

CISA Glossary 1 June 2008

Term	Definition
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 Control	Refers to the processes, rules and deployment mechanisms which control access to information systems, resources and physical access to premises.
Access Control List (ACL)	An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals. Scope Note: Access Control Lists are also referred to as access control tables.
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.
Alternative Routing	A service that allows the option of having an alternate route to complete a call when the marked destination is not available. Scope Note: In signaling, alternate routing is the process of allocating substitute routes for a given signaling traffic stream in case of failure(s) affecting the normal signaling links or routes of that traffic stream.
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	A computer program or set of programs that perform the processing of records for a specific function. Scope Note: An application program contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort.
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 Programming Interface (API)	A set of routines, protocols and tools referred to as "building blocks" used in business application software development. Scope Note: A good API makes it easier to develop a program by providing all the building blocks related to functional characteristics of an operating system, which applications need to specify when, for example, interfacing with an operating system (e.g., provided by MS-Windows, different versions of UNIX). A programmer would utilize these APIs in developing applications that can operate effectively and efficiently on the platform chosen.

Term	Definition
Arithmetic-Logic Unit (ALU)	The area of the central processing unit that performs mathematical and analytical operations.
Asymmetric Key (Public Key)	A technology for scrambling data content using one key for encryption and another for decryption.
Attribute Sampling	An audit technique used to select items from a population for audit testing purposes based on selecting all those items that have certain attributes or characteristics (such as all items over a certain size).
Audit Evidence	Information used to support the audit opinion.
Audit Objective	The specific goal(s) of an audit. Scope Note: 'These often center on substantiating the existence of internal controls to minimize business risk.
Audit Plan	<p>1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion.</p> <p>Scope Note: The plan includes the areas to be audited, the type of work planned, the high level objectives and scope of the work, and topics such as budget, resource allocation, schedule dates, type of report and its intended audience and other general aspects of the work.</p> <p>2. A high level description of the audit work to be performed in a certain period of time.</p>
Audit Program	A step-by-step set of audit procedures and instructions that should be performed to complete an audit.
Audit Risk	The probability that information or financial reports may contain material errors and that the auditor may not detect an error that has occurred.
Audit Trail	A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source.
Auditability	The level to which transactions can be traced and audited through a system.
Authentication	<p>1. The act of verifying the identity of a user.</p> <p>Scope Note: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.</p> <p>2. The user's eligibility to access computerized information.</p>
Backup	Files, equipment, data and procedures available for use in the event of a failure or loss, if the originals are destroyed or out of service.
Balanced Scorecard	The balanced scorecard, developed by Robert S. Kaplan and David P. Norton, is a coherent set of performance measures organized into four categories. It includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives.
Bandwidth	The range between the highest and lowest transmittable frequencies. It equates to the transmission capacity of an electronic line and is expressed in bytes per second or Hertz (cycles per second).

Term	Definition
Batch Control	<p>Correctness checks built into data processing systems and applied to batches of input data, particularly in the data preparation stage.</p> <p>Scope Note: There are two main forms of batch controls: sequence control, which involves numbering the records in a batch consecutively so that the presence of each record can be confirmed, and control total, which is a total of the values in selected fields within the transactions.</p>
Batch Processing	<p>The processing of a group of transactions at the same time.</p> <p>Scope Note: Transactions are collected and processed against the master files at a specified time.</p>
Benchmark	<p>A test that has been designed to evaluate the performance of a system.</p> <p>In a benchmark test, a system is subjected to a known workload and the performance of the system against this workload is measured.</p> <p>Scope Note: Typically, the purpose is to compare the measured performance with that of other systems that have been subject to the same benchmark test.</p>
Benchmarking	<p>A systematic approach to comparing an organization's performance against peers and competitors in an effort to learn the best ways of conducting business.</p> <p>Scope Note: Examples include: benchmarking of quality, logistical efficiency and various other metrics.</p>
Biometrics	<p>A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint.</p>
Black Box Testing	<p>A testing approach which focuses on the functionality of the application or product and does not require knowledge of the code intervals.</p>
Bus	<p>Common path or channel between hardware devices.</p> <p>Scope Note: A bus can be between components internal to a computer or between external computers in a communications network.</p>
Bus Configuration	<p>All devices (nodes) are linked along one communication line where transmissions are received by all attached nodes.</p> <p>Scope Note: 'This architecture is reliable in very small networks, as well as easy to use and understand. This configuration requires the least amount of cable to connect the computers together and, therefore, is less expensive than other cabling arrangements. It is also easy to extend, and two cables can be easily joined with a connector to make a longer cable for more computers to join the network. A repeater can also be used to extend a bus configuration.</p>
Business Case	<p>Documentation of the rationale for making a business investment, used both to support a business decision on whether to proceed or not with the investment and as an operational tool to support management of the investment through its full economic life cycle.</p>
Business Continuity Plan (BCP)	<p>Plan used by organization to respond to disruption of critical business processes. Depends on contingency plan for restoration of critical systems.</p>

