Trust in, and value from, information systems

CISA® Glossary

Term	Definition
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 control	The processes, rules and deployment mechanisms that 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: Also referred to as access control tables
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
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.
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, alternative 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 It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected

© 2012 ISACA All rights reserved.

Term	Definition
Application	A computer program or set of programs that performs the processing of records for a specific function Scope Note: Contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort
Application controls	The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved
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 that applications need to specify, for example, when interfacing with the operating system (e.g., provided by Microsoft Windows, different versions of UNIX). A programmer utilizes these APIs in developing applications that can operate effectively and efficiently on the platform chosen.
Application software tracing and mapping	Specialized tools that can be used to analyze the flow of data through the processing logic of the application software and document the logic, paths, control conditions and processing sequences Scope Note: Both the command language or job control statements and programming language can be analyzed. This technique includes program/system: mapping, tracing, snapshots, parallel simulations and code comparisons.
Asymmetric key (public key)	A cipher technique in which different cryptographic keys are used to encrypt and decrypt a message Scope Note: See Public key encryption.
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	The 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	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 Scope Note: 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 2. A high-level description of the audit work to be performed in a certain period of time
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

© 2012 ISACA All rights reserved.

Term	Definition
Audit trail	A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source
Authentication	1. The act of verifying identity (i.e., user, system) Scope Note: Risk: Can also refer to the verification of the correctness of a piece of data 2. The act of verifying the identity of a user and the user's eligibility to access computerized information Scope Note: Assurance: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.
Backbone	The main communication channel of a digital network. The part of a network that handles the major traffic Scope Note: Employs the highest-speed transmission paths in the network and may also run the longest distances. Smaller networks are attached to the backbone, and networks that connect directly to the end user or customer are called "access networks." A backbone can span a geographic area of any size from a single building to an office complex to an entire country. Or, it can be as small as a backplane in a single cabinet.
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 (BSC)	Developed by Robert S. Kaplan and David P. Norton as a coherent set of performance measures organized into four categories that 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).
Batch control	Correctness checks built into data processing systems and applied to batches of input data, particularly in the data preparation stage 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.
Batch processing	The processing of a group of transactions at the same time Scope Note: Transactions are collected and processed against the master files at a specified time.
Baud rate	The rate of transmission for telecommunications data, expressed in bits per second (bps)
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.
Biometrics	A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint

Term	Definition
Black box testing	A testing approach that focuses on the functionality of the application or product and does not require knowledge of the code intervals
Broadband	Multiple channels are formed by dividing the transmission medium into discrete frequency segments. Scope Note: Broadband generally requires the use of a modem.
Brouter	Device that performs the functions of both a bridge and a router Scope Note: A brouter operates at both the data link and the network layers. It connects same data link type LAN segments as well as different data link ones, which is a significant advantage. Like a bridge, it forwards packets based on the data link layer address to a different network of the same type. Also, whenever required, it processes and forwards messages to a different data link type network based on the network protocol address. When connecting same data link type networks, it is as fast as a bridge and is able to connect different data link type networks.
Buffer	Memory reserved to temporarily hold data to offset differences between the operating speeds of different devices, such as a printer and a computer Scope Note: In a program, buffers are reserved areas of random access memory (RAM) that hold data while they are being processed.
Bus configuration	All devices (nodes) are linked along one communication line where transmissions are received by all attached nodes. 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.
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 continuity plan (BCP)	A plan used by an enterprise to respond to disruption of critical business processes. Depends on the contingency plan for restoration of critical systems
Business impact analysis (BIA)	A process to determine the impact of losing the support of any resource Scope Note: The BIA assessment study will establish the escalation of that loss over time. 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.
Business process reengineering (BPR)	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

© 2012 ISACA All rights reserved.

Term	Definition
Capability Maturity Model (CMM)	1. 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. Scope Note: 2. CMM for software, from the Software Engineering Institute (SEI), is a model used by many enterprises to identify best practices useful in helping them assess and increase the maturity of their software development processes Scope Note: CMM ranks software development enterprises 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. A maturity model that indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives A collection of instructions that an enterprise can follow to gain better control over its software development process
Capacity stress testing	Testing an application with large quantities of data to evaluate its performance during peak periods. Also called volume testing
Card swipe	A physical control technique that uses a secured card or ID to gain access to a highly sensitive location. Scope Note: If built correctly, card swipes act as a preventive control over physical access to those sensitive locations. After a card has been swiped, the application attached to the physical card swipe device logs all card users who try to access the secured location. The card swipe device prevents unauthorized access and logs all attempts to enter the secured location.
Certificate (Certification) authority (CA)	A trusted third party that serves authentication infrastructures or enterprises and registers entities and issues them certificates
Certificate revocation list (CRL)	An instrument for checking the continued validity of the certificates for which the certification authority (CA) has responsibility Scope Note: The 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.
Certification practice statement (CPS)	A detailed set of rules governing the certificate authority's operations. It provides an understanding of the value and trustworthiness of certificates issued by a given certificate authority (CA). Scope Note: In terms of the controls that an enterprise observes, the method it uses to validate the authenticity of certificate applicants and the CA's expectations of how its certificates may be used

Term	Definition
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.
Challenge/response token	A method of user authentication that is carried out through use of the Challenge Handshake Authentication Protocol (CHAP) Scope Note: When a user tries to log into the server using CHAP, the server sends the user a "challenge," which is a random value. The user enters a password, which is used as an encryption key to encrypt the "challenge" and return it to the server. The server is aware of the password. It, therefore, encrypts the "challenge" value and compares it with the value received from the user. If the values match, the user is authenticated. The challenge/response activity continues throughout the session and this protects the session from password sniffing attacks. In addition, CHAP is not vulnerable to "man-in-the-middle" attacks because the challenge value is a random value that changes on each access attempt.
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
Check digit	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. Scope Note: Check digit control is effective in detecting transposition and transcription errors.
Checkpoint restart procedures	A point in a routine at which sufficient information can be stored to permit restarting the computation from that point

© 2012 ISACA All rights reserved.

