Term	Definition
Abend	An abnormal end to a computer job; termination of a task prior to its completion because of an error condition that cannot be resolved by recovery facilities while the task is executing.
Acceptable interruption window	The maximum period of time that a system can be unavailable before compromising the achievement of the enterprise's business objectives.
Acceptable Use policy	A policy that establishes an agreement between users and the enterprise and defines for all parties' the ranges of use that are approved before gaining access to a network or the Internet.
Access 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 Notes: Also referred to as access control tables.
Access control table	An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals.
Access Method	The technique used for selecting records in a file, one at a time, for processing, retrieval or storage.The access method is related to, but distinct from, the file organization, which determines how the records are stored.
Access path	The logical route that an end user takes to access computerized information. Scope Notes: 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.
Access server	Provides centralized access control for managing remote access dial-up services.
Accountability	The ability to map a given activity or event back to the responsible party.
Accountable party	The individual, group or entity that is ultimately responsible for a subject matter, process or scope. Scope Notes: Within the IT Assurance Framework (ITAF), the term "management" is equivalent to "accountable party."
Acknowledgment (ACK)	A flag set in a packet to indicate to the sender that the previous packet sent was accepted correctly by the receiver without errors, or that the receiver is now ready to accept a transmission.
Active recovery site (Mirrored)	A recovery strategy that involves two active sites, each capable of taking over the other's workload in the event of a disaster. Scope Notes: Each site will have enough idle processing power to restore data from the other site and to accommodate the excess workload in the event of a disaster.
Active response	A response in which the system either automatically, or in concert with the user, blocks or otherwise affects the progress of a detected attack. Scope Notes: Takes one of three forms: amending the environment, collecting more information or striking back against the user.
Activity	The main actions taken to operate the COBIT process.
Address	Within computer storage, the code used to designate the location of a specific piece of data
Address space	The number of distinct locations that may be referred to with the machine address Scope Notes: For most binary machines, it is equal to 2n, where n is the number of bits in the machine address.
Addressing	The method used to identify the location of a participant in a network. Scope Notes: Ideally, specifies where the participant is located rather than who they are (name) or how to get there (routing).
Adjusting period	The calendar can contain "real" accounting periods and/or adjusting accounting periods. The "real" accounting periods must not overlap and cannot have any gaps between them. Adjusting accounting periods can overlap with other accounting periods. Scope Notes: For example, a period called DEC-93 can be defined that includes 01-DEC-1993 through 31-DEC-1993. An adjusting period called DEC31-93 can also be defined that includes only one day: 31-DEC-1993 through 31-DEC-1993.
Administrative control	The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies.
Adware	A software package that automatically plays, displays or downloads advertising material to a computer after the software is installed on it or while the application is being used. Scope Notes: In most cases, this is done without any notification to the user or without the user's consent. The term adware may also refer to software that displays advertisements, whether or not it does so with the user's consent; such programs display advertisements as an alternative to shareware registration fees. These are classified as adware in the sense of advertising supported software, but not as spyware. Adware in this form does not operate surreptitiously or mislead the user, and it provides the user with a specific service.
Alert situation	The point in an emergency procedure when the elapsed time passes a threshold and the interruption is not resolved. The enterprise entering into an alert situation initiates a series of escalation steps.
Allocation entry	A recurring journal entry used to allocate revenues or costs. Scope Notes: For example, an allocation entry could be defined to allocate costs to each department based on head count.
Alpha	The use of alphabetic characters or an alphabetic character string
Alternate facilities	Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed. Scope Notes: Includes other buildings, offices or data processing centers
Alternate process	Automatic or manual process designed and established to continue critical business processes from point-of-failure to return-to-normal.

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 Notes: In signaling, alternate routing is the process of allocating substitute routes for a given signaling traffic stream in case of failure(s) affecting the normal signaling links or routes of that traffic stream.
American Standard Code for Information Interchange	See ASCII
Amortization	The process of cost allocation that assigns the original cost of an intangible asset to the periods benefited; calculated in the same way as depreciation.
Analog	A transmission signal that varies continuously in amplitude and time and is generated in wave formation. Scope Notes: Analog signals are used in telecommunications
Analytical technique	The examination of ratios, trends, and changes in balances and other values between periods to obtain a broad understanding of the enterprise's financial or operational position and to identify areas that may require further or closer investigation. Scope Notes: Often used when planning the assurance assignment
Anomaly	Unusual or statistically rare.
Anomaly detection	Detection on the basis of whether the system activity matches that defined as abnormal.
Anonymity	The quality or state of not being named or identified.
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.
Appearance	The act of giving the idea or impression of being or doing something.
Appearance of independence	Behavior adequate to meet the situations occurring during audit work (interviews, meetings, reporting, etc.). Scope Notes: An IS auditor should be aware that appearance of independence depends on the perceptions of others and can be influenced by improper actions or associations.
Applet	A program written in a portable, platform-independent computer language, such as Java, JavaScript or Visual Basic. Scope Notes: An applet is usually embedded in an HyperText Markup Language (HTML) page downloaded from web servers and then executed by a browser on client machines to run any web-based application (e.g., generate web page input forms, run audio/video programs, etc.). Applets can only perform a restricted set of operations, thus preventing, or at least minimizing, the possible security compromise of the host computers. However, applets expose the user's machine to risk if not properly controlled by the browser, which should not allow an applet to access a machine's information without prior authorization of the user.
Application	A computer program or set of programs that performs the processing of records for a specific function. Scope Notes: Contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort
Application acquisition review	An evaluation of an application system being acquired or evaluated, that considers such matters as: appropriate controls are designed into the system; the application will process information in a complete, accurate and reliable manner; the application will function as intended; the application will function in compliance with any applicable statutory provisions; the system is acquired in compliance with the established system acquisition process.
Application benchmarking	The process of establishing the effective design and operation of automated controls within an application.
Application controls	The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved.
Application development review	An evaluation of an application system under development that considers matters such as: appropriate controls are designed into the system; the application will process information in a complete, accurate and reliable manner; the application will function as intended; the application will function in compliance with any applicable statutory provisions; the system is developed in compliance with the established system development life cycle process.
Application implementation review	An evaluation of any part of an implementation project. Scope Notes: Examples include project management, test plans and user acceptance testing (UAT) procedures.
Application layer	In the Open Systems Interconnection (OSI) communications model, the application layer provides services for an application program to ensure that effective communication with another application program in a network is possible. Scope Notes: The application layer is not the application that is doing the communication; a service layer that provides these services.
Application maintenance review	An evaluation of any part of a project to perform maintenance on an application system. Scope Notes: Examples include project management, test plans and user acceptance testing (UAT) procedures.
Application or managed service provider (ASP/MSP)	A third party that delivers and manages applications and computer services, including security services to multiple users via the Internet or a private network.
Application program	A program that processes business data through activities such as data entry, update or query. Scope Notes: Contrasts with systems programs, such as an operating system or network control program, and with utility programs such as copy or sort
Application programming	The act or function of developing and maintaining application programs in production.

Application programming interface (API)	A set of routines, protocols and tools referred to as "building blocks" used in business application software development. Scope Notes: 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 proxy	A service that connects programs running on internal networks to services on exterior networks by creating two connections, one from the requesting client and another to the destination service.
Application security	Refers to the security aspects supported by the application, primarily with regard to the roles or responsibilities and audit trails within the applications.
Application service provider (ASP)	Also known as managed service provider (MSP), it deploys, hosts and manages access to a packaged application to multiple parties from a centrally managed facility. Scope Notes: The applications are delivered over networks on a subscription basis.
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 Notes: 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.
Application system	An integrated set of computer programs designed to serve a particular function that has specific input, processing and output activities. Scope Notes: Examples include general ledger, manufacturing resource planning and human resource (HR) management.
Architecture	Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support enterprise objectives.
Arithmetic logic unit (ALU)	The area of the central processing unit that performs mathematical and analytical operations
Artificial intelligence	Advanced computer systems that can simulate human capabilities, such as analysis, based on a predetermined set of rules
ASCII	Representing 128 characters, the American Standard Code for Information Interchange (ASCII) code normally uses 7 bits. However, some variations of the ASCII code set allow 8 bits. This 8-bit ASCII code allows 256 characters to be represented.
Assembler	A program that takes as input a program written in assembly language and translates it into machine code or machine language
Assembly Language	A low-level computer programming language which uses symbolic code and produces machine instructions.
Assessment	A broad review of the different aspects of a company or function that includes elements not covered by a structured assurance initiative. Scope Notes: May include opportunities for reducing the costs of poor quality, employee perceptions on quality aspects, proposals to senior management on policy, goals, etc.
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.
Assurance	Pursuant to an accountable relationship between two or more parties, an IT audit and assurance professional is engaged to issue a written communication expressing a conclusion about the subject matters for which the accountable party is responsible. Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter. Scope Notes: Assurance engagements could include support for audited financial statements, reviews of controls, compliance with required standards and practices, and compliance with agreements, licenses, legislation and regulation.
Assurance initiative	An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the enterprise. Scope Notes: Examples may include financial, performance, compliance and system security engagements.
Asymmetric key (public key)	A cipher technique in which different cryptographic keys are used to encrypt and decrypt a message Scope Notes: See public key encryption.
Asynchronous Transfer Mode (ATM)	A high-bandwidth low-delay switching and multiplexing technology that allows integration of real-time voice and video as well as data. It is a data link layer protocol. Scope Notes: ATM is a protocol-independent transport mechanism. It allows high-speed data transfer rates at up to 155 Mbit/s. The acronym ATM should not be confused with the alternate usage for ATM, which refers to an automated teller machine.
Asynchronous transmission	Character-at-a-time transmission.
Attest reporting engagement	An engagement in which an IS auditor is engaged to either examine management's assertion regarding a particular subject matter or the subject matter directly. Scope Notes: The IS auditor's report consists of an opinion on one of the following: The subject matter. These reports relate directly to the subject matter itself rather than to an assertion. In certain situations management will not be able to make an assertion over the subject of the engagement. An example of this situation is when IT services are outsourced to third party. Management will not ordinarily be able to make an assertion over the controls that the third party is responsible for. Hence, an IS auditor would have to report directly on the subject matter rather than on an assertion.
Attitude	Way of thinking, behaving, feeling, etc.
Attribute sampling	Method to select a portion of a population based on the presence or absence of a certain characteristic

Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met. Scope Notes: May be carried out by internal or external groups.
Audit accountability	Performance measurement of service delivery including cost, timeliness and quality against agreed service levels.
Audit authority	A statement of the position within the enterprise, including lines of reporting and the rights of access.
Audit charter	A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal audit activity. </br/>Scope Notes: The charter should: </br/>- Establish the internal audit funtion's position within the enterprise </br/>- Authorise access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagementsDefine the scope of audit function's activities
Audit evidence	The information used to support the audit opinion.
Audit expert systems	Expert or decision support systems that can be used to assist IS auditors in the decision-making process by automating the knowledge of experts in the field. Scope Notes: This technique includes automated risk analysis, systems software and control objectives software packages.
Audit objective	The specific goal(s) of an audit. Scope Notes: 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 Notes: 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 responsibility	The roles, scope and objectives documented in the service level agreement (SLA) between management and audit.
Audit risk	The risk of reaching an incorrect conclusion based upon audit findings. </br/>Scope Notes: The three components of audit risk are: - Control risk - Detection risk - Inherent risk
Audit sampling	The application of audit procedures to less than 100 percent of the items within a population to obtain audit evidence about a particular characteristic of the population.
Audit trail	A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source
Audit universe	An inventory of audit areas that is compiled and maintained to identify areas for audit during the audit planning process. Scope Notes: Traditionally, the list includes all financial and key operational systems as well as other units that would be audited as part of the overall cycle of planned work. The audit universe serves as the source from which the annual audit schedule is prepared. The universe will be periodically revised to reflect changes in the overall risk profile.
Auditability	The level to which transactions can be traced and audited through a system.
Auditable unit	Subjects, units or systems that are capable of being defined and evaluated. Scope Notes: Auditable units may include: - Policies, procedures and practices - Cost centers, profit centers and investment centers - General ledger account balances - Information systems (manual and computerized) - Major contracts and programs - Organizational units, such as product or service lines - Functions, such as information technology (IT), purchasing, marketing, production, finance, accounting and human resources (HR) - Transaction systems for activities, such as sales, collection, purchasing, disbursement, inventory and cost accounting, production, treasury, payroll, and capital assets - Financial statements - Laws and regulations
Authentication	1. The act of verifying identity, i.e., user, system. Scope Notes: 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, the user's eligibility to access computerized information. Scope Notes: 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.
Automated application controls	Controls that have been programmed and embedded within an application.
Availability	Ensuring timely and reliable access to and use of information
Awareness	Being acquainted with, mindful of, conscious of and well informed on a specific subject, which implies knowing and understanding a subject and acting accordingly.
Accountability of governance	Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritization and decision making; and monitoring performance, compliance and progress against plans. In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson. Scope Notes: COBIT 5 perspective
Alignment	A state where the enablers of governance and management of enterprise IT support the goals and strategies of the enterprise Scope Notes: COBIT 5 perspective
Application architecture	Description of the logical grouping of capabilities that manage the objects necessary to process information and support the enterprise's objectives. Scope Notes: COBIT 5 perspective

Architecture board	A group of stakeholders and experts who are accountable for guidance on enterprise-architecture-related matters and decisions, and for setting architectural policies and standards Scope Notes: COBIT 5 perspective
Advanced Encryption Standard (AES)	A public algorithm that supports keys from 128 bits to 256 bits in size
Advanced persistent threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives using multiple attack vectors (NIST SP800-61). </br/>Scope Notes: The APT: 1. pursues its objectives repeatedly over an extended period of time 2. Adapts to defenders' efforts to resist it 3. is determined to maintain the level of interaction needed to execute its objectives
Adversary	A threat agent
Assertion	Any formal declaration or set of declarations about the subject matter made by management. </br/>Scope Notes: Assertions should usually be in writing and commonly contain a list of specific attributes about the subject matter or about a process involving the subject matter.
Assurance engagement	An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the enterprise. </br/>Scope Notes: Examples may include financial, performance, compliance and system security engagements
Attack	An actual occurrence of an adverse event
Attack mechanism	A method used to deliver the exploit. Unless the attacker is personally performing the attack, an attack mechanism may involve a payload, or container, that delivers the exploit to the target.
Attack vector	A path or route used by the adversary to gain access to the target (asset). </br/>Scope Notes: There are two types of attack vectors: ingress and egress (also known as data exfiltration)
Attenuation	Reduction of signal strength during transmission
Audit subject matter risk	Risk relevant to the area under review: - Business risk (customer capability to pay, credit worthiness, market factors, etc.) - Contract risk (liability, price, type, penalties, etc.) - Country risk (political, environment, security, etc.) - Project risk (resources, skill set, methodology, product stability, etc.) - Technology risk (solution, architecture, hardware and software infrastructure network, delivery channels, etc.). </br/>Scope Notes: See inherent risk
Auditor's opinion	A formal statement expressed by the IS audit or assurance professional that describes the scope of the audit, the procedures used to produce the report and whether or not the findings support that the audit criteria have been met. </br/>Scope Notes: The types of opinions are: - Unqualified opinion: Notes no exceptions or none of the exceptions noted aggregate to a significant deficiency - Qualified opinion: Notes exceptions aggregated to a significant deficiency (but not a material weakness) - Adverse opinion: Notes one or more significant deficiencies aggregating to a material weakness
Authenticity	Undisputed authorship
Application containerization	A mechanism that is used to isolate applications from each other within the context of a running operating system instance. In much the same way that a logical partition (LPAR) provides segmentation of system resources in mainframes, a computing environment employing containers segments and isolates the underlying system services so that they are logically sequestered from each other.
asymmetric cipher	Most implementations of asymmetric ciphers combine a widely distributed public key and a closely held, protected private key. A message that is encrypted by the public key can only be decrypted by the mathematically related, counterpart
Backbone	The main communication channel of a digital network. The part of a network that handles the major traffic Scope Notes: 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.
Backup center	An alternate facility to continue IT/IS operations when the primary data processing (DP) center is unavailable.
Badge	A card or other device that is presented or displayed to obtain access to an otherwise restricted facility, as a symbol of authority (e.g., the police), or as a simple means of identification. Scope Notes: Also used in advertising and publicity.
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).
Bar code	A printed machine-readable code that consists of parallel bars of varied width and spacing.
Base case	A standardized body of data created for testing purposes. Scope Notes: Users normally establish the data. Base cases validate production application systems and test the ongoing accurate operation of the system.