Term	Definition
Business Impact Analysis (BIA)	<p>A process to determine the impact of losing the support of any resource.</p> <p>Scope Note: The business impact analysis assessment study will establish the escalation of that loss overtime. It is predicated on the fact that senior management, when provided reliable data to document the potential impact of a lost resource, can make the appropriate decision.</p>
Business Process Reengineering (BPR)	<p>The thorough analysis and significant redesign of business processes and management systems to establish a better performing structure, more responsive to the customer base and market conditions, while yielding material cost savings.</p>
Bypass Label Processing (BLP)	<p>A technique of reading a computer file while bypassing the internal file/data set label. This process could result in bypassing of the security access control system.</p>
Capability Maturity Model (CMM)	<p>Contains the essential elements of effective processes for one or more disciplines. It also describes an evolutionary improvement path from ad hoc, immature processes to disciplined, mature processes with improved quality and effectiveness.</p>
Certificate Authority (CA)	<p>A trusted third party that serves authentication infrastructures or organizations and registers entities and issues them certificates.</p>
Certificate Revocation List (CRL)	<p>An instrument for checking the continued validity of the certificates for which the certification authority (CA) has responsibility.</p> <p>Scope Note: CRL details digital certificates that are no longer valid. The time gap between two updates is very critical and is also a risk in digital certificates verification.</p>
Change Management	<p>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.</p> <p>Scope Note: Change management includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives), organizational design, stakeholder management, human resource policies and procedures, executive coaching, change leadership training, team building and communications planning and execution.</p>
Check Digit	<p>A numeric value, which has been calculated mathematically, is added to data to ensure that original data have not been altered or that an incorrect, but valid match has occurred.</p> <p>Scope Note: Check digit control is effective in detecting transposition and transcription errors.</p>
Ciphertext	<p>Information generated by an encryption algorithm to protect the plaintext and is unintelligible to the unauthorized reader.</p>
Client-server	<p>A group of computers connected by a communications network, where the client is the requesting machine and the server is the supplying machine.</p> <p>Scope Note: Software is specialized at both ends. Processing may take place on either the client or the server but it is transparent to the user.</p>

Term	Definition
Cold Site	<p>An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place.</p> <p>Scope Note: The site is ready to receive the necessary replacement computer equipment in the event the users have to move from their main computing location to the alternative computer facility.</p>
Compensating Control	<p>An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions.</p>
Completely Connected (Mesh) Configuration	<p>A network topology in which devices are connected with many redundant interconnections between network nodes (primarily used for backbone networks).</p>
Compliance Testing	<p>Tests of control designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period.</p>
Computer Emergency Response Team (CERT)	<p>A group of people integrated at the organization 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.</p>
Computer-Aided Software Engineering (CASE)	<p>The use of software packages that aid in the development of all phases of an information system.</p> <p>Scope Note: System analysis, design programming and documentation are provided. Changes introduced in one CASE chart will update all other related charts automatically. CASE can be installed on a microcomputer for easy access.</p>
Computer-Assisted Audit Technique (CAATs)	<p>Any automated audit technique, such as generalized audit software, test data generators, computerized audit programs and specialized audit utilities.</p>
Concurrency Control	<p>Refers to a class of controls used in database management systems (DBMS) to ensure that transactions are processed in an atomic, consistent, isolated and durable manner (ACID). This implies that only serial and recoverable schedules are permitted, and that committed transactions are not discarded when undoing aborted transactions.</p>
Configuration Management	<p>The control of changes to a set of configuration items over a system life cycle.</p>
Contingency Planning	<p>Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances.</p>
Continuous Improvement	<p>The goals of continuous improvement (Kaizen) include the elimination of waste, defined as "activities that add cost but do not add value;" just-in-time delivery; production load leveling of amounts and types; standardized work; paced moving lines; right-sized equipment.</p> <p>Scope Note: A closer definition of the Japanese usage of Kaizen is "to take it apart and put back together in a better way." What is taken apart is usually a process, system, product or service. Kaizen is a daily activity whose purpose goes beyond improvement. It is also a process that, when done correctly, humanizes the workplace, eliminates hard work (both mental and physical), and teaches people how to do rapid experiments using the scientific method and how to learn to see and eliminate waste in business processes.</p>