Term	Definition
Checksum	A mathematical value that is assigned to a file and used to “test” the file at a later date to verify that the data contained in the file has not been maliciously changed Scope Note: A cryptographic checksum is created by performing a complicated series of mathematical operations (known as a cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as the checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum. Cryptographic checksums are used in data transmission and data storage. Cryptographic checksums are also known as message authentication codes, integrity check-values, modification detection codes or message integrity codes.
Circuit-switched network	A data transmission service requiring the establishment of a circuit-switched connection before data can be transferred from source data terminal equipment (DTE) to a sink DTE Scope Note: A circuit-switched data transmission service uses a connection network.
Circular routing	In open systems architecture, circular routing is the logical path of a message in a communication network based on a series of gates at the physical network layer in the open systems interconnection (OSI) model.
Client-server	A group of computers connected by a communication network, in which the client is the requesting machine and the server is the supplying machine 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.
Cluster controller	A communication terminal control hardware unit that controls a number of computer terminals Scope Note: All messages are buffered by the controller and then transmitted to the receiver.
Coaxial cable	Composed of an insulated wire that runs through the middle of each cable, a second wire that surrounds the insulation of the inner wire like a sheath, and the outer insulation which wraps the second wire Scope Note: Has a greater transmission capacity than standard twisted-pair cables, but has a limited range of effective distance
Cohesion	The extent to which a system unit--subroutine, program, module, component, subsystem--performs a single dedicated function. Scope Note: Generally, the more cohesive the unit, the easier it is to maintain and enhance a system because it is easier to determine where and how to apply a change.
Cold site	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 Scope Note: The site is ready to receive the necessary replacement computer equipment in the event that the users have to move from their main computing location to the alternative computer facility.

Term	Definition
Compensating control	An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions
Completely connected (mesh) configuration	A network topology in which devices are connected with many redundant interconnections between network nodes (primarily used for backbone networks)
Completeness check	A procedure designed to ensure that no fields are missing from a record
Compliance testing	Tests of control designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period
Comprehensive audit	An audit designed to determine the accuracy of financial records as well as to evaluate the internal controls of a function or department
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.
Computer forensics	The application of the scientific method to digital media to establish factual information for judicial review Scope Note: This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities. As a discipline, it combines elements of law and computer science to collect and analyze data from information systems (e.g., personal computers, networks, wireless communication and digital storage devices) in a way that is admissible as evidence in a court of law.
Computer sequence checking	Verifies that the control number follows sequentially and that any control numbers out of sequence are rejected or noted on an exception report for further research
Computer-aided software engineering (CASE)	The use of software packages that aid in the development of all phases of an information system 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.
Computer-assisted audit technique (CAAT)	Any automated audit technique, such as generalized audit software (GAS), test data generators, computerized audit programs and specialized audit utilities
Concurrency control	Refers to a class of controls used in a database management system (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.
Configuration management	The control of changes to a set of configuration items over a system life cycle
Console log	An automated detail report of computer system activity
Contingency planning	Process of developing advance arrangements and procedures that enable an enterprise to respond to an event that could occur by chance or unforeseen circumstances.

© 2012 ISACA All rights reserved.

Term	Definition
Continuity	Preventing, mitigating and recovering from disruption Scope Note: The terms "business resumption planning," "disaster recovery planning" and "contingency planning" also may be used in this context; they all concentrate on the recovery aspects of continuity.
Continuous auditing approach	This approach allows IS auditors to monitor system reliability on a continuous basis and to gather selective audit evidence through the computer.
Continuous improvement	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 (JIT) delivery; production load leveling of amounts and types; standardized work; paced moving lines; and right-sized equipment Scope Note: A closer definition of the Japanese usage of Kaizen is "to take it apart and put it 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.
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 Inherent risk)
Cookie	A message kept in the web browser for the purpose of identifying users and possibly preparing customized web pages for them Scope Note: 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 identity and enable restricted web services).
Corporate governance	The system by which enterprises are directed and controlled. The board of directors is responsible for the governance of their enterprise. It consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives.
Corrective control	Designed to correct errors, omissions and unauthorized uses and intrusions, once they are detected

Term	Definition
Coupling	Measure of interconnectivity among structure of software programs. Coupling depends on the interface complexity between modules. This can be defined as the point at which entry or reference is made to a module, and what data pass across the interface. Scope Note: In application software design, it is preferable to strive for the lowest possible coupling between modules. Simple connectivity among modules results in software that is easier to understand and maintain and is less prone to a ripple or domino effect caused when errors occur at one location and propagate through the system.
Critical infrastructure	Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation.
Critical success factor (CSF)	The most important issue or action 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 enterprise manage customer relationships in an organized manner.
Data custodian	The individual(s) and department(s) responsible for the storage and safeguarding of computerized data
Data dictionary	A database that contains the name, type, range of values, source and authorization for access for each data element in a database. It also indicates which application programs use those data so that when a data structure is contemplated, a list of the affected programs can be generated Scope Note: May be a stand-alone information system used for management or documentation purposes, or it may control the operation of a database
Data diddling	Changing data with malicious intent before or during input into the system
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 owner	The individual(s), normally a manager or director, who has 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 enterprises and individuals to meet their information processing and retrieval requirements
Database administrator (DBA)	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.

© 2012 ISACA All rights reserved.

Term	Definition
Database management system (DBMS)	A software system that controls the organization, storage and retrieval of data in a database
Database replication	The process of creating and managing duplicate versions of a database Scope Note: Replication not only copies a database but also synchronizes a set of replicas so that changes made to one replica are reflected in all of the others. The beauty of replication is that it enables many users to work with their own local copy of a database, but have the database updated as if they were working on a single centralized database. For database applications in which, geographically users are distributed widely, replication is often the most efficient method of database access.
Data-oriented systems development	Focuses on providing ad hoc reporting for users by developing a suitable accessible database of information and to provide useable data rather than a function
Decentralization	The process of distributing computer processing to different locations within an enterprise
Decision support systems (DSS)	An interactive system that provides the user with easy access to decision models and data, to support semi structured decision-making tasks
Decryption	A technique used to recover the original plaintext from the ciphertext so that it is intelligible to the reader The decryption is a reverse process of the encryption.
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.
Demodulation	The process of converting an analog telecommunications signal into a digital computer signal
Dial-back	Used as a control over dial-up telecommunications lines. The telecommunications link established through dial-up into the computer from a remote location is interrupted so the computer can dial back to the caller. The link is permitted only if the caller is calling from a valid phone number or telecommunications channel.
Dial-in access control	Prevents unauthorized access from remote users who attempt to access a secured environment Ranges from a dial-back control to remote user authentication
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 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
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