Baseband	A form of modulation in which data signals are pulsed directly on the transmission medium without frequency division and usually utilize a transceiver. Scope Notes: The entire bandwidth of the transmission medium (e.g., coaxial cable) is utilized for a single channel.
Batch control	Correctness checks built into data processing systems and applied to batches of input data, particularly in the data preparation stage. Scope Notes: 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 Notes: 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).
Benchmark	A test that has been designed to evaluate the performance of a system. Scope Notes: In a benchmark test, a system is subjected to a known workload and the performance of the system against this workload is measured. Typically, the purpose is to compare the measured performance with that of other systems that have been subject to the same benchmark test.
Benchmarking	A systematic approach to comparing enterprise performance against peers and competitors in an effort to learn the best ways of conducting business. Scope Notes: Examples include benchmarking of quality, logistic efficiency and various other metrics.
Benefit	In business, an outcome whose nature and value (expressed in various ways) are considered advantageous by an enterprise.
Best practice	A proven activity or process that has been successfully used by multiple enterprises.
Binary code	A code whose representation is limited to 0 and 1.
Biometric locks	Door and entry locks that are activated by such biometric features as voice, eye retina, fingerprint or signature.
Biometrics	A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint.
Bit-stream image	Bit-stream backups, also referred to as mirror image backups, involve the backup of all areas of a computer hard disk drive or other type of storage media. Scope Notes: Such backups exactly replicate all sectors on a given storage device including all files and ambient data storage areas.
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 Notes: Broadband generally requires the use of a modem.
Brouter	Device that performs the functions of both a bridge and a router. Scope Notes: 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.
Browser	A computer program that enables the user to retrieve information that has been made publicly available on the Internet; also, that permits multimedia (graphics) applications on the World Wide Web.
Brute force	A class of algorithms that repeatedly try all possible combinations until a solution is found.
Brute force attack	Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found.
Budget	Estimated cost and revenue amounts for a given range of periods and set of books. Scope Notes: There can be multiple budget versions for the same set of books.
Budget formula	A mathematical expression used to calculate budget amounts based on actual results, other budget amounts and statistics. Scope Notes: With budget formulas, budgets using complex equations, calculations and allocations can be automatically created.
Budget hierarchy	A group of budgets linked together at different levels such that the budgeting authority of a lower-level budget is controlled by an upper-level budget.
Budget organization	An entity (department, cost center, division or other group) responsible for entering and maintaining budget data.
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 Notes: In a program, buffers are reserved areas of random access memory (RAM) that hold data while they are being processed.

Buffer overflow	Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Scope Notes: Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
Bulk data transfer	A data recovery strategy that includes a recovery from complete backups that are physically shipped offsite once a week. Scope Notes: Specifically, logs are batched electronically several times daily, and then loaded into a tape library located at the same facility as the planned recovery.
Bus	Common path or channel between hardware devices. Scope Notes: Can be located between components internal to a computer or between external computers in a communication network.
Bus configuration	All devices (nodes) are linked along one communication line where transmissions are received by all attached nodes. Scope Notes: 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 balanced scorecard	A tool for managing organizational strategy that uses weighted measures for the areas of financial performance (lag) indicators, internal operations, customer measurements, learning and growth (lead) indicators, combined to rate the enterprise.
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 control	The policies, procedures, practices and organizational structures designed to provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented or detected.
Business dependency assessment	A process of identifying resources critical to the operation of a business process.
Business function	An activity that an enterprise does, or needs to do, to achieve its objectives.
Business goal	The translation of the enterprise's mission from a statement of intention into performance targets and results.
Business impact	The net effect, positive or negative, on the achievement of business objectives.
Business impact analysis (BIA)	A process to determine the impact of losing the support of any resource. Scope Notes: 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 impact analysis/assessment (BIA)	Evaluating the criticality and sensitivity of information assets. An exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and the supporting system. Scope Notes: This process also includes addressing: - Income loss - Unexpected expense - Legal issues (regulatory compliance or contractual) - Interdependent processes - Loss of public reputation or public confidence
Business interruption	Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) that disrupts the normal course of business operations at an enterprise.
Business Model for Information Security (BMIS)	A holistic and business-oriented model that supports enterprise governance and management information security, and provides a common language for information security professionals and business management.
Business objective	A further development of the business goals into tactical targets and desired results and outcomes.
Business process	An inter-related set of cross-functional activities or events that result in the delivery of a specific product or service to a customer.
Business process integrity	Controls over the business processes that are supported by the enterprise resource planning system (ERP).
Business process owner	The individual responsible for identifying process requirements, approving process design and managing process performance. Scope Notes: Must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities
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.
Business risk	A probable situation with uncertain frequency and magnitude of loss (or gain).
Business service provider (BSP)	An application service provider (ASP) that also provides outsourcing of business processes such as payment processing, sales order processing and application development.
Business sponsor	The individual accountable for delivering the benefits and value of an IT-enabled business investment program to the enterprise.

Business-to-business	Transactions in which the acquirer is an enterprise or an individual operating in the ambits of his/her professional activity. In this case, laws and regulations related to consumer protection are not applicable. Scope Notes: The contract’s general terms should be communicated to the other party and specifically approved. Some companies require the other party to fill out check-boxes where there is a description such as "I specifically approve the clauses" This is not convincing; the best solution is the adoption of a digital signature scheme, which allows the approval of clauses and terms with the non-repudiation condition.
Business-to-consumer	Selling processes in which the involved parties are the enterprise, which offers goods or services, and a consumer. In this case there is comprehensive legislation that protects the consumer. Scope Notes: Comprehensive legislation includes: - Regarding contracts established outside the merchant’s property (such as the right to end the contract with full refund or the return policy for goods) - Regarding distance contracts (such as rules that establish how a contract should be written, specific clauses and the need to transmit to the consumer and approve it) - Regarding electronic form of the contract (such as on the Internet, the possibility for the consumer to exit from the procedure without having his/her data recorded)
Business-to-consumer e-commerce (B2C)	Refers to the processes by which enterprises conduct business electronically with their customers and/or public at large using the Internet as the enabling technology.
Bypass label processing (BLP)	A technique of reading a computer file while bypassing the internal file/data set label. This process could result in bypassing of the security access control system.
Baseline architecture	The existing description of the fundamental underlying design of the components of the business system before entering a cycle of architecture review and redesign Scope Notes: COBIT 5 perspective
Benefits realization	One of the objectives of governance. The bringing about of new benefits for the enterprise, the maintenance and extension of existing forms of benefits, and the elimination of those initiatives and assets that are not creating sufficient value Scope Notes: COBIT 5 perspective
Business continuity	Preventing, mitigating and recovering from disruption Scope Notes: The terms 'business resumption planning', 'disaster recovery planning' and 'contingency planning' also may be used in this context; they focus on recovery aspects of continuity, and for that reason the 'resilience' aspect should also be taken into account. COBIT 5 perspective
Business process control	The policies, procedures, practices and organizational structures designed to provide reasonable assurance that a business process will achieve its objectives. Scope Notes: COBIT 5 perspective
Back door	A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions
Bastion	System heavily fortified against attacks
Block cipher	A public algorithm that operates on plaintext in blocks (strings or groups) of bits
Botnet	A term derived from “robot network;” is a large automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as a denial-of-service attack on selected victims
Boundary	Logical and physical controls to define a perimeter between the organization and the outside world
Bridge	Data link layer device developed in the early 1980s to connect local area networks (LANs) or create two separate LAN or wide area network (WAN) network segments from a single segment to reduce collision domains. </br/>Scope Notes: A bridge acts as a store-and-forward device in moving frames toward their destination. This is achieved by analyzing the MAC header of a data packet, which represents the hardware address of an NIC.
Bring your own device (BYOD)	An enterprise policy used to permit partial or full integration of user-owned mobile devices for business purposes
Broadcast	A method to distribute information to multiple recipients simultaneously
Blockchain	A distributed, protected journaling and ledger system. Use of blockchain technologies can enable anything from digital currency (e.g. Bitcoin) to any other value-bearning transaction.
Base58 Encoding	Base58 Encoding is a binary-to-text encoding process that converts long bit sequences into alphanumeric text, which is easier for users
Base64 Encoding	Base64 Encoding is a binary-to-text encoding process that converts long bit sequences into alphanumeric text.
Cadbury	The Committee on the Financial Aspects of Corporate Governance, set up in May 1991 by the UK Financial Reporting Council, the London Stock Exchange and the UK accountancy profession, was chaired by Sir Adrian Cadbury and produced a report on the subject commonly known in the UK as the Cadbury Report.
Capability	An aptitude, competency or resource that an enterprise may possess or require at an enterprise, business function or individual level that has the potential, or is required, to contribute to a business outcome and to create value.

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. 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. </br/>Scope Notes: 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.
Capital expenditure/expense (CAPEX)	An expenditure that is recorded as an asset because it is expected to benefit more than the current period. The asset is then depreciated or amortized over the expected useful life of the asset.
Card swipe	A physical control technique that uses a secured card or ID to gain access to a highly sensitive location. Scope Notes: 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.
Cathode ray tube (CRT)	A vacuum tube that displays data by means of an electron beam striking the screen, which is coated with suitable phosphor material or a device similar to a television screen on which data can be displayed.
Central processing unit (CPU)	Computer hardware that houses the electronic circuits that control/direct all operations of the computer system.
Centralized data processing	Identified by one central processor and databases that form a distributed processing configuration.
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 Notes: 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 Notes: 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.
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 Notes: 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 Notes: 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 Notes: 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.
Channel service unit/dgital service unit (CSU/DSU)	Interfaces at the physical layer of the open systems interconnection (OSI) reference model, data terminal equipment (DTE) to data circuit terminating equipment (DCE), for switched carrier networks.
Chargeback	The redistribution of expenditures to the units within a company that gave rise to them. Scope Notes: Chargeback is important because without such a policy, misleading views may be given as to the real profitability of a product or service because certain key expenditures will be ignored or calculated according to an arbitrary formula.