Term	Definition
Control Objective	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process.
Control Practice	Key control mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business.
Control Risk	The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls. (See also Inherent Risk)
Cookie	<p>A message kept in the web browser for the purpose of identifying users and possibly preparing customized web pages for them.</p> <p>Scope Note: For the first time a cookie is set, a user may be required to go through a registration process. Subsequent to this, whenever the cookie's message is sent to the server, a customized view, based on that user's preferences, can be produced. The browser's implementation of cookies has however brought several security concerns, allowing breaches of security and the theft of personal information (e.g., user passwords that validate the user's identity and enable restricted web services).</p>
Corrective Controls	Designed to correct errors, omissions and unauthorized uses and intrusions, once they are detected.
COSO	<p>Committee of Sponsoring Organizations of the Treadway Commission.</p> <p>Scope Note: Its 1992 report "Internal Control--Integrated Framework" is an internationally accepted standard for corporate governance. See www.coso.org.</p>
Critical Infrastructure	Systems whose incapacity or destruction would have a debilitating effect on the economic security of an organization, community or nation.
Critical Success Factors (CSFs)	Critical success factor; the most important issues or actions for management to achieve control over and within its IT processes.
Customer Relationship Management (CRM)	A way to identify, acquire and retain customers. CRM is also an industry term for software solutions that help an organization manage customer relationships in an organized manner.
Data Communications	The transfer of data between separate computer processing sites/devices using telephone lines, microwave and/or satellite links.
Data Custodian	Individuals and departments responsible for the storage and safeguarding of computerized data.
Data Leakage	Siphoning out or leaking information by dumping computer files or stealing computer reports and tapes.
Data Owner	Individuals, normally managers or directors, who have responsibility for the integrity, accurate reporting and use of computerized data.
Data Structure	The relationships among files in a database and among data items within each file.
Database	A stored collection of related data needed by organizations and individuals to meet their information processing and retrieval requirements.
Database Administrator (DBA)	<p>An individual or department responsible for the security and information classification of the shared data stored on a database system. This responsibility includes the design, definition and maintenance of the database.</p>
Database Management System (DBMS)	A software system that controls the organization, storage and retrieval of data in a database.
Decryption	A technique used to recover the original plaintext from the ciphertext such that it is intelligible to the reader. The decryption is a reverse process of the encryption.

Term	Definition
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 Signature	A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.
Disaster Recovery	Activities and programs designed to return the organization to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.
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 Tolerance	The time gap the business can accept the non-availability of IT facilities.
Discovery Sampling	A form of attribute sampling that is used to determine a specified probability of finding at least one example of an occurrence (attribute) in a population.
Diskless Workstations	A workstation or PC on a network that does not have its own disk, but instead, stores files on a network file server.
Domain Name System (DNS) Poisoning	Corrupts the table of an Internet server's DNS replacing an Internet address with the address of another vagrant or scoundrel address. Scope Note: If a Web user looks for the page with that address, the request is redirected by the scoundrel entry in the table to a different address. Cache poisoning differs from another form of DNS poisoning, in which the attacker spoofs valid e-mail accounts and floods the inboxes of administrative and technical contacts. Cache poisoning is related to URL poisoning or location poisoning, where an Internet user behavior is tracked by adding an identification number to the location line of the browser that can be recorded as the user visits successive pages on the site. Also called DNS cache poisoning or cache poisoning.
Duplex Routing	The method or communication mode of routing data over the communication network (also see half duplex and full duplex).
E-commerce	The processes by which organizations conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology. Scope Note: E-commerce encompasses both business-to-business (B2B) and business-to-consumer (B2C) e-commerce models, but does not include existing non-Internet e-commerce methods based on private networks such as EDI and SWIFT.
Edit Controls	Detects errors in the input portion of information that is sent to the computer for processing. The controls may be manual or automated and allow the user to edit data errors before processing.
Electronic Data Interchange (EDI)	The electronic transmission of transactions (information) between two organizations. EDI promotes a more efficient paperless environment. EDI transmissions can replace the use of standard documents, including invoices or purchase orders.
Encapsulation (objects)	Encapsulation is the technique used by layered protocols in which a lower layer protocol accepts a message from a higher layer protocol and places it in the data portion of a frame in the lower layer.
Encryption	The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext).

Term	Definition
Enterprise Resource Planning (ERP)	<p>An integrated system containing multiple business subsystems.</p> <p>Scope Note: Examples of enterprise resource planning include SAP, Oracle Financials and J.D. Edwards.</p>
Escrow Agreement	<p>A legal arrangement whereby an asset (often money, but sometimes other property such as art, a deed of title, web site, software source code or a cryptographic key) is delivered to a third party (called an escrow agent) to be held in trust or otherwise pending a contingency or the fulfillment of a condition or conditions in a contract.</p> <p>Scope Note: Upon the occurrence of the escrow agreement, the escrow agent will deliver the asset to the proper recipient; otherwise the escrow agent is bound by his/her fiduciary duty to maintain the escrow account. Source code escrow means deposit of the source code for the software into an account held by an escrow agent. Escrow is typically requested by a party licensing software (e.g., licensee or buyer), to ensure maintenance of the software. The software source code is released by the escrow agent to the licensee if the licensor (e.g., seller or contractor) files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.</p>
Evidence	<p>The information an auditor gathers in the course of performing an IS audit; relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support.</p>
Executable Code	<p>The machine language code that is generally referred to as the object or load module.</p>
Exposure	<p>The potential loss to an area due to the occurrence of an adverse event.</p>
Extensible Markup Language (XML)	<p>Promulgated through the World Wide Web Consortium, XML is a web-based application development technique that allows designers to create their own customized tags, thus, enabling the definition, transmission, validation and interpretation of data between applications and organizations.</p>
Fault Tolerance	<p>A system's level of resilience to seamlessly react from hardware and/or software failure.</p>
Feasibility Study	<p>A phase of an SDLC methodology that researches the feasibility and adequacy of resources for the development or acquisition of a system solution to a user need.</p>
Firewall	<p>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.</p>
Firmware	<p>Memory chips with embedded program code that hold their content when power is turned off.</p>
Generalized Audit Software (GAS)	<p>Multipurpose audit software that can be used for such general processes, such as record selection, matching, recalculation and reporting.</p>
Hardware	<p>The physical components of a computer system.</p>
Help Desk	<p>A service offered via phone/Internet by an organization to its clients or employees, which provides information, assistance, and troubleshooting advices regarding software, hardware, or networks.</p> <p>Scope Note: A help desk is staffed by people that can either resolve the problem on their own or escalate the problem to specialized personnel. A help desk is often equipped with dedicated CRM-type software that logs the problems and tracks them until they are solved.</p>