Term	Definition
Distributed data processing network	A system of computers connected together by a communication network Scope Note: Each computer processes its data and the network supports the system as a whole. Such a network enhances communication among the linked computers and allows access to shared files.
Diverse routing	The method of routing traffic through split cable facilities or duplicate cable facilities Scope Note: This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. However, acquiring this type of access is time-consuming and costly. Most carriers provide facilities for alternate and diverse routing, although the majority of services are transmitted over terrestrial media. These cable facilities are usually located in the ground or basement. Ground-based facilities are at great risk due to the aging infrastructures of cities. In addition, cable-based facilities usually share room with mechanical and electrical systems that can impose great risk due to human error and disastrous events.
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 "in" boxes of administrative and technical contacts. Cache poisoning is related to URL poisoning or location poisoning, in which 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. It is also called DNS cache poisoning or cache poisoning.
Downtime report	A report that identifies the elapsed time when a computer is not operating correctly because of machine failure
Dry-pipe fire extinguisher system	Refers to a sprinkler system that does not have water in the pipes during idle usage, unlike a fully charged fire extinguisher system that has water in the pipes at all times Scope Note: The dry-pipe system is activated at the time of the fire alarm and water is emitted to the pipes from a water reservoir for discharge to the location of the fire.
Duplex routing	The method or communication mode of routing data over the communication network
Dynamic Host Configuration Protocol (DHCP)	A protocol used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask and IP addresses of domain name system (DNS) servers from a DHCP server Scope Note: The DHCP server ensures that all IP addresses are unique (e.g., no IP address is assigned to a second client while the first client's assignment is valid [its lease has not expired]). Thus, IP address pool management is done by the server and not by a human network administrator.
Echo checks	Detects line errors by retransmitting data back to the sending device for comparison with the original transmission

Term	Definition
E-commerce	The processes by which enterprises 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 electronic data interchange (EDI) and Society for Worldwide Interbank Financial Telecommunication (SWIFT).
Edit control	Detects errors in the input portion of information that is sent to the computer for processing May be manual or automated and allow the user to edit data errors before processing
Editing	Ensures that data conform to predetermined criteria and enable early identification of potential errors
Electronic data interchange (EDI)	The electronic transmission of transactions (information) between two enterprises EDI promotes a more efficient paperless environment. EDI transmissions can replace the use of standard documents, including invoices or purchase orders.
Electronic funds transfer (EFT)	The exchange of money via telecommunications EFT refers to any financial transaction that originates at a terminal and transfers a sum of money from one account to another
Embedded audit module (EAM)	Integral part of an application system that is designed to identify and report specific transactions or other information based on pre-determined criteria Identification of reportable items occurs as part of real-time processing. Reporting may be real-time online or may use store and forward methods. Also known as integrated test facility or continuous auditing module.
Encapsulation (objects)	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)
Encryption key	A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext
End-user computing	The ability of end users to design and implement their own information system utilizing computer software products
ERP (enterprise resource planning) system	A packaged business software system that allows an enterprise to automate and integrate the majority of its business processes, share common data and practices across the entire enterprise, and produce and access information in a real-time environment Scope Note: Examples of ERP include SAP, Oracle Financials and J.D. Edwards.
Escrow agent	A person, agency or enterprise that is authorized to act on behalf of another to create a legal relationship with a third party in regard to an escrow agreement; the custodian of an asset according to an escrow agreement Scope Note: As it relates to a cryptographic key, an escrow agent is the agency or enterprise charged with the responsibility for safeguarding the key components of the unique key.

© 2012 ISACA All rights reserved.

Term	Definition
Escrow agreement	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 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.
Ethernet	A popular network protocol and cabling scheme that uses a bus topology and carrier sense multiple access/collision detection (CSMA/CD) to prevent network failures or collisions when two devices try to access the network at the same time
Evidence	1. Information that proves or disproves a stated issue Scope Note: 2. Information that 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 Scope Note: Audit perspective
Exception reports	An exception report is generated by a program that identifies transactions or data that appear to be incorrect. Scope Note: Exception reports may be outside a predetermined range or may not conform to specified criteria.
Executable code	The machine language code that is generally referred to as the object or load module
Expert system	The most prevalent type of computer system that arises from the research of artificial intelligence Scope Note: An expert system has a built in hierarchy of rules, which are acquired from human experts in the appropriate field. Once input is provided, the system should be able to define the nature of the problem and provide recommendations to solve the problem.
Exposure	The potential loss to an area due to the occurrence of an adverse event
eXtensible Markup Language (XML)	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 enterprises.

© 2012 ISACA All rights reserved.

Term	Definition
Extranet	A private network that resides on the Internet and allows a company to securely share business information with customers, suppliers or other businesses as well as to execute electronic transactions Scope Note: Different from an Intranet in that it is located beyond the company's firewall. Therefore, an extranet relies on the use of securely issued digital certificates (or alternative methods of user authentication) and encryption of messages. A virtual private network (VPN) and tunneling are often used to implement extranets, to ensure security and privacy.
Fallback procedures	A plan of action or set of procedures to be performed if a system implementation, upgrade or modification does not work as intended Scope Note: May involve restoring the system to its state prior to the implementation or change. Fallback procedures are needed to ensure that normal business processes continue in the event of failure and should always be considered in system migration or implementation.
False authorization	Also called false acceptance, occurs when an unauthorized person is identified as an authorized person by the biometric system
False enrollment	Occurs when an unauthorized person manages to enroll into the biometric system Scope Note: Enrollment is the initial process of acquiring a biometric feature and saving it as a personal reference on a smart card, a PC or in a central database.
Fault tolerance	A system’s level of resilience to seamlessly react to hardware and/or software failure
Feasibility study	A phase of a system development life cycle (SDLC) methodology that researches the feasibility and adequacy of resources for the development or acquisition of a system solution to a user need
Fiber-optic cable	Glass fibers that transmit binary signals over a telecommunications network Scope Note: Fiber-optic systems have low transmission losses as compared to twisted-pair cables. They do not radiate energy or conduct electricity. They are free from corruption and lightning-induced interference, and they reduce the risk of wiretaps.
File allocation table (FAT)	A table used by the operating system to keep track of where every file is located on the disk Scope Note: Since a file is often fragmented and thus subdivided into many sectors within the disk, the information stored in the FAT is used when loading or updating the contents of the file.
File layout	Specifies the length of the file record and the sequence and size of its fields Scope Note: Also will specify the type of data contained within each field; for example, alphanumeric, zoned decimal, packed and binary.