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 Notes: Check digit control is effective in detecting transposition and transcription errors.
Check digit verification (self-checking digit)	A programmed edit or routine that detects transposition and transcription errors by calculating and checking the check digit.
Checklist	A list of items that is used to verify the completeness of a task or goal. Scope Notes: Used in quality assurance (and in general, in information systems audit), to check process compliance, code standardization and error prevention, and other items for which consistency processes or standards have been defined
Checkpoint restart procedures	A point in a routine at which sufficient information can be stored to permit restarting the computation from that point.
Chief executive officer (CEO)	The highest ranking individual in an enterprise.
Chief financial officer (CFO)	The individual primarily responsible for managing the financial risk of an enterprise.
Chief information officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy, aligning IT and business strategies, and planning, resourcing and managing the delivery of IT services, information and the deployment of associated human resources. Scope Notes: In some cases, the CIO role has been expanded to become the chief knowledge officer (CKO) who deals in knowledge, not just information. Also see chief technology officer (CTO).
Chief technology officer (CTO)	The individual who focuses on technical issues in an enterprise. Scope Notes: Often viewed as synonymous with chief information officer (CIO)
Ciphertext	Information generated by an encryption algorithm to protect the plaintext and that is unintelligible to the unauthorized reader.
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 Notes: 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.
Cleartext	Data that is not encrypted. Also known as plaintext.
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 Notes: 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 Notes: 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 Notes: Has a greater transmission capacity than standard twisted-pair cables, but has a limited range of effective distance
COBIT	1. COBIT or formerly known as Control Objectives for Information and Related Technology (COBIT), now used only as the acronym in its fifth iteration. A complete, internationally accepted framework for governing and managing enterprise information and technology (IT) that supports enterprise executives and management in their definition and achievement of business goals and related IT goals. COBIT describes five principles and seven enablers that support enterprises in the development, implementation, and continuous improvement and monitoring of good IT-related governance and management practices Scope Notes: Earlier versions of COBIT focused on control objectives related to IT processes, management and control of IT processes and IT governance aspects. Adoption and use of the COBIT framework are supported by guidance from a growing family of supporting products. (See www.isaca.org/cobit for more information.) 2. COBIT 4.1 and earlier: Formally known as Control Objectives for Information and related Technology (COBIT). A complete, internationally accepted process framework for IT that supports business and IT executives and management in their definition and achievement of business goals and related IT goals by providing a comprehensive IT governance, management, control and assurance model. COBIT describes IT processes and associated control objectives, management guidelines (activities, accountabilities, responsibilities and performance metrics) and maturity models. COBIT supports enterprise management in the development, implementation, continuous improvement and monitoring of good IT-related practices. Scope Notes: Adoption and use of the COBIT framework are supported by guidance for executives and management (Board Briefing on IT Governance, 2nd Edition), IT governance implementers (COBIT Quickstart, 2nd Edition; IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition; and COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance), and IT assurance and audit professionals (IT Assurance Guide Using COBIT). Guidance also exists to support its applicability for certain legislative and regulatory requirements (e.g., IT Control Objectives for Sarbanes-Oxley, IT Control Objectives for Basel II) and its relevance to information security (COBIT Security Baseline). COBIT is mapped to other frameworks and standards to illustrate complete coverage of the IT management life cycle and support its use in enterprises using multiple IT-related framework and standards.
CoCo	Criteria of Control, published by the Canadian Institute of Chartered Accountants in 1995.

Coevolving	Originated as a biological term, refers to the way two or more ecologically interdependent species become intertwined over time. Scope Notes: As these species adapt to their environment they also adapt to one another. Today's multi-business companies need to take their cue from biology to survive. They should assume that links among businesses are temporary and that the number of connections-not just their content-matters. Rather than plan collaborative strategy from the top, as traditional companies do, corporate executives in coevolving companies should simply set the context and let collaboration (and competition) emerge from business units.
Coherence	Establishing a potent binding force and sense of direction and purpose for the enterprise, relating different parts of the enterprise to each other and to the whole to act as a seemingly unique entity.
Cohesion	The extent to which a system unit--subroutine, program, module, component, subsystem--performs a single dedicated function. Scope Notes: 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 Notes: 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.
Combined Code on Corporate Governance	The consolidation in 1998 of the "Cadbury," "Greenbury" and "Hampel" Reports. Scope Notes: Named after the Committee Chairs, these reports were sponsored by the UK Financial Reporting Council, the London Stock Exchange, the Confederation of British Industry, the Institute of Directors, the Consultative Committee of Accountancy Bodies, the National Association of Pension Funds and the Association of British Insurers to address the financial aspects of corporate governance, directors' remuneration and the implementation of the Cadbury and Greenbury recommendations.
Communication processor	A computer embedded in a communications system that generally performs the basic tasks of classifying network traffic and enforcing network policy functions. Scope Notes: An example is the message data processor of a defense digital network (DDN) switching center. More advanced communication processors may perform additional functions.
Communications controller	Small computers used to connect and coordinate communication links between distributed or remote devices and the main computer, thus freeing the main computer from this overhead function.
Community strings	Authenticate access to management information base (MIB) objects and function as embedded passwords. Scope Notes: Examples are: - Read-only (RO)-Gives read access to all objects in the MIB except the community strings, but does not allow write access - Read-write (RW)-Gives read and write access to all objects in the MIB, but does not allow access to the community strings - Read-write-all-Gives read and write access to all objects in the MIB, including the community strings (only valid for Catalyst 4000, 5000 and 6000 series switches) Simple Network Management Protocol (SNMP) community strings are sent across the network in cleartext. The best way to protect an operating system (OS) software-based device from unauthorized SNMP management is to build a standard IP access list that includes the source address of the management station(s). Multiple access lists can be defined and tied to different community strings. If logging is enabled on the access list, then log messages are generated every time that the device is accessed from the management station. The log message records the source IP address of the packet.
Comparison program	A program for the examination of data, using logical or conditional tests to determine or to identify similarities or differences.
Compensating control	An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions.
Competencies	The strengths of an enterprise or what it does well. Scope Notes: Can refer to the knowledge, skills and abilities of the assurance team or individuals conducting the work.
Compiler	A program that translates programming language (source code) into machine executable instructions (object code).
Completely Automated Public Touring test to tell Computers and Humans Apart (CAPTCHA)	A type of challenge-response test used in computing to ensure that the response is not generated by a computer. An example is the site request for web site users to recognize and type a phrase posted using various challenging-to-read fonts.
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.
Component	A general term that is used to mean one part of something more complex. Scope Notes: For example, a computer system may be a component of an IT service, or an application may be a component of a release unit. Components are co-operating packages of executable software that make their services available through defined interfaces. Components used in developing systems may be commercial off-the-shelf software (COTS) or may be purposely built. However, the goal of component-based development is to ultimately use as many pre-developed, pretested components as possible.
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.
Computationally greedy	Requiring a great deal of computing power; processor intensive.

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 Notes: 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 server	1. A computer dedicated to servicing requests for resources from other computers on a network. Servers typically run network operating systems. 2. A computer that provides services to another computer (the client).
Computer-aided software engineering (CASE)	The use of software packages that aid in the development of all phases of an information system. Scope Notes: 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.
Concurrent access	A fail-over process, in which all nodes run the same resource group (there can be no [Internet Protocol] IP or [mandatory access control] MAC address in a concurrent resource group) and access the external storage concurrently.
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.
Configurable control	Typically, an automated control that is based on, and therefore dependent on, the configuration of parameters within the application system.
Configuration item (CI)	Component of an infrastructure-or an item, such as a request for change, associated with an infrastructure-which is (or is to be) under the control of configuration management. Scope Notes: May vary widely in complexity, size and type, from an entire system (including all hardware, software and documentation) to a single module or a minor hardware component
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.
Consulted	In a RACI (responsible, accountable, consulted, informed) chart, refers to those people whose opinions are sought on an activity (two-way communication).
Content filtering	Controlling access to a network by analyzing the contents of the incoming and outgoing packets and either letting them pass or denying them based on a list of rules. Scope Notes: Differs from packet filtering in that it is the data in the packet that are analyzed instead of the attributes of the packet itself (e.g., source/target IP address, transmission control protocol [TCP] flags)
Context	The overall set of internal and external factors that might influence or determine how an enterprise, entity, process or individual acts Scope Notes: Context includes: - technology context (technological factors that affect an enterprise's ability to extract value from data) - data context (data accuracy, availability, currency and quality) - skills and knowledge (general experience and analytical, technical and business skills), - organizational and cultural context (political factors and whether the enterprise prefers data to intuition) - strategic context (strategic objectives of the enterprise) COBIT 5 perspective
Contingency plan	A plan used by an enterprise or business unit to respond to a specific systems failure or disruption.
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.
Continuity	Preventing, mitigating and recovering from disruption. Scope Notes: 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 availability	Nonstop service, with no lapse in service; the highest level of service in which no downtime is allowed.