Term	Definition
Heuristic Filter	<p>A method often employed by antispam software to filter spam using criteria established in a centralized rule database.</p> <p>Scope Note: Every e-mail message is given a rank, based upon its header and contents, which is then matched against preset thresholds. A message that surpasses the threshold will be flagged as spam and discarded, returned to its sender or put in a spam directory for further review by the intended recipient.</p>
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 markup language (HTML)	A language designed for the creation of web pages with hypertext and other information to be displayed in a web browser; used to structure information--denoting certain text as headings, paragraphs, lists and so on--and can be used to describe, to some degree, the appearance and semantics of a document.
Impact Assessment	A review of the possible consequences of a risk.
Incident	A series of unexpected events that involves an attack or series of attacks (compromise and/or breach of security) at one or more sites.
Incident Response	The response of an organization to a disaster or other significant event that may significantly affect the organization, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.
Independence	<p>1. Self-governance.</p> <p>2. Freedom from conflict of interest and undue influence.</p> <p>Scope Note: The IS auditor should be free to make his/her own decisions, not influenced by the organization being audited and its people (managers and employers).</p>
Information Processing Facility (IPF)	The computer room and support areas.
Information Security	Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) 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 risks are managed appropriately and verifying that the enterprise's resources are used responsibly.
Inherent Risk	The risk that a material error could occur, assuming that there are no related internal controls to prevent or detect the error (Also see control risk).
Input Controls	Techniques and procedures used to verify, validate and edit data, to ensure that only correct data are entered into the computer.
Instant Messaging	<p>Instant messaging is an online mechanism or a form of real-time communication between two or more people based on typed text and multimedia data.</p> <p>Scope Note: Instant messaging text is conveyed via computers or another electronic device (e.g., cell phone or PDA) connected over a network, such as the Internet.</p>
Integrity	The accuracy, completeness and validity of information.

Term	Definition
Internal Control	The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.
Internet Packet (IP) Spoofing	An attack using packets with the spoofed source Internet packet (IP) addresses. Scope Note: This technique exploits applications that use authentication based on IP addresses. This technique also may enable an unauthorized user to gain root access on the target system.
ISO 9001:2000	Code of practice for quality management from the International Organization for Standardization (ISO). ISO 9001:2000, which specifies requirements for a quality management system for any organization that needs to demonstrate its ability to consistently provide product or service that meets particular quality targets.
IT Governance Framework	A model that integrates a set of guidelines, policies and methods that represent the organizational approach to the IT governance. Scope Note: Per COBIT 4.0, IT governance is the responsibility of the board of directors and executive management. It is an integral part of institutional governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives.
IT Incident	Any event that is not part of the ordinary operation of a service that causes, or may cause, an interruption to, or a reduction in, the quality of that service.
IT Infrastructure	The set of hardware, software and facilities that integrates an organizations' IT assets. Scope Note: Specifically, the equipment (including servers, routers, switches, and cabling), software, services and products used in storing, processing, transmitting and displaying all forms of information for the organization's users.
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	Committee at the level of the board of directors to ensure the board is involved in major IT matters/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.
ITIL	The UK Office of Government Commerce (OGC) IT Infrastructure Library. A set of guides on the management and provision of operational IT services.
Judgment Sampling	Any sample that is selected subjectively or in such a manner that the sample selection process is not random or the sampling results are not evaluated mathematically.
Key Goal Indicators (KGIs)	Key goal indicator; measures that tell management, after the fact, whether an IT process has achieved its business requirements, usually expressed in terms of information criteria.
Key Management Practices	Those management practices required to successfully execute business processes.
Key Performance Indicators (KPIs)	Measures that determine how well the process is performing in enabling the goal to be reached. Scope Note: KPIs are lead indicators of whether a goal will likely be reached, and are good indicators of capabilities, practices and skills. They measure the activity goals, which are the actions the process owner must take to achieve effective process performance.