© 2012 ISACA All rights reserved.

Term	Definition
File server	A high-capacity disk storage device or a computer that stores data centrally for network users and manages access to those data Scope Note: File servers can be dedicated so that no process other than network management can be executed while the network is available; file servers can be non-dedicated so that standard user applications can run while the network is available.
Financial audit	An audit designed to determine the accuracy of financial records and information
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
Firmware	Memory chips with embedded program code that hold their content when power is turned off
Foreign key	A value that represents a reference to a tuple (a row in a table) containing the matching candidate key value Scope Note: The problem of ensuring that the database does not include any invalid foreign key values is known as the referential integrity problem. The constraint that values of a given foreign key must match values of the corresponding candidate key is known as a referential constraint. The relation (table) that contains the foreign key is referred to as the referencing relation and the relation that contains the corresponding candidate key as the referenced relation or target relation. (In the relational theory it would be a candidate key, but in real database management systems (DBMSs) implementations it is always the primary key.)
Format checking	The application of an edit, using a predefined field definition to a submitted information stream; a test to ensure that data conform to a predefined format
Frame relay	A packet-switched wide-area-network (WAN) technology that provides faster performance than older packet-switched WAN technologies Scope Note: Best suited for data and image transfers. Because of its variable-length packet architecture, it is not the most efficient technology for real-time voice and video. In a frame-relay network, end nodes establish a connection via a permanent virtual circuit (PVC).
Function point analysis	A technique used to determine the size of a development task, based on the number of function points Scope Note: Function points are factors such as inputs, outputs, inquiries and logical internal sites.
General computer control	A Control, other than an application control, that relates to the environment within which computer-based application systems are developed, maintained and operated, and that is therefore applicable to all applications The objectives of general controls are to ensure the proper development and implementation of applications and the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.
Generalized audit software (GAS)	Multipurpose audit software that can be used for general processes, such as record selection, matching, recalculation and reporting

Term	Definition
Hacker	An individual who attempts to gain unauthorized access to a computer system
Handprint scanner	A biometric device that is used to authenticate a user through palm scans
Hardware	The physical components of a computer system
Hash total	The total of any numeric data field in a document or computer file This total is checked against a control total of the same field to facilitate accuracy of processing.
Help desk	A service offered via telephone/Internet by an enterprise to its clients or employees that provides information, assistance and troubleshooting advice regarding software, hardware or networks. Scope Note: A help desk is staffed by people who can either resolve the problem on their own or escalate the problem to specialized personnel. A help desk is often equipped with dedicated customer relationship management (CRM) software that logs the problems and tracks them until they are solved.
Heuristic filter	A method often employed by antispam software to filter spam using criteria established in a centralized rule database Scope Note: Every e-mail message is given a rank, based on 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.
Hexadecimal	A numbering system that uses a base of 16 and uses 16 digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F Programmers use hexadecimal numbers as a convenient way of representing binary numbers.
Hierarchical database	A database structured in a tree/root or parent/child relationship Scope Note: Each parent can have many children, but each child may have only one parent.
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 sure as headings, paragraphs, lists--and can be used to describe, to some degree, the appearance and semantics of a document
Image processing	The process of electronically inputting source documents by taking an image of the document, thereby eliminating the need for key entry
Impact assessment	A review of the possible consequences of a risk Scope Note: See also Impact analysis.

© 2012 ISACA All rights reserved.

Term	Definition
Impersonation	A security concept related to Windows NT that allows a server application to temporarily "be" the client in terms of access to secure objects Scope Note: Impersonation has three possible levels: identification, letting the server inspect the client's identity; impersonation, letting the server act on behalf of the client; and delegation, the same as impersonation but extended to remote systems to which the server connects (through the preservation of credentials). Impersonation by imitating or copying the identification, behavior or actions of another may also be used in social engineering to obtain otherwise unauthorized physical access.
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.
Incremental testing	Deliberately testing only the value-added functionality of a software component
Independence	1. Self-governance 2. Freedom from conflict of interest and undue influence Scope Note: The IS auditor should be free to make his/her own decisions, not influenced by the enterprise being audited and its people (managers and employers).
Indexed Sequential Access Method (ISAM)	A disk access method that stores data sequentially while also maintaining an index of key fields to all the records in the file for direct access capability
Indexed sequential file	A file format in which records are organized and can be accessed, according to a pre-established key that is part of the record
Information processing facility (IPF)	The computer room and support areas
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 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
Inherent risk	1. The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls) 2. The risk that a material error could occur, assuming that there are no related internal controls to prevent or detect the error Scope Note: Audit perspective; also see Control risk
Inheritance (objects)	Database structures that have a strict hierarchy (no multiple inheritance) Inheritance can initiate other objects irrespective of the class hierarchy, thus there is no strict hierarchy of objects
Initial program load (IPL)	The initialization procedure that causes an operating system to be loaded into storage at the beginning of a workday or after a system malfunction.
Input control	Techniques and procedures used to verify, validate and edit data to ensure that only correct data are entered into the computer
Instant messaging (IM)	An online mechanism or a form of real-time communication between two or more people based on typed text and multimedia data Scope Note: Text is conveyed via computers or another electronic device (e.g., cellular phone or handheld device) connected over a network, such as the Internet.
Integrated services digital network (ISDN)	A public end-to-end digital telecommunications network with signaling, switching and transport capabilities supporting a wide range of service accessed by standardized interfaces with integrated customer control Scope Note: The standard allows transmission of digital voice, video and data over 64-Kpbs lines.
Integrated test facilities (ITF)	A testing methodology in which test data are processed in production systems Scope Note: The data usually represent a set of fictitious entities such as departments, customers or products. Output reports are verified to confirm the correctness of the processing.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
Interface testing	A testing technique that is used to evaluate output from one application while the information is sent as input to another application
Internal controls	The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected
Internet Protocol (IP) packet 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.

