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 agreements between two or more organizations 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 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 information technology components, including data or other key business processes, where by 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.
Risk Assessment	A process used to identify and evaluate risks and their potential effects. Scope Note: Risk assessment includes assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.
Risk Avoidance	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 Transfer	The process of assigning risk to another organization, usually through the purchase of an insurance policy or outsourcing the service.
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 organization.
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.

Term	Definition
Shell Programming	<p>A script written for the shell, or command line interpreter, of an operating system. It is often considered a simple domain-specific programming language.</p> <p>Scope Note: Typical operations performed by shell scripts include file manipulation, program execution and printing text. Usually, shell script refers to scripts written for a Unix shell, while COMMAND.COM (DOS) and cmd.exe (Windows) command line scripts are usually called batch files. Many shell script interpreters double as command line interface such as the various Unix shells, Windows PowerShell or the MS-DOS COMMAND.COM. Others, such as AppleScript, add scripting capability to computing environments lacking a command line interface. Other examples of programming languages primarily intended for shell scripting include digital command language (DCL) and job control language (JCL).</p>
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.
Split Knowledge	A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items; a condition under which two or more entities separately have key components that individually convey no knowledge of the plain text key that will be produced when the key components are combined in the cryptographic module.
Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system.
Threat Analysis	<p>An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against organization assets.</p> <p>Scope Note: The threat analysis usually also defines the level of threat and the likelihood of it materializing.</p>
Two-factor Authentication	The use of two independent mechanisms for authentication, for example, requiring a smart card and a password. Typically the combination of something you know, are or have.
Virtual Private Network (VPN)	<p>A secure private network that uses the public telecommunications infrastructure to transmit data.</p> <p>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.</p>
Virus Signature Files	The file of virus patterns that are compared with existing files to determine if they are infected with a virus or worm.
Warm Site	Similar to a hot site; however, it is not fully equipped with all necessary hardware needed for recovery.
Web Hosting	<p>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.</p> <p>Scope Note: Most hosting is "shared" which means that web sites of multiple companies are on the same server to share/reduce costs.</p>
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	Programmed network attacks in which a self-replicating program does not attach itself to programs, but rather spreads independently of users' actions.