Term	Definition
Librarian	The individual responsible for the safeguard and maintenance of all program and data files.
Licensing Agreement	A contract that establishes the terms and conditions under which a piece of software is being licensed (i.e., made legally available for use) from the software developer (owner) to the user.
Life Cycle	A series of stages that characterize the course of existence of an organizational investment (e.g., product, project, program).
Limit Check	Tests of specified amount fields against stipulated high or low limits of acceptability. Scope Note: When both high and low values are used, the test may be called a range check.
Local Area Network (LAN)	Communications networks that serve several users within a specified geographical area. Scope Note: Personal computer LANs function as distributed processing systems in which each computer in the network does its own processing and manages some of its data. Shared data are stored in a file server that acts as a remote disk drive for all users in the network.
Log	To record details of information or events in an organized record-keeping system, usually sequenced in the order they occurred.
Malware	Short for malicious software, malware is software designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Scope Note: Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, not really malicious although it is generally unwanted. However, spyware can also be used to gather information for identity theft or other clearly illicit purposes.
Mapping	Diagramming data that are to be exchanged electronically, including how it is to be used and what business management systems need it. Also see application tracing and mapping. Scope Note: Mapping is a preliminary step for developing an applications link.
Materiality	An auditing concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. An expression of the relative significance or importance of a particular matter in the context of the organization as a whole.
Maturity	In business, indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives.
Maturity Model	The Capability Maturity Model (CMM) for Software (CMM), from the Software Engineering Institute (SEI), is a model used by many organizations to identify best practices useful in helping them assess and increase the maturity of their software development processes. Scope Note: The CMM ranks software development organizations according to a hierarchy of five process maturity levels. Each level ranks the development environment according to its capability of producing quality software. A set of standards is associated with each of the five levels. The standards for level one describe the most immature or chaotic processes and the standards for level five describe the most mature or quality processes. 1) A model that indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives (2) A collection of instructions an organization can follow to gain better control over its software development process.

Term	Definition
Media Oxidation	<p>The deterioration of the media upon which data is digitally stored due to exposure to oxygen and moisture.</p> <p>Scope Note: Tapes deteriorating in a warm, humid environment are an example of media oxidation. Proper environmental controls should prevent, or significantly slow, this process.</p>
Middleware	<p>Another term for an application programmer interface (API). It refers to the interfaces that allow programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services.</p>
Mission-Critical Application	<p>An application that is vital to the operation of the organization. The term is very popular for describing the applications required to run the day-to-day business.</p>
Monetary Unit Sampling	<p>A sampling technique that estimates the amount of overstatement in an account balance.</p>
Network Administrator	<p>Responsible for planning, implementing and maintaining the telecommunications infrastructure, and also may be responsible for voice networks.</p> <p>Scope Note: For smaller organizations, the network administrator may also maintain a LAN and assist end users.</p>
Nondisclosure Agreement (NDA)	<p>A legal contract between at least two parties that outlines confidential materials the parties wish to share with one another for certain purposes, but wish to restrict from generalized use; a contract through which the parties agree not to disclose information covered by the agreement.</p> <p>Scope Note: Also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement. An NDA creates a confidential relationship between parties to protect any type of trade secret. An NDA can protect non-public business information. In the case of certain governmental entities, confidentiality of information other than trade secrets may be subject to statutory requirements, and in some cases may be required to be revealed to an outside party requesting the information. NDAs can be "mutual", meaning both parties are restricted in their use of the materials provided, or they can only restrict a single party.</p>
Normalization	<p>The elimination of redundant data.</p>
Object Code	<p>Machine-readable instructions produced from a compiler or assembler program that has accepted and translated the source code.</p>
Offsite Storage	<p>A facility located away from the building housing the primary information processing facility (IPF), used for storage of computer media such as offline backup data and storage files.</p>
Operating System	<p>A master control program that runs the computer and acts as a scheduler and traffic controller.</p> <p>Scope Note: The operating system is the first program copied into the computer's memory after the computer is turned on and must reside in memory at all times. It is the software that interfaces between the computer hardware (disk, keyboard, mouse, network, modem, printer) and the application software (word processor, spreadsheet, e-mail), which also controls access to the devices and is partially responsible for security components and sets the standards for the application programs that run in it.</p>
Operational Control	<p>These controls deal with the everyday operation of a company or organization to ensure all objectives are achieved.</p>
Outsourcing	<p>A formal agreement with a third party to perform IS or other business functions for an organization.</p>