Term	Definition
Irregularity	Intentional violation of an established management policy or regulatory requirement It may consist of deliberate misstatements or omission of information concerning the area under audit or the enterprise as a whole; gross negligence or unintentional illegal acts.
IT governance framework	A model that integrates a set of guidelines, policies and methods that represent the organizational approach to IT governance Scope Note: Per COBIT, 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 enterprise's IT sustains and extends the enterprise'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 enterprise's 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 enterprise’s users
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.
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 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 management practice	Management practices that are required to successfully execute business processes
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.
Leased line	A communication line permanently assigned to connect two points, as opposed to a dial-up line that is only available and open when a connection is made by dialing the target machine or network Also known as a dedicated line

© 2012 ISACA All rights reserved.

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 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)	Communication network that serves several users within a specified geographic area Scope Note: A personal computer LAN functions as a distributed processing system 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 in which they occurred
Logical access controls	The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files
Magnetic card reader	Reads cards with a magnetic surface on which data can be stored and retrieved
Malware	Short for malicious 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, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes.
Management information system (MIS)	An organized assembly of resources and procedures required to collect, process and distribute data for use in decision making
Mapping	Diagramming data that are to be exchanged electronically, including how they are to be used and what business management systems need them. See also Application Tracing and Mapping. Scope Note: Mapping is a preliminary step for developing an applications link.
Masking	A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report
Master file	A file of semi permanent information that is used frequently for processing data or for more than one purpose

Term	Definition
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 enterprise as a whole
Maturity	In business, indicates the degree of reliability or dependency that the business can place on a process achieving the desired goals or objectives
Maturity model	Scope Note: See Capability Maturity Model (CMM).
Media access control (MAC)	Applied to the hardware at the factory and cannot be modified, MAC is a unique, 48-bit, hard-coded address of a physical layer device, such as an Ethernet local area network (LAN) or a wireless network card
Media oxidation	The deterioration of the media on which data are digitally stored due to exposure to oxygen and moisture 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.
Memory dump	The act of copying raw data from one place to another with little or no formatting for readability Scope Note: Usually, dump refers to copying data from the main memory to a display screen or a printer. Dumps are useful for diagnosing bugs. After a program fails, one can study the dump and analyze the contents of memory at the time of the failure. A memory dump will not help unless each person knows what to look for because dumps are usually output in a difficult-to-read form (binary, octal or hexadecimal).
Message switching	A telecommunications methodology that controls traffic in which a complete message is sent to a concentration point and stored until the communications path is established
Microwave transmission	A high-capacity line-of-sight transmission of data signals through the atmosphere which often requires relay stations
Middleware	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.
Milestone	A terminal element that marks the completion of a work package or phase Scope Note: Typically marked by a high-level event such as project completion, receipt, endorsement or signing of a previously-defined deliverable or a high-level review meeting at which the appropriate level of project completion is determined and agreed to. A milestone is associated with a decision that outlines the future of a project and, for an outsourced project, may have a payment to the contractor associated with it.
Mission-critical application	An application that is vital to the operation of the enterprise. The term is very popular for describing the applications required to run the day-to-day business.
Monetary unit sampling	A sampling technique that estimates the amount of overstatement in an account balance
Network	A system of interconnected computers and the communication equipment used to connect them

Term	Definition
Network administrator	Responsible for planning, implementing and maintaining the telecommunications infrastructure; also may be responsible for voice networks Scope Note: For smaller enterprises, the network administrator may also maintain a local area network (LAN) and assist end users.
Network attached storage (NAS)	Utilizes dedicated storage devices that centralize storage of data Scope Note: NA storage devices generally do not provide traditional file/print or application services.
Nondisclosure agreement (NDA)	A legal contract between at least two parties that outlines confidential materials that 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 Scope Note: Also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement. An NDA creates a confidential relationship between the parties to protect any type of trade secret. As such, an NDA can protect non-public business information. In the case of certain governmental entities, the confidentiality of information other than trade secrets may be subject to applicable statutory requirements, and in some cases may be required to be revealed to an outside party requesting the information. Generally, the governmental entity will include a provision in the contract to allow the seller to review a request for information that the seller identifies as confidential and the seller may appeal such a decision requiring disclosure. NDAs are commonly signed when two companies or individuals are considering doing business together and need to understand the processes used in one another's businesses solely for the purpose of evaluating the potential business relationship. NDAs can be "mutual," meaning that both parties are restricted in their use of the materials provided, or they can only restrict a single party. It is also possible for an employee to sign an NDA or NDA-like agreement with a company at the time of hiring; in fact, some employment agreements will include a clause restricting "confidential information" in general.
Normalization	The elimination of redundant data
Numeric check	An edit check designed to ensure that the data element in a particular field is numeric.
Object code	Machine-readable instructions produced from a compiler or assembler program that has accepted and translated the source code
Object orientation	An approach to system development in which the basic unit of attention is an object, which represents an encapsulation of both data (an object's attributes) and functionality (an object's methods) Scope Note: Objects usually are created using a general template called a class. A class is the basis for most design work in objects. A class and its objects communicate in defined ways. Aggregate classes interact through messages, which are directed requests for services from one class (the client) to another class (the server). A class may share the structure or methods defined in one or more other classes--a relationship known as inheritance.
Objectivity	The ability to exercise judgment, express opinions and present recommendations with impartiality
Offsite storage	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

© 2012 ISACA All rights reserved.