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 Notes: 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 center	Hosts the recovery meetings where disaster recovery operations are managed.
Control framework	A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an enterprise.
Control group	Members of the operations area who are responsible for the collection, logging and submission of input for the various user groups.
Control objective	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process.
Control Objectives for Enterprise Governance	A discussion document that sets out an "enterprise governance model" focusing strongly on both the enterprise business goals and the information technology enablers that facilitate good enterprise governance, published by the Information Systems Audit and Control Foundation in 1999.
Control perimeter	The boundary defining the scope of control authority for an entity. Scope Notes: For example, if a system is within the control perimeter, the right and ability exist to control it in response to an attack.
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).
Control risk self-assessment	A method/process by which management and staff of all levels collectively identify and evaluate risk and controls with their business areas. This may be under the guidance of a facilitator such as an auditor or risk manager.
Control section	The area of the central processing unit (CPU) that executes software, allocates internal memory and transfers operations between the arithmetic-logic, internal storage and output sections of the computer.
Control weakness	A deficiency in the design or operation of a control procedure. Control weaknesses can potentially result in risk relevant to the area of activity not being reduced to an acceptable level (relevant risk threatens achievement of the objectives relevant to the area of activity being examined). Control weaknesses can be material when the design or operation of one or more control procedures does not reduce to a relatively low level the risk that misstatements caused by illegal acts or irregularities may occur and not be detected by the related control procedures.
Cookie	A message kept in the web browser for the purpose of identifying users and possibly preparing customized web pages for them. Scope Notes: 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 exchange rate	An exchange rate that can be used optionally to perform foreign currency conversion. The corporate exchange rate is generally a standard market rate determined by senior financial management for use throughout the enterprise.
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.
Corporate security officer (CSO)	Responsible for coordinating the planning, development, implementation, maintenance and monitoring of the information security program.
Corrective control	Designed to correct errors, omissions and unauthorized uses and intrusions, once they are detected.
COSO	Committee of Sponsoring Organizations of the Treadway Commission. Scope Notes: COSO's "Internal Control--Integrated Framework" is an internationally accepted standard for corporate governance. See www.coso.org.
Countermeasure	Any process that directly reduces a threat or vulnerability.
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 Notes: 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.
Coverage	The proportion of known attacks detected by an intrusion detection system (IDS).
Crack	To "break into" or "get around" a software program. Scope Notes: For example, there are certain newsgroups that post serial numbers for pirated versions of software. A cracker may download this information in an attempt to crack the program so he/she can use it. It is commonly used in the case of cracking (unencrypting) a password or other sensitive data.

Credentialed analysis	In vulnerability analysis, passive monitoring approaches in which passwords or other access credentials are required. Scope Notes: Usually involves accessing a system data object
Criteria	The standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter. Scope Notes: Criteria should be: Objective--free from bias, Measurable--provide for consistent measurement, Complete--include all relevant factors to reach a conclusion, Relevant--relate to the subject matter.In an attestation engagement, benchmarks against which management's written assertion on the subject matter can be evaluated. The practitioner forms a conclusion concerning subject matter by referring to suitable criteria.
Critical functions	Business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the enterprise.
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.
Criticality analysis	An analysis to evaluate resources or business functions to identify their importance to the enterprise, and the impact if a function cannot be completed or a resource is not available.
Cross-certification	A certificate issued by one certificate authority (CA) to a second CA so that users of the first certification authority are able to obtain the public key of the second CA and verify the certificates it has created. Scope Notes: Often refers to certificates issued to each other by two CAs at the same level in a hierarchy
Cross-site request forgery (CSRF)	A type of malicious exploit of a web site whereby unauthorized commands are transmitted from a user that the web site trusts (also known as a one-click attack or session riding); acronym pronounced "sea-surf".
Cryptography	The art of designing, analyzing and attacking cryptographic schemes.
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.
Cybercop	An investigator of activities related to computer crime.
Code of ethics	A document designed to influence individual and organizational behavior of employees, by defining organizational values and the rules to be applied in certain situations. Scope Notes: A code of ethics is adopted to assist those in the enterprise called upon to make decisions understand the difference between 'right' and 'wrong' and to apply this understanding to their decisions. COBIT 5 perspective
Competence	The ability to perform a specific task, action or function successfully Scope Notes: COBIT 5 perspective
Control	The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature. Scope Notes: Also used as a synonym for safeguard or countermeasure. See also Internal control.
Culture	A pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things Scope Notes: COBIT 5 perspective
Chief Information Security Officer (CISO)	The person in charge of information security within the enterprise
Chief Security Officer (CSO)	The person usually responsible for all security matters both physical and digital in an enterprise
Cipher	An algorithm to perform encryption
Cloud computing	Convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction
Collision	The situation that occurs when two or more demands are made simultaneously on equipment that can handle only one at any given instant (Federal Standard 1037C)
Common Attack Pattern Enumeration and Classification (CAPEC)	A catalogue of attack patterns as “an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed” published by the MITRE Corporation
Compartmentalization	A process for protecting very-high value assets or in environments where trust is an issue. Access to an asset requires two or more processes, controls or individuals.
Compliance	Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies
Compliance documents	Policies, standard and procedures that document the actions that are required or prohibited. Violations may be subject to disciplinary actions.
Consumerization	A new model in which emerging technologies are first embraced by the consumer market and later spread to the business
Containment	Actions taken to limit exposure after an incident has been identified and confirmed
Criticality	The importance of a particular asset or function to the enterprise, and the impact if that asset or function is not available
Cross-site scripting (XSS)	A type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. </br/>Scope Notes: Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. (OWASP)
Cryptosystem	A pair of algorithms that take a key and convert plaintext to ciphertext and back
Cyberespionage	Activities conducted in the name of security, business, politics or technology to find information that ought to remain secret. It is not inherently military.

Cybersecurity	The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems
Cybersecurity architecture	Describes the structure, components and topology (connections and layout) of security controls within an enterprise's IT infrastructure. </br/>Scope Notes: The security architecture shows how defense-in-depth is implemented and how layers of control are linked and is essential to designing and implementing security controls in any complex environment.
Cyberwarfare	Activities supported by military organizations with the purpose to threat the survival and well-being of society/foreign entity
CACS	http://www.isaca.org/ecommerce/Pages/north-america-cacs.aspx
checksum	A checksum value is generated by algorithm and associated with an input value and/or whole input file. The checksum value can be used to assess its corresponding input data or file at a later date and verify that the input has not been maliciously altered. It is highly improbable that an unauthorized party could alter the input without also altering the corresponding checksum output. If a subsequent checksum value no longer matches the initial value, the input may have been altered or corrupted.
Damage evaluation	The determination of the extent of damage that is necessary to provide for an estimation of the recovery time frame and the potential loss to the enterprise.
Dashboard	A tool for setting expectations for an enterprise at each level of responsibility and continuous monitoring of the performance against set targets.
Data analysis	Typically in large enterprises in which the amount of data processed by the enterprise resource planning (ERP) system is extremely voluminous, analysis of patterns and trends proves to be extremely useful in ascertaining the efficiency and effectiveness of operations. Scope Notes: Most ERP systems provide opportunities for extraction and analysis of data (some with built-in tools) through the use of tools developed by third parties that interface with the ERP systems.
Data classification	The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the enterprise.
Data classification scheme	An enterprise scheme for classifying data by factors such as criticality, sensitivity and ownership.
Data communications	The transfer of data between separate computer processing sites/devices using telephone lines, microwave and/or satellite links.
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 Notes: 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 Notes: 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 flow	The flow of data from the input (in Internet banking, ordinarily user input at his/her desktop) to output (in Internet banking, ordinarily data in a bank's central database).Data flow includes travel through the communication lines, routers, switches and firewalls as well as processing through various applications on servers, which process the data from user fingers to storage in a bank's central database.
Data integrity	The property that data meet with a priority expectation of quality and that the data can be relied on.
Data leakage	Siphoning out or leaking information by dumping computer files or stealing computer reports and tapes.
Data normalization	A structured process for organizing data into tables in such a way that it preserves the relationships among the data.
Data owner	The individual(s), normally a manager or director, who has responsibility for the integrity, accurate reporting and use of computerized data.
Data security	Those controls that seek to maintain confidentiality, integrity and availability of information.
Data structure	The relationships among files in a database and among data items within each file.
Data warehouse	A generic term for a system that stores, retrieves and manages large volumes of data. Scope Notes: Data warehouse software often includes sophisticated comparison and hashing techniques for fast searches as well as for advanced filtering.
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.
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 Notes: 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.
Database specifications	These are the requirements for establishing a database application. They include field definitions, field requirements and reporting requirements for the individual information in the database.
Datagram	A packet (encapsulated with a frame containing information), that is transmitted in a packet-switching network from source to destination.
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.
Decryption key	A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption.
Default	A computer software setting or preference that states what will automatically happen in the event that the user has not stated another preference. For example, a computer may have a default setting to launch or start Netscape whenever a GIF file is opened; however, if using Photoshop is the preference for viewing a GIF file, the default setting can be changed to Photoshop. In the case of default accounts, these are accounts that are provided by the operating system vendor (e.g., root in UNIX).
Default deny policy	A policy whereby access is denied unless it is specifically allowed; the inverse of default allow.
Default password	The password used to gain access when a system is first installed on a computer or network device. Scope Notes: There is a large list published on the Internet and maintained at several locations. Failure to change these after the installation leaves the system vulnerable.
Defense in depth	The practice of layering defenses to provide added protection.Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an enterprise's computing and information resources.
Degauss	The application of variable levels of alternating current for the purpose of demagnetizing magnetic recording media. Scope Notes: 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.
Demographic	A fact determined by measuring and analyzing data about a population; it relies heavily on survey research and census data.
Denial-of-service attack (DoS)	An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.
Depreciation	The process of cost allocation that assigns the original cost of equipment to the periods benefited. Scope Notes: The most common method of calculating depreciation is the straight-line method, which assumes that assets should be written off in equal amounts over their lives.
Detailed IS controls	Controls over the acquisition, implementation, delivery and support of IS systems and services made up of application controls plus those general controls not included in pervasive controls.
Detective application controls	Designed to detect errors that may have occurred based on predefined logic or business rules. Usually executed after an action has taken place and often cover a group of transactions.
Detective control	Exists to detect and report when errors, omissions and unauthorized uses or entries occur.
Device	A generic term for a computer subsystem, such as a printer, serial port or disk drive . A device frequently requires its own controlling software, called a device driver.
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 certification	A process to authenticate (or certify) a party's digital signature; carried out by trusted third parties.
Digital code signing	The process of digitally signing computer code to ensure its integrity.
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.
Direct reporting engagement	An engagement in which management does not make a written assertion about the effectiveness of their control procedures and an IS auditor provides an opinion about subject matter directly, such as the effectiveness of the control procedures.