Term	Definition
Packet	<p>Data unit that is routed from source to destination in a packet-switched network.</p> <p>Scope Note: A packet contains both routing information and data. Transmission Control Protocol/Internet Protocol (TCP/IP) is such a packet-switched network.</p>
Packet Switching	<p>The process of transmitting messages in convenient pieces that can be reassembled at the destination.</p>
Parity Check	<p>A general hardware control, which helps to detect data errors when data are read from memory or communicated from one computer to another.</p> <p>Scope Note: A 1-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, the computer reports an error. The probability of a parity check detecting an error is 50 percent.</p>
Password	<p>A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system.</p>
Penetration Testing	<p>A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers.</p>
Performance Drivers	<p>Measures that are considered the 'drivers' of lag indicators. They can be measured before the outcome is clear and, therefore, are called 'lead indicators'.</p> <p>Scope Note: There is an assumed relationship between the two that suggests that improved performance in a leading indicator will drive better performance in the lagging indicator. They are also referred to as key performance indicators (KPIs) and are used to indicate whether goals are likely to be met.</p>
Performance Testing	<p>Comparing the system's performance to other equivalent systems using well defined benchmarks.</p>
Personal Digital Assistant (PDA)	<p>Also called palmtop and pocket computer, these are handheld devices that provide computing, Internet, networking and telephone characteristics.</p>
Personal Identification Number (PIN)	<p>A type of password (i.e., a secret number assigned to an individual) that, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual.</p> <p>Scope Note: PINs have been adopted by financial institutions as the primary means of verifying customers in an electronic funds transfer system (EFTS).</p>
Phishing	<p>This is a type of e-mail attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering.</p> <p>Scope Note: Phishing attacks may take the form of masquerading as a lottery organization advising the recipient of a large win or the user's bank; in either case, the intent is to obtain account and PIN details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.</p>
Point-of-Sale (POS) Systems	<p>Enable the capture of data at the time and place of transaction.</p> <p>Scope Note: POS terminals may include use of optical scanners for use with bar codes or magnetic card readers for use with credit cards. POS systems may be online to a central computer or may use stand-alone terminals or microcomputers that hold the transactions until the end of a specified period when they are sent to the main computer for batch processing.</p>

Term	Definition
Policy	<p>Generally, a document that records a high-level principle or course of action which has been decided upon. A policy's 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.</p> <p>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</p>
Portfolio	A grouping of "objects of interest" (investment programs, IT services, IT projects, other IT assets or resources) managed and monitored to optimize business value. (The investment portfolio is of primary interest to Val IT. T service, project, asset and other resource portfolios are of primary interest to COBIT).
Preventive Controls	An internal control that is used to prevent undesirable events, errors and other occurrences that an organization has determined could have a negative material effect on a process or end product.
Privacy	Freedom from unauthorized intrusion or disclosure of information about individuals.
Problem Escalation Procedure	<p>The process of escalating a problem up from junior to senior support staff, and ultimately to higher levels of management.</p> <p>Scope Note: Problem escalation procedure is often used in help desk management, where an unresolved problem is escalated up the chain of command, until it is solved.</p>
Procedure	A document containing steps that specify how to achieve an activity. Procedures are defined as part of processes.
Procedures	A detailed description of the steps necessary to perform specific operations in conformance with applicable standards.
Process	<p>Generally, a collection of procedures influenced by the organization's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs.</p> <p>Scope Note: Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.</p>
Program Evaluation and Review Technique (PERT)	A project management technique used in the planning and control of system projects.
Project	A structured set of activities concerned with delivering a defined capability (that is necessary but not sufficient to achieve a required business outcome) to the enterprise based on an agreed-upon schedule and budget.
Project Portfolio	<p>The set of projects owned by a company.</p> <p>Scope Note: A project portfolio usually includes the main guidelines relative to each project including objectives, costs, timelines and other information specific to the project.</p>
Prototyping	<p>The process of quickly putting together a working model (a prototype) in order to test various aspects of a design, illustrate ideas or features and gather early user feedback.</p> <p>Scope Note: Prototyping uses programmed simulation techniques to represent a model of the final system to the user for advisement and critique. The emphasis is on end-user screens and reports. Internal controls are not a priority item since this is only a model.</p>

Term	Definition
Public Key Encryption	A cryptographic system that uses two keys. One is a public key, which is known to everyone, and the second is a private or secret key, which is only known to the recipient of the message.
Public Key Infrastructure	A series of processes and technologies for the association of cryptographic keys with the entity to whom those keys were issued.
Quality Assurance (QA)	A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. (ISO/IEC 24765)
Rapid Application Development	A methodology that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality by using a series of proven application development techniques, within a well-defined methodology.
Reciprocal Agreement	<p>Emergency processing agreements between two or more organizations with similar equipment or applications.</p> <p>Scope Note: Typically, participants of a reciprocal agreement promise to provide processing time to each other when an emergency arises.</p>
Recovery Point Objective (RPO)	The recovery point objective is determined based on the acceptable data loss in case of disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data. RPO effectively quantifies permissible amount of data loss in case of interruption.
Recovery Strategy	<p>An approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major outage.</p> <p>Scope Note: Plans and methodologies are determined by the organization's strategy. There may be more than one methodology or solution for an organization's strategy. Examples of methodologies and solutions include: contracting for hot site or cold site, building an internal hot site or cold site, identifying an alternate work area, a consortium or reciprocal agreement, contracting for mobile recovery or crate and ship, and many others.</p>
Redundant Array of Inexpensive Disks (RAID)	Provides performance improvements and fault-tolerant capabilities via hardware or software solutions, by writing to a series of multiple disks to improve performance and/or save large files simultaneously.
Reengineering	<p>A process involving the extraction of components from existing systems and restructuring these components to develop new systems or to enhance the efficiency of existing systems.</p> <p>Scope Note: Existing software systems can be modernized to prolong their functionality. An example of this is a software code translator that can take an existing hierarchical database system and transpose it to a relational database system. CASE includes a source code reengineering feature.</p>
Registration Authority (RA)	The individual or institution that validates and entity's proof of identity and ownership of a key pair.
Regression Testing	A testing technique used to retest earlier program abends or logical errors that occurred during the initial testing phase.
Request for Proposal (RFP)	A document distributed to software vendors requesting them to submit a proposal to develop or provide a software product.
Requirements Definition	<p>A technique used where the affected user groups define the requirements of the system for meeting the defined needs.</p> <p>Scope Note: Some of these requirements are business, regulatory, security as well as development related.</p>