Term	Definition
Online data processing	Achieved by entering information into the computer via a video display terminal Scope Note: With online data processing, the computer immediately accepts or rejects the information as it is entered.
Open system	System for which detailed specifications of the composition of its component are published in a nonproprietary environment, thereby enabling competing enterprises to use these standard components to build competitive systems Scope Note: The advantages of using open systems include portability, interoperability and integration.
Operating system (OS)	A master control program that runs the computer and acts as a scheduler and traffic controller Scope Note: The operating system is the first program copied into the computer's memory after the computer is turned on; it 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.
Operational audit	An audit designed to evaluate the various internal controls, economy and efficiency of a function or department
Operational control	Deals with the everyday operation of a company or enterprise to ensure that all objectives are achieved
Optical scanner	An input device that reads characters and images that are printed or painted on a paper form into the computer
Outsourcing	A formal agreement with a third party to perform IS or other business functions for an enterprise
Packet switching	The process of transmitting messages in convenient pieces that can be reassembled at the destination
Paper test	A walk-through of the steps of a regular test, but without actually performing the steps Scope Note: Usually used in disaster recovery and contingency testing; team members review and become familiar with the plans and their specific roles and responsibilities
Parallel testing	The process of feeding test data into two systems, the modified system and an alternative system (possibly the original system), and comparing results to demonstrate the consistency and inconsistency between two versions of the application
Parity check	A general hardware control that helps to detect data errors when data are read from memory or communicated from one computer to another 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.
Partitioned file	A file format in which the file is divided into multiple sub files and a directory is established to locate each sub file

© 2012 ISACA All rights reserved.

Term	Definition
Passive assault	Intruders attempt to learn some characteristic of the data being transmitted Scope Note: With a passive assault, intruders may be able to read the contents of the data so the privacy of the data is violated. Alternatively, although the content of the data itself may remain secure, intruders may read and analyze the plaintext source and destination identifiers attached to a message for routing purposes, or they may examine the lengths and frequency of messages being transmitted.
Password	A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system
Patch management	An area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk Scope Note: Patch management tasks include the following: maintaining current knowledge of available patches; deciding what patches are appropriate for particular systems; ensuring that patches are installed properly; testing systems after installation; and documenting all associated procedures, such as specific configurations required. A number of products are available to automate patch management tasks. Patches are sometimes ineffective and can sometimes cause more problems than they fix. Patch management experts suggest that system administrators take simple steps to avoid problems, such as performing backups and testing patches on non-critical systems prior to installations. Patch management can be viewed as part of change management.
Penetration testing	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers
Performance driver	A measure that is considered the "driver" of a lag indicator It can be measured before the outcome is clear and, therefore, is called a "lead indicator." 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.
Performance testing	Comparing the system's performance to other equivalent systems, using well-defined benchmarks
Peripherals	Auxiliary computer hardware equipment used for input, output and data storage Scope Note: Examples of peripherals include disk drives and printers.
Personal identification number (PIN)	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 Scope Note: PINs have been adopted by financial institutions as the primary means of verifying customers in an electronic funds transfer (EFT) system.

© 2012 ISACA All rights reserved.

Term	**Definition**
Phishing	This is a type of electronic mail (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 Scope Note: Phishing attacks may take the form of masquerading as a lottery organization advising the recipient or the user's bank of a large win; in either case, the intent is to obtain account and personal identification number (PIN) details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.
Plaintext	Digital information, such as cleartext, that is intelligible to the reader
Point-of-sale (POS) systems	Enables the capture of data at the time and place of transaction 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
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
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. IT service, project, asset and other resource portfolios are of primary interest to COBIT.)
Preventive control	An internal control that is used to avoid undesirable events, errors and other occurrences that an enterprise has determined could have a negative material effect on a process or end product
Privacy	Freedom from unauthorized intrusion or disclosure of information about an individual
Private branch exchange (PBX)	A telephone exchange that is owned by a private business, as opposed to one owned by a common carrier or by a telephone company

© 2012 ISACA All rights reserved.

Term	Definition
Private key cryptosystems	Used in data encryption, it utilizes a secret key to encrypt the plaintext to the ciphertext. Private key cryptosystems also use the same key to decrypt the ciphertext to the corresponding plaintext. Scope Note: In this case, the key is symmetric such that the encryption key is equivalent to the decryption key.
Problem escalation procedure	The process of escalating a problem up from junior to senior support staff, and ultimately to higher levels of management Scope Note: Problem escalation procedure is often used in help desk management, when an unresolved problem is escalated up the chain of command, until it is solved.
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.
Process	Generally, a collection of activities influenced by the enterprise’s policies and procedures that takes inputs from a number of sources, (including other processes), manipulates the inputs and produces outputs 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.
Production program	Program used to process live or actual data that were received as input into the production environment
Production software	Software that is being used and executed to support normal and authorized organizational operations Scope Note: Production software is to be distinguished from test software, which is being developed or modified, but has not yet been authorized for use by management.
Professional competence	Proven level of ability, often linked to qualifications issued by relevant professional bodies and compliance with their codes of practice and standards
Program Evaluation and Review Technique (PERT)	A project management technique used in the planning and control of system projects
Program flowchart	Shows the sequence of instructions in a single program or subroutine Scope Note: The symbols used in program flowcharts should be the internationally accepted standard. Program flowcharts should be updated when necessary.
Program narrative	Provides a detailed explanation of program flowcharts, including control points and any external input
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-on schedule and budget
Project portfolio	The set of projects owned by a company Scope Note: It usually includes the main guidelines relative to each project, including objectives, costs, time lines and other information specific to the project.
Protocol	The rules by which a network operates and controls the flow and priority of transmissions
Protocol converter	Hardware devices, such as asynchronous and synchronous transmissions, that convert between two different types of transmission

Term	Definition
Prototyping	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 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.
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.
Public key cryptosystem	Used in data encryption, it uses an encryption key, as a public key, to encrypt the plaintext to the ciphertext. It uses the different decryption key, as a secret key, to decrypt the ciphertext to the corresponding plaintext. Scope Note: In contrast to a private key cryptosystem, the decryption key should be secret; however, the encryption key can be known to everyone. In a public key cryptosystem, two keys are asymmetric, such that the encryption key is not equivalent to the decryption key.
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 See also Asymmetric Key.
Public key infrastructure (PKI)	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)
Radio wave interference	The superposition of two or more radio waves resulting in a different radio wave pattern that is more difficult to intercept and decode properly
Random access memory (RAM)	The computer's primary working memory Scope Note: Each byte of RAM can be accessed randomly regardless of adjacent bytes.
Range check	Range checks ensure that data fall within a predetermined range
Rapid application development	A methodology that enables enterprises 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
Real-time processing	An interactive online system capability that immediately updates computer files when transactions are initiated through a terminal
Reasonable assurance	A level of comfort short of a guarantee, but considered adequate given the costs of the control and the likely benefits achieved
Reasonableness check	Compares data to predefined reasonability limits or occurrence rates established for the data

© 2012 ISACA All rights reserved.