Disaster	1. A sudden, unplanned calamitous event causing great damage or loss. Any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time. Similar terms are business interruption, outage and catastrophe. 2. The period when organization management decides to divert from normal production responses and exercises its disaster recovery plan. Typically signifies the beginning of a move from a primary to an alternate location.
Disaster declaration	The communication to appropriate internal and external parties that the disaster recovery plan (DRP) is being put into operation.
Disaster notification fee	The fee that the recovery site vendor charges when the customer notifies them that a disaster has occurred and the recovery site is required. Scope Notes: The fee is implemented to discourage false disaster notifications.
Disaster recovery	Activities and programs designed to return the enterprise to an acceptable condition.The ability to respond to an interruption in services by implementing a disaster recovery plan (DRP) to restore an enterprise's critical business functions.
Disaster recovery plan (DRP)	A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster
Disaster recovery plan (DRP) desk checking	Typically a read-through of a disaster recovery plan (DRP) without any real actions taking place. Scope Notes: Generally involves a reading of the plan, discussion of the action items and definition of any gaps that might be identified
Disaster recovery plan (DRP) walk-through	Generally a robust test of the recovery plan requiring that some recovery activities take place and are tested. A disaster scenario is often given and the recovery teams talk through the steps that they would need to take to recover. As many aspects of the plan as possible should be tested.
Disaster tolerance	The time gap during which the business can accept the non-availability of IT facilities.
Disclosure controls and procedures	The processes in place designed to help ensure that all material information is disclosed by an enterprise in the reports that it files or submits to the U.S. Security and Exchange Commission (SEC). Scope Notes: Disclosure Controls and Procedures also require that disclosures be authorized, complete and accurate, and recorded, processed, summarized and reported within the time periods specified in the SEC rules and forms. Deficiencies in controls, and any significant changes to controls, must be communicated to the enterprise’s audit committee and auditors in a timely manner. An enterprise’s principal executive officer and financial officer must certify the existence of these controls on a quarterly basis.
Discount rate	An interest rate used to calculate a present value which might or might not include the time value of money, tax effects, risk or other factors.
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.
Discretionary access control (DAC)	A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Scope Notes: The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
Disk mirroring	The practice of duplicating data in separate volumes on two hard disks to make storage more fault tolerant. Mirroring provides data protection in the case of disk failure because data are constantly updated to both disks.
Diskless workstations	A workstation or PC on a network that does not have its own disk, but instead stores files on a network file server.
Distributed data processing network	A system of computers connected together by a communication network. Scope Notes: 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.
Distributed denial-of-service attack (DDoS)	A denial-of-service (DoS) assault from multiple sources.
Diverse routing	The method of routing traffic through split cable facilities or duplicate cable facilities. Scope Notes: 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	In COBIT, the grouping of control objectives into four logical stages in the life cycle of investments involving IT (Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate).
Domain name system (DNS)	A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and e-mail servers.
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 Notes: 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.

Double-loop step	Integrates the management of tactics (financial budgets and monthly reviews) and the management of strategy. Scope Notes: A reporting system, based on the balanced scorecard (BSC), that allows process to be monitored against strategy and corrective actions to be taken as required
Downloading	The act of transferring computerized information from one computer to another computer.
Downtime report	A report that identifies the elapsed time when a computer is not operating correctly because of machine failure.
Driver (value and risk)	A driver includes an event or other activity that results in the identification of an assurance/audit need.
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 Notes: 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.
Dual control	A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource so that no single entity acting alone can access that resource.
Due care	The level of care expected from a reasonable person of similar competency under similar conditions.
Due diligence	The performance of those actions that are generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review and/or analysis.
Due professional care	Diligence that a person, who possesses a special skill, would exercise under a given set of circumstances.
Dumb terminal	A display terminal without processing capability. Scope Notes: Dumb terminals are dependent on the main computer for processing. All entered data are accepted without further editing or validation.
Duplex routing	The method or communication mode of routing data over the communication network.
Dynamic analysis	Analysis that is performed in a real-time or continuous form.
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 Notes: 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.
Dynamic partitioning	The variable allocation of central processing unit (CPU) processing and memory to multiple applications and data on a server.
Data retention	Refers to the policies that govern data and records management for meeting internal, legal and regulatory data archival requirements
Demilitarized zone (DMZ)	A screened (firewalled) network segment that acts as a buffer zone between a trusted and untrusted network. </br/>Scope Notes: A DMZ is typically used to house systems such as web servers that must be accessible from both internal networks and the Internet.
Detection risk	The risk that the IS audit or assurance professional's substantive procedures will not detect an error that could be material, individually or in combination with other errors. </br/>Scope Notes: . </br/>Scope Notes: . </br/>Scope Notes: See audit risk
Digital certificate	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.
Digital forensics	The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings
Domain name system (DNS) exfiltration	Tunneling over DNS to gain network access. Lower-level attack vector for simple to complex data transmission, slow but difficult to detect.
Dynamic ports	Dynamic and/or private ports--49152 through 65535: Not listed by IANA because of their dynamic nature.
Echo checks	Detects line errors by retransmitting data back to the sending device for comparison with the original transmission.
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 Notes: 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).
Economic value add (EVA)	Technique developed by G. Bennett Stewart III and registered by the consulting firm of Stern, Stewart, in which the performance of the corporate capital base (including depreciated investments such as training, research and development) as well as more traditional capital investments such as physical property and equipment are measured against what shareholders could earn elsewhere.
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 document	An administrative document (a document with legal validity, such as a contract) in any graphical, photographic, electromagnetic (tape) or other electronic representation of the content. Scope Notes: Almost all countries have developed legislation concerning the definition, use and legal validity of an electronic document. An electronic document, in whatever media that contains the data or information used as evidence of a contract or transaction between parties, is considered together with the software program capable to read it. The definition of a legally valid document as any representation of legally relevant data, not only those printed on paper, was introduced into the legislation related to computer crime. In addition, many countries in defining and disciplining the use of such instruments have issued regulations defining specifics, such as the electronic signature and data interchange formats.
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.
Electronic signature	Any technique designed to provide the electronic equivalent of a handwritten signature to demonstrate the origin and integrity of specific data. Digital signatures are an example of electronic signatures.
Electronic vaulting	A data recovery strategy that allows enterprises to recover data within hours after a disaster. Scope Notes: Typically used for batch/journal updates to critical files to supplement full backups taken periodically; includes recovery of data from an offsite storage media that mirrors data via a communication link
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.
Engagement letter	Formal document which defines an IS auditor's responsibility, authority and accountability for a specific assignment.
Enterprise	A group of individuals working together for a common purpose, typically within the context of an organizational form such as a corporation, public agency, charity or trust.
Enterprise architecture (EA)	Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support the enterprise’s objectives.
Enterprise architecture (EA) for IT	Description of the fundamental underlying design of the IT components of the business, the relationships among them, and the manner in which they support the enterprise’s objectives.
Enterprise governance	A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise’s resources are used responsibly.
Enterprise risk management (ERM)	The discipline by which an enterprise in any industry assesses, controls, exploits, finances and monitors risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders.
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 Notes: Examples of ERP include SAP, Oracle Financials and J.D. Edwards.
Error	A deviation from accuracy or correctness. Scope Notes: As it relates to audit work, errors may relate to control deviations (compliance testing) or misstatements (substantive testing).
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 Notes: 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.
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 Notes: 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.
Event	Something that happens at a specific place and/or time
Event type	For the purpose of IT risk management, one of three possible sorts of events: threat event, loss event and vulnerability event. Scope Notes: Being able to consistently and effectively differentiate the different types of events that contribute to risk is a critical element in developing good risk-related metrics and well-informed decisions. Unless these categorical differences are recognized and applied, any resulting metrics lose meaning and, as a result, decisions based on those metrics are far more likely to be flawed.
Evidence	1. Information that proves or disproves a stated issue. 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. </br/>Scope Notes: Audit perspective
Exception reports	An exception report is generated by a program that identifies transactions or data that appear to be incorrect. Scope Notes: Exception reports may be outside a predetermined range or may not conform to specified criteria.
Exclusive-OR (XOR)	The exclusive-OR operator returns a value of TRUE only if just one of its operands is TRUE. Scope Notes: The XOR operation is a Boolean operation that produces a 0 if its two Boolean inputs are the same (0 and 0 or 1 and 1) and that produces a 1 if its two inputs are different (1 and 0). In contrast, an inclusive-OR operator returns a value of TRUE if either or both of its operands are TRUE.
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 Notes: 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.
Extended Binary-coded for Decimal Interchange Code (EBCDIC)	An 8-bit code representing 256 characters; used in most large computer systems
Extended enterprise	Describes an enterprise that extends outside its traditional boundaries. Such enterprise concentrate on the processes they do best and rely on someone outside the entity to perform the remaining processes.
eXtensible Access Control Markup Language (XACML)	A declarative online software application user access control policy language implemented in Extensible Markup Language (XML).
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.
External router	The router at the extreme edge of the network under control, usually connected to an Internet service provider (ISP) or other service provider; also known as border router.
External storage	The location that contains the backup copies to be used in case recovery or restoration is required in the event of a disaster.
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 Notes: 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.
Enterprise goal	 Scope Notes: See Business goal
Eavesdropping	Listening a private communication without permission
Egress	Network communications going out
Elliptical curve cryptography (ECC)	An algorithm that combines plane geometry with algebra to achieve stronger authentication with smaller keys compared to traditional methods, such as RSA, which primarily use algebraic factoring.. </br/>Scope Notes: Smaller keys are more suitable to mobile devices.
Encapsulation security payload (ESP)	Protocol, which is designed to provide a mix of security services in IPv4 and IPv6. ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. (RFC 4303). </br/>Scope Notes: The ESP header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode).
Encryption algorithm	A mathematically based function or calculation that encrypts/decrypts data
Eradication	When containment measures have been deployed after an incident occurs, the root cause of the incident must be identified and removed from the network.. </br/>Scope Notes: Eradication methods include: restoring backups to achieve a clean state of the system, removing the root cause, improving defenses and performing vulnerability analysis to find further potential damage from the same root cause.
Exploit	Full use of a vulnerability for the benefit of an attacker
Fail-over	The transfer of service from an incapacitated primary component to its backup component.
Fail-safe	Describes the design properties of a computer system that allow it to resist active attempts to attack or bypass it.