Term	Definition
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.
Reverse Engineering	A software engineering technique whereby an existing application system code can be redesigned and coded using computer-aided software engineering (CASE) technology.
Ring Configuration	<p>Used in either token ring or FDDI networks, all stations (nodes) are connected to a multi-station access unit (MSAU), which physically resembles a star-type topology.</p> <p>Scope Note: A ring configuration is created when these MSAUs are linked together in forming a network. Messages in this network are sent in a deterministic fashion from sender and receiver via a small frame, referred to as a token ring. To send a message, a sender obtains the token with the right priority as the token travels around the ring, with receiving nodes reading those messages addressed to it.</p>
Risk	The combination of the probability of an event and its consequence. (ISO/IEC73)
Risk Analysis	<p>The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats.</p> <p>Scope Note: Risk analysis often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of such event.</p>
Risk Assessment	<p>A process used to identify and evaluate risks and their potential effects.</p> <p>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.</p>
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.
Rounding Down	A method of computer fraud involving a computer code that instructs the computer to remove small amounts of money from an authorized computer transaction by rounding down to the nearest whole value denomination and rerouting the rounded off amount to the perpetrator's account.
Router	<p>A networking device that can send (route) data packets from one local area network (LAN) or wide area network (WAN) to another, based on addressing at the network layer (Layer 3) in the OSI model.</p> <p>Scope Note: Networks connected by routers can use different or similar networking protocols. Routers usually are capable of filtering packets based on parameters, such as source addresses, destination addresses, protocol and network applications (ports).</p>
Run-to-Run Totals	Provide evidence that a program processes all input data and that it processed the data correctly.
Scheduling	A method used in the information processing facility (IPF) to determine and establish the sequence of computer job processing.

Term	Definition
Scope Creep	<p>Also called requirement creep, this refers to uncontrolled changes in a project's scope.</p> <p>Scope Note: Scope creep can occur when the scope of a project is not properly defined, documented and controlled. Typically, the scope increase consists of either new products or new features of already approved products. Hence, the project team drifts away from its original purpose. Because of one's tendency to focus on only one dimension of a project, scope creep can also result in a project team overrunning its original budget and schedule. For example, scope creep can be a result of poor change control, lack of proper identification of what products and features are required to bring about the achievement of project objectives in the first place, or a weak project manager or executive sponsor.</p>
Secure Sockets Layer (SSL)	<p>A protocol that is used to transmit private documents through the Internet.</p> <p>Scope Note: The SSL protocol uses a private key to encrypt the data that is to be transferred through the SSL connection.</p>
Security Administrator	<p>The person responsible for implementing, monitoring and enforcing security rules established and authorized by management.</p>
Security Awareness	<p>The extent to which every member of an organization and every other individual who potentially has access to the organization's information understand:</p> <ul style="list-style-type: none"> -Security and the levels of security appropriate to the organization -The importance of security and consequences of a lack of security -Their individual responsibilities regarding security (and act accordingly). <p>'This definition is based on the definition for IT security awareness as defined in Implementation Guide: How to Make Your Organization Aware of IT Security, European Security Forum (ESF), London, UK, 1993)</p>
Security Policy	<p>A high-level document representing an organization's information security philosophy and commitment.</p>
Security Procedures	<p>The formal documentation of specific operational steps and processes that specify how security goals and objectives set forward in the security policy and standards are to be achieved.</p>
Security Testing	<p>Ensuring the modified or new system includes appropriate controls and does not introduce any security holes that might compromise other systems or misuses of the system or its information.</p>
Segregation/Separation of Duties	<p>A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals responsibility for initiating and recording transactions and custody of assets to separate individuals.</p> <p>Scope Note: Segregation and separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.</p>
Service Level Agreement (SLA)	<p>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.</p>
Session Border Controller (SBC)	<p>Provide security features for VoIP traffic similar to that provided by firewalls.</p> <p>Scope Note: SBCs can be configured to filter specific VoIP protocols, monitor for denial-of-service (DOS) attacks, and provide network address and protocol translation features.</p>