Term	Definition
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 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 strategy	An approach by an enterprise that will ensure its recovery and continuity in the face of a disaster or other major outage Scope Note: Plans and methodologies are determined by the enterprise's strategy. There may be more than one methodology or solution for an enterprise'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.
Recovery time objective (RTO)	The amount of time allowed for the recovery of a business function or resource after a disaster occurs
Redundancy check	Detects transmission errors by appending calculated bits onto the end of each segment of data
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	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 Scope Note: Existing software systems can be modernized to prolong their functionality. An example is a software code translator that can take an existing hierarchical database system and transpose it to a relational database system. Computer-aided software engineering (CASE) includes a source code reengineering feature.
Registration authority (RA)	The individual institution that validates an 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

Term	Definition
Remote procedure call (RPC)	The traditional Internet service protocol widely used for many years on UNIX-based operating systems and supported by the Internet Engineering Task Force (IETF) that allows a program on one computer to execute a program on another (e.g., server) Scope Note: The primary benefit derived from its use is that a system developer need not develop specific procedures for the targeted computer system. For example, in a client-server arrangement, the client program sends a message to the server with appropriate arguments, and the server returns a message containing the results of the program executed. Common Object Request Broker Architecture (CORBA) and Distributed Component Object Model (DCOM) are two newer object-oriented methods for related RPC functionality.
Repository	An enterprise database that stores and organizes data
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	A technique used in which the affected user groups define the requirements of the system for meeting the defined needs Scope Note: Some of these are business-, regulatory-, and security-related requirements as well as development-related requirements.
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
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	Used in either token ring or fiber distributed data interface (FDDI) networks, all stations (nodes) are connected to a multi-station access unit (MSAU), that physically resembles a star-type topology. Scope Note: A ring configuration is created when MSAUs are linked together in forming a network. Messages in the 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.
Ring topology	A type of local area network (LAN) architecture in which the cable forms a loop, with stations attached at intervals around the loop Scope Note: In ring topology, signals transmitted around the ring take the form of messages. Each station receives the messages and each station determines, on the basis of an address, whether to accept or process a given message. However, after receiving a message, each station acts as a repeater, retransmitting the message at its original signal strength.
Risk	The combination of the probability of an event and its consequence. (ISO/IEC 73)

Term	Definition
Risk analysis	1. A process by which frequency and magnitude of IT risk scenarios are estimated Scope Note: 2. 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 Scope Note: It often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of that event.
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 management	1. The coordinated activities to direct and control an enterprise with regard to risk Scope Note: In the International Standard, the term "control" is used as a synonym for "measure." (ISO/IEC Guide 73:2002) 2. One of the governance objectives. Entails recognizing risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage it within the context of the enterprise’s risk appetite. Scope Note: COBIT 5 perspective
Risk mitigation	The management of risk through the use of countermeasures and controls
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)
Router	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 open systems interconnection (OSI) model 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).
Run-to-run totals	Provide evidence that a program processes all input data and that it processed the data correctly
Salami technique	A method of computer fraud involving a computer code that instructs the computer to slice off small amounts of money from an authorized computer transaction and reroute this amount to the perpetrator’s account

© 2012 ISACA All rights reserved.

Term	Definition
Scheduling	A method used in the information processing facility (IPF) to determine and establish the sequence of computer job processing
Scope creep	Also called requirement creep, this refers to uncontrolled changes in a project’s scope. 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.
Screening routers	A router configured to permit or deny traffic based on a set of permission rules installed by the administrator
Secure Sockets Layer (SSL)	A protocol that is used to transmit private documents through the Internet Scope Note: The SSL protocol uses a private key to encrypt the data that are to be transferred through the SSL connection.
Security administrator	The person responsible for implementing, monitoring and enforcing security rules established and authorized by management
Security awareness	The extent to which every member of an enterprise and every other individual who potentially has access to the enterprise's information understand: -Security and the levels of security appropriate to the enterprise -The importance of security and consequences of a lack of security -Their individual responsibilities regarding security (and act accordingly) Scope Note: 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, 1993
Security 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 A security incident normally includes an estimation of its level of impact. A limited number of impact levels are defined and, for each, the specific actions required and the people who need to be notified are identified.
Security policy	A high-level document representing an enterprise’s information security philosophy and commitment
Security procedures	The formal documentation of operational steps and processes that specify how security goals and objectives set forward in the security policy and standards are to be achieved
Segregation/separation of duties (SoD)	A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets Scope Note: Segregation/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.

© 2012 ISACA All rights reserved.

Term	Definition
Sequence check	Verification that the control number follows sequentially and any control numbers out of sequence are rejected or noted on an exception report for further research Scope Note: Can be alpha or numeric and usually utilizes a key field
Sequential file	A computer file storage format in which one record follows another Scope Note: Records can be accessed sequentially only. It is required with magnetic tape.
Service bureau	A computer facility that provides data processing services to clients on a continual basis
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
Servlet	A Java applet or a small program that runs within a web server environment Scope Note: A Java servlet is similar to a common gateway interface (CGI) program, but unlike a CGI program, once started, it stays in memory and can fulfill multiple requests, thereby saving server execution time and speeding up the services.
Smart card	A small electronic device that contains electronic memory, and possibly an embedded integrated circuit Scope Note: Smart cards can be used for a number of purposes including the storage of digital certificates or digital cash, or they can be used as a token to authenticate users.
Software	Programs and supporting documentation that enable and facilitate use of the computer Scope Note: Software controls the operation of the hardware and the processing of data.
Source code	The language in which a program is written 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.
SPOOL (simultaneous peripheral operations online)	An automated function that can be based on an operating system or application in which electronic data being transmitted between storage areas are spooled or stored until the receiving device or storage area is prepared and able to receive the information Scope Note: Spool allows more efficient electronic data transfers from one device to another by permitting higher speed sending functions, such as internal memory, to continue on with other operations instead of waiting on the slower speed receiving device, such as a printer.

© 2012 ISACA All rights reserved.