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 Notes: 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.
Fall-through logic	An optimized code based on a branch prediction that predicts which way a program will branch when an application is presented.
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 Notes: 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.
False negative	In intrusion detection, an error that occurs when an attack is misdiagnosed as a normal activity.
False positive	A result that has been mistakenly identified as a problem when, in reality, the situation is normal.
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 Notes: 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.
Field	An individual data element in a computer record. Scope Notes: Examples include employee name, customer address, account number, product unit price and product quantity in stock.
File	A named collection of related records.
File allocation table (FAT)	A table used by the operating system to keep track of where every file is located on the disk. Scope Notes: 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 Notes: Also will specify the type of data contained within each field; for example, alphanumeric, zoned decimal, packed and binary.
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 Notes: 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.
File Transfer Protocol (FTP)	A protocol used to transfer files over a Transmission Control Protocol/Internet Protocol (TCP/IP) network (Internet, UNIX, etc.).
Filtering router	A router that is configured to control network access by comparing the attributes of the incoming or outgoing packets to a set of rules.
FIN (Final)	A flag set in a packet to indicate that this packet is the final data packet of the transmission.
Financial audit	An audit designed to determine the accuracy of financial records and information.
Finger	A protocol and program that allows the remote identification of users logged into a system.
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.
Fiscal year	Any yearly accounting period without regard to its relationship to a calendar year.
Foreign key	A value that represents a reference to a tuple (a row in a table) containing the matching candidate key value. Scope Notes: 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.)
Forensic examination	The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise.
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.
Fourth-generation language (4GL)	High-level, user-friendly, nonprocedural computer language used to program and/or read and process computer files.
Frame relay	A packet-switched wide-area-network (WAN) technology that provides faster performance than older packet-switched WAN technologies. Scope Notes: 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).

Framework	 Scope Notes: See Control framework and IT governance framework.
Frequency	A measure of the rate by which events occur over a certain period of time
Function point analysis	A technique used to determine the size of a development task, based on the number of function points. Scope Notes: Function points are factors such as inputs, outputs, inquiries and logical internal sites.
Full economic life cycle	The period of time during which material business benefits are expected to arise from, and/or during which material expenditures (including investments, running and retirement costs) are expected to be incurred by, an investment program Scope Notes: COBIT 5 perspective
Freeware	Software available free of charge
Gateway	A device (router, firewall) on a network that serves as an entrance to another network.
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.
Generic process control	A control that applies to all processes of the enterprise.
Geographic disk mirroring	A data recovery strategy that takes a set of physically disparate disks and synchronously mirrors them over high-performance communication lines. Any write to a disk on one side will result in a write on the other side. The local write will not return until the acknowledgment of the remote write is successful.
Geographical information system (GIS)	A tool used to integrate, convert, handle, analyze and produce information regarding the surface of the earth. Scope Notes: GIS data exist as maps, tri-dimensional virtual models, lists and tables
Governance	Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives Scope Notes: Conditions can include the cost of capital, foreign exchange rates, etc. Options can include shifting manufacturing to other locations, sub-contracting portions of the enterprise to thirdparties, selecting a product mix from many available choices, etc.
Guideline	A description of a particular way of accomplishing something that is less prescriptive than a procedure.
Good practice	A proven activity or process that has been successfully used by multiple enterprises and has been shown to produce reliable results
Governance enabler	Something (tangible or intangible) that assists in the realization of effective governance Scope Notes: COBIT 5 perspective
Governance framework	A framework is a basic conceptual structure used to solve or address complex issues. An enabler of governance. A set of concepts, assumptions and practices that define how something can be approached or understood, the relationships amongst the entities involved, the roles of those involved, and the boundaries (what is and is not included in the governance system). Scope Notes: Examples: COBIT, COSO's Internal Control--Integrated Framework
Governance of enterprise IT	A governance view that ensures that information and related technology support and enable the enterprise strategy and the achievement of enterprise objectives; this also includes the functional governance of IT, i.e., ensuring that IT capabilities are provided efficiently and effectively. Scope Notes: COBT 5 perspective
Governance/ management practice	For each COBIT process, the governance and management practices provide a complete set of high-level requirements for effective and practical governance and management of enterprise IT. They are statements of actions from governance bodies and management. Scope Notes: COBIT 5 perspective
Governance, Risk Management and Compliance (GRC)	A business term used to group the three close-related disciplines responsible for the protection of assets, and operations
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.
Harden	To configure a computer or other network device to resist attacks.
Hardware	The physical components of a computer system.
Hash function	An algorithm that maps or translates one set of bits into another (generally smaller) so that a message yields the same result every time the algorithm is executed using the same message as input. Scope Notes: It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm or to find two different messages that produce the same hash result using the same algorithm.
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 Notes: 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 Notes: 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 Notes: Each parent can have many children, but each child may have only one parent.
Honeypot	A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems. Scope Notes: Also known as "decoy server"
Hot site	A fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster.
Hub	A common connection point for devices in a network, hubs are used to connect segments of a local area network (LAN). Scope Notes: A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
Hurdle rate	Also known as required rate of return, above which an investment makes sense and below which it does not. Scope Notes: Often based on the cost of capital, plus or minus a risk premium, and often varied based on prevailing economic conditions
Hybrid application controls	Consist of a combination of manual and automated activities, all of which must operate for the control to be effective. Scope Notes: Sometimes referred to as computer-dependent application controls
Hyperlink	An electronic pathway that may be displayed in the form of highlighted text, graphics or a button that connects one web page with another web page address.
Hypertext	A language that enables electronic documents that present information to be connected by links instead of being presented sequentially, as is the case with normal text.
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.
Hypertext Transfer Protocol Secure (HTTPS)	A protocol for accessing a secure web server, whereby all data transferred are encrypted.
Hypertext Transfer Protocol (HTTP)	A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit hypertext markup language (HTML), extensible markup language (XML) or other pages to client browsers.
Hashing	Using a hash function (algorithm) to create hash valued or checksums that validate message integrity
Hijacking	An exploitation of a valid network session for unauthorized purposes
Horizontal defense-in depth	Controls are placed in various places in the path to access an asset (this is functionally equivalent to concentric ring model above).
Human firewall	A person prepared to act as a network layer of defense through education and awareness
hash	A cryptographic hash function takes an input of an arbitrary length and produces an output (also known as a message digest) that is a standard-sized binary string. The output is unique to the input in such a way that even a minor change to the input results in a completely different output. Modern cryptographic hash functions are also resistant to collisions (situations in which different inputs produce identical output); a collision, while possible, is statistically improbable. Cryptographic hash functions are developed so that input cannot be determined readily from the output.
Identity access management (IAM)	Encapsulates people, processes and products to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources. The goal of IAM is to provide appropriate access to enterprise resources.
Idle standby	A fail-over process in which the primary node owns the resource group and the backup node runs idle, only supervising the primary node. Scope Notes: In case of a primary node outage, the backup node takes over. The nodes are prioritized, which means that the surviving node with the highest priority will acquire the resource group. A higher priority node joining the cluster will thus cause a short service interruption.
IEEE (Institute of Electrical and Electronics Engineers)	Pronounced I-triple-E; IEEE is an organization composed of engineers, scientists and students. Scope Notes: Best known for developing standards for the computer and electronics industry
Image processing	The process of electronically inputting source documents by taking an image of the document, thereby eliminating the need for key entry.
Impact analysis	A study to prioritize the criticality of information resources for the enterprise based on costs (or consequences) of adverse events.In an impact analysis, threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames. This analysis is the basis for establishing the recovery strategy.
Impact assessment	A review of the possible consequences of a risk. Scope Notes: See also Impact analysis.