Term	Definition
Sign-on Procedure	<p>The procedure performed by a user to gain access to an application or operating system.</p> <p>Scope Note: If the user is properly identified and authenticated by the system's security, they will be able to access the software.</p>
Source Code	<p>The language in which a program is written.</p> <p>Scope Note: Source code is translated into object code by assemblers and compilers. In some cases, source code may be converted automatically into another language by a conversion program. Source code is not executable by the computer directly. It must first be converted into a machine language.</p>
Spyware	<p>Software whose purpose is to monitor a computer user's actions (e.g., web sites they visit) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user.</p> <p>Scope Note: A particularly malicious form of spyware is software that monitors keystrokes (e.g., to obtain passwords) or otherwise gathers sensitive information such as credit card numbers, which it then transmits to a malicious third party. The term has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.</p>
Standard	<p>A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as ISO.</p>
Statistical Sampling	<p>A method of selecting a portion of a population, by means of mathematical calculations and probabilities, for the purpose of making scientifically and mathematically sound inferences regarding the characteristics of the entire population.</p>
Substantive Testing	<p>Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period.</p>
Supply Chain Management (SCM)	<p>A concept that allows an organization to more effectively and efficiently manage the activities of design, manufacturing, distribution, service and recycling of products and services its their customers.</p>
Switches	<p>Typically associated as a data link layer device, switches enable LAN network segments to be created and interconnected, which also has the added benefit of reducing collision domains in Ethernet-based networks.</p>
System development life cycle (SDLC)	<p>The phases deployed in the development or acquisition of a software system.</p> <p>Scope Note: Typical phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review, but not the service delivery or benefits realization activities.</p>
System Software	<p>A collection of computer programs used in the design, processing and control of all applications.</p> <p>Scope Note: The programs and processing routines that control the computer hardware, including the operating system and utility programs.</p>
System Testing	<p>Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements.</p> <p>Scope Note: System test procedures typically are performed by the system maintenance staff in their development library.</p>
Tape Management System (TMS)	<p>A system software tool that logs, monitors and directs computer tape usage.</p>
Threat	<p>A potential cause of an unwanted incident. (ISO/IEC 13335)</p>

Term	Definition
Throughput	The quantity of useful work made by the system per unit of time. Throughput can be measured in instructions per second or some other unit of performance. When referring to a data transfer operation, Throughput measures the useful data transfer rate and is expressed in kbps, Mbps and Gbps.
Token	A device that is used to authenticate a user, typically in addition to a username and password. Scope Note: A token is usually a credit card-sized device that displays a pseudo random number that changes every few minutes.
Topology	The physical layout of how computers are linked together. Scope Note: Examples of topology include ring, star and bus
Transaction	Business events or information grouped together because they have a single or similar purpose. Scope Note: Typically, a transaction is applied to a calculation or event that then results in the updating of a holding or master file.
Transmission Control Protocol/Internet Protocol (TCP/IP)	Provides the basis for the Internet; a set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access and network management.
Trojan Horse	Purposefully hidden malicious or damaging code within an authorized computer program. Scope Note: Unlike viruses, they do not replicate themselves, but they can be just as destructive to a single computer.
Tunneling	Commonly used to bridge between incompatible hosts/routers or to provide encryption, a method by which one network protocol encapsulates another protocol within itself. Scope Note: When protocol A encapsulates protocol B, then a protocol A header and optional tunneling headers are appended to the original protocol B packet. Protocol A then becomes the data link layer of protocol B. Examples of tunneling protocols include IPSec, Point-to-point Protocol Over Ethernet (PPPoE), and Layer 2 Tunneling Protocol (L2TP).
Uninterruptible Power Supply (UPS)	Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level.
Unit Testing	A testing technique that is used to test program logic within a particular program or module. Scope Note: The purpose of the test is to ensure that the internal operation of the program performs according to specification. It uses a set of test cases that focus on the control structure of the procedural design.
Universal Serial BUS (USB)	An external bus standard that provides capabilities to transfer data at a rate of 12 Mbps. Scope Note: A USB port can connect up to 127 peripheral devices.

Term	Definition
Utility Programs	Specialized system software used to perform particular computerized functions and routines that are frequently required during normal processing. Scope Note: Examples of utility programs include sorting, backing up and erasing data.
Virus	A program with the ability to reproduce by modifying other programs to include a copy of itself. Scope Note: A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network.
Voice-over Internet Protocol (VoIP)	Also called IP Telephony, Internet telephony and Broadband Phone, this is a technology that makes it possible to have a voice conversation over the Internet or over any dedicated Internet Protocol (IP) network instead of dedicated voice transmission lines.
Vulnerability Analysis	Process of identifying and classifying vulnerabilities.
Warm Site	Similar to a hot site; however, it is not fully equipped with all necessary hardware needed for recovery.
Waterfall Development	Also known as traditional development, it is a procedure-focused development cycle with formal sign-off at the completion of each level.
Wi-Fi Protected Access (WPA)	A class of systems used to secure wireless (Wi-Fi) computer networks. Scope Note: WPA was created in response to several serious weaknesses researchers found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security with two significant issues. First, either WPA or WPA2 must be enabled and chosen in preference to WEP; WEP is usually presented as the first security choice in most installation instructions. Second, in the “personal” mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.
Wired Equivalent Privacy (WEP)	A scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks (also known as Wi-Fi networks). Scope Note: Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network (in particular it does not protect users of the network from each other), hence the name. Several serious weaknesses were identified by cryptanalysts, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the weaknesses, WEP provides a level of security that can deter casual snooping.
Wiretapping	The practice of eavesdropping on information being transmitted over telecommunications links.