Term	Definition
Spyware	Software whose purpose is to monitor a computer user's actions (e.g., web sites visited) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user Scope Note: A particularly malicious form of spyware is software that monitors keystrokes 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
Standard	A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as International Organization for Standardization (ISO)
Star topology	A type of local area network (LAN) architecture that utilizes a central controller to which all nodes are directly connected Scope Note: With star topology, all transmissions from one station to another pass through the central controller which is responsible for managing and controlling all communication. The central controller often acts as a switching device.
Statistical sampling	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
Storage area networks (SANs)	A variation of a local area network (LAN) that is dedicated for the express purpose of connecting storage devices to servers and other computing devices Scope Note: SANs centralize the process for the storage and administration of data.
Structured programming	A top-down technique of designing programs and systems that makes programs more readable, more reliable and more easily maintained
Structured Query Language (SQL)	The primary language used by both application programmers and end users in accessing relational databases
Substantive testing	Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period
Supply chain management (SCM)	A concept that allows an enterprise to more effectively and efficiently manage the activities of design, manufacturing, distribution, service and recycling of products and service its customers
Surge suppressor	Filters out electrical surges and spikes
Suspense file	A computer file used to maintain information (transactions, payments or other events) until the proper disposition of that information can be determined Scope Note: Once the proper disposition of the item is determined, it should be removed from the suspense file and processed in accordance with the proper procedures for that particular transaction. Two examples of items that may be included in a suspense file are receipt of a payment from a source that is not readily identified or data that do not yet have an identified match during migration to a new application.

Term	Definition
Switches	Typically associated as a data link layer device, switches enable local area network (LAN) segments to be created and interconnected, which has the added benefit of reducing collision domains in Ethernet-based networks.
Synchronous transmission	Block-at-a-time data transmission
System development life cycle (SDLC)	The phases deployed in the development or acquisition of a software system Scope Note: SDLC is an approach used to plan, design, develop, test and implement an application system or a major modification to an application system. 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.
System exit	Special system software features and utilities that allow the user to perform complex system maintenance Scope Note: Use of system exits often permits the user to operate outside of the security access control system.
System flowchart	Graphic representations of the sequence of operations in an information system or program Scope Note: Information system flowcharts show how data from source documents flow through the computer to final distribution to users. Symbols used should be the internationally accepted standard. System flowcharts should be updated when necessary.
Table look-up	Used to ensure that input data agree with predetermined criteria stored in a table
Tape management system (TMS)	A system software tool that logs, monitors and directs computer tape usage
Test data	Simulated transactions that can be used to test processing logic, computations and controls actually programmed in computer applications Individual programs or an entire system can be tested. Scope Note: This technique includes Integrated Test Facilities (ITFs) and Base Case System Evaluations (BCSEs).
Test generators	Software used to create data to be used in the testing of computer programs
Test programs	Programs that are tested and evaluated before approval into the production environment Scope Note: Test programs, through a series of change control moves, migrate from the test environment to the production environment and become production programs.
Third-party review	An independent audit of the control structure of a service organization, such as a service bureau, with the objective of providing assurance to the users of the service organization that the internal control structure is adequate, effective and sound
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)

© 2012 ISACA All rights reserved.

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 device the size of a credit card that displays a pseudo random number that changes every few minutes.
Token ring topology	A type of local area network (LAN) ring topology in which a frame containing a specific format, called the token, is passed from one station to the next around the ring Scope Note: When a station receives the token, it is allowed to transmit. The station can send as many frames as desired until a predefined time limit is reached. When a station either has no more frames to send or reaches the time limit, it transmits the token. Token passing prevents data collisions that can occur when two computers begin transmitting at the same time.
Topology	The physical layout of how computers are linked together Scope Note: Examples of topology include ring, star and bus.
Transaction log	A manual or automated log of all updates to data files and databases
Transmission Control Protocol/Internet Protocol (TCP/IP)	Provides the basis for the Internet; a set of communication protocols that encompass media access, packet transport, session communication, file transfer, electronic mail (e-mail), terminal emulation, remote file access and network management
Trap door	Unauthorized electronic exit, or doorway, out of an authorized computer program into a set of malicious instructions or programs
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, 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).
Twisted pair	A low-capacity transmission medium; a pair of small, insulated wires that are twisted around each other to minimize interference from other wires in the cable
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

Term	Definition
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.
User awareness	A training process in security-specific issues to reduce security problems; users are often the weakest link in the security chain.
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.
Utility script	A sequence of commands input into a single file to automate a repetitive and specific task Scope Note: The utility script is executed, either automatically or manually, to perform the task. In UNIX, these are known as shell scripts.
Vaccine	A program designed to detect computer viruses
Validity check	Programmed checking of data validity in accordance with predetermined criteria
Value-added network (VAN)	A data communication network that adds processing services such as error correction, data translation and/or storage to the basic function of transporting data
Variable sampling	A sampling technique used to estimate the average or total value of a population based on a sample; a statistical model used to project a quantitative characteristic, such as a monetary amount
Verification	Checks that data are entered correctly
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, a technology that makes it possible to have a voice conversation over the Internet or over any dedicated Internet Protocol (IP) network instead of over dedicated voice transmission lines
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
Waterfall development	Also known as traditional development, a procedure-focused development cycle with formal sign-off at the completion of each level

© 2012 ISACA All rights reserved.

Term	**Definition**
Web Services Description Language (WSDL)	A language formatted with extensible markup language (XML) Used to describe the capabilities of a web service as collections of communication endpoints capable of exchanging messages; WSDL is the language used by Universal Description, Discovery and Integration (UDDI). See also Universal Description, Discovery and Integration (UDDI).
White box testing	A testing approach that uses knowledge of a program/module’s underlying implementation and code intervals to verify its expected behavior
Wide area network (WAN)	A computer network connecting different remote locations that may range from short distances, such as a floor or building, to extremely long transmissions that encompass a large region or several countries
Wide area network (WAN) switch	A data link layer device used for implementing various WAN technologies such as asynchronous transfer mode, point-to-point frame relay solutions, and integrated services digital network (ISDN). Scope Note: WAN switches are typically associated with carrier networks providing dedicated WAN switching and router services to enterprises via T-1 or T-3 connections.
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 that 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 six to eight 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
X.25 Interface	An interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode on some public data networks

© 2012 ISACA All rights reserved.