Impersonation	As a security concept related to Windows NT, allows a server application to temporarily "be" the client in terms of access to secure objects. Scope Notes: 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.
Implement	In business, includes the full economic life cycle of the investment program through retirement; (i.e., when the full expected value of the investment is realized, as much value as is deemed possible has been realized, or it is determined that the expected value cannot be realized and the program is terminated).
Implementation life cycle review	Refers to the controls that support the process of transformation of the enterprise's legacy information systems into the enterprise resource planning (ERP) applications. Scope Notes: Largely covers all aspects of systems implementation and configuration, such as change management
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. The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional and organizational levels. Independence includes Independence of mind and Independence in appearance. </br/>Scope Notes: See Independence of mind and Independence in appearance.
Independent appearance	The avoidance of facts and circumstances that are so significant that a reasonable and informed third party would be likely to conclude, weighing all the specific facts and circumstances, that a firm's, audit function's, or a member of the audit team's, integrity, objectivity or professional skepticism has been compromised.
Independent attitude	Impartial point of view which allows an IS auditor to act objectively and with fairness.
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 architecture	Information architecture is one component of IT architecture (together with applications and technology).
Information criteria	Attributes of information that must be satisfied to meet business requirements.
Information engineering	Data-oriented development techniques that work on the premise that data are at the center of information processing and that certain data relationships are significant to a business and must be represented in the data structure of its systems.
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 security program	The overall combination of technical, operational and procedural measures and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis.
Information systems (IS)	The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies. Scope Notes: Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.
Information technology (IT)	The hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form.
Informed	In a RACI chart (Responsible, Accountable, Consulted, Informed), Informed refers to those people who are kept up to date on the progress of an activity (one-way communication).
Infrastructure as a Service (IaaS)	Offers the capability to provision processing, storage, networks and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, which can include operating systems (OSs) and applications.
Inherent risk	The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)
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.

Initialization vector (IV) collisions	A major concern is the way that wired equivalent privacy (WEP) allocates the RC4 initialization vectors (IVs) used to create the keys that are used to drive a pseudo random number generator that is eventually used for encryption of the wireless data traffic. The IV in WEP is a 24-bit field--a small space that practically guarantees reuse, resulting in key reuse. The WEP standard also fails to specify how these IVs are assigned. Many wireless network cards reset these IVs to zero and then increment them by one for every use. If an attacker can capture two packets using the same IV (the same key if the key has not been changed), mechanisms can be used to determine portions of the original packets. This and other weaknesses result in key reuse, resulting in susceptibility to attacks to determine the keys used. These attacks require a large number of packets (5-6 million) to actually fully derive the WEP key, but on a large, busy network this can occur in a short time, perhaps in as quickly as 10 minutes (although, even some of the largest corporate networks will likely require much more time than this to gather enough packets). In WEP-protected wireless networks, many times multiple, or all, stations use the same shared key. This increases the chances of IV collisions greatly. The result of this is that the network becomes insecure if the WEP keys are not changed often. This furthers the need for a WEP key management protocol.
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 Notes: 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 Notes: The standard allows transmission of digital voice, video and data over 64-Kbps lines.
Integrated test facilities (ITF)	A testing methodology in which test data are processed in production systems. Scope Notes: 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	The 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 control environment	The relevant environment on which the controls have effect.
Internal control over financial reporting	A process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principals.Includes those policies and procedures that: - Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant. - Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant - Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements.
Internal control structure	The dynamic, integrated processes--effected by the governing body, management and all other staff--that are designed to provide reasonable assurance regarding the achievement of the following general objectives: - Effectiveness, efficiency and economy of operations - Reliability of management - Compliance with applicable laws, regulations and internal policies Management's strategies for achieving these general objectives are affected by the design and operation of the following components: - Control environment - Information system - Control procedures
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.
Internal penetrators	Authorized user of a computer system who oversteps his/her legitimate access rights. Scope Notes: This category is divided into masqueraders and clandestine users.
Internal rate of return (IRR)	The discount rate that equates an investment cost with its projected earnings. Scope Notes: When discounted at the IRR, the present value of the cash outflow will equal the present value of the cash inflow. The IRR and net present value (NPV) are measures of the expected profitability of aninvestment project.
Internal storage	The main memory of the computer's central processing unit (CPU).
Internet	1. Two or more networks connected by a router. 2. The world's largest network using Transmission Control Protocol/Internet Protocol (TCP/IP) to link government, university and commercial institutions.
Internet banking	Use of the Internet as a remote delivery channel for banking services. Scope Notes: Services include traditional ones, such as opening an account or transferring funds to different accounts, and new banking services, such as electronic bill presentment and payment (allowing customers to receive and pay bills on a bank's web site).

Internet Control Message Protocol (ICMP)	A set of protocols that allow systems to communicate information about the state of services on other systems. Scope Notes: For example, ICMP is used in determining whether systems are up, maximum packet sizes on links, whether a destination host/network/port is available. Hackers typically use (abuse) ICMP to determine information about the remote site.
Internet Engineering Task Force (IETF)	An organization with international affiliates as network industry representatives that sets Internet standards. This includes all network industry developers and researchers concerned with the evolution and planned growth of the Internet.
Internet Inter-ORB Protocol (IIOP)	Developed by the object management group (OMG) to implement Common Object Request Broker Architecture (CORBA) solutions over the World Wide Web. Scope Notes: CORBA enables modules of network-based programs to communicate with one another. These modules or program parts, such as tables, arrays, and more complex program subelements, are referred to as objects. Use of IIOP in this process enables browsers and servers to exchange both simple and complex objects. This differs significantly from HyperText Transfer Protocol (HTTP), which only supports the transmission of text.
Internet protocol (IP)	Specifies the format of packets and the addressing scheme.
Internet Protocol (IP) packet spoofing	An attack using packets with the spoofed source Internet packet (IP) addresses. Scope Notes: 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.
Internet service provider (ISP)	A third party that provides individuals and enterprises with access to the Internet and a variety of other Internet-related services.
Interruption window	The time that the company can wait from the point of failure to the restoration of the minimum and critical services or applications. After this time, the progressive losses caused by the interruption are excessive for the enterprise.
Intranet	A private network that uses the infrastructure and standards of the Internet and World Wide Web, but is isolated from the public Internet by firewall barriers.
Intrusion	Any event during which unauthorized access occurs.
Intrusion detection	The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack.
Intrusion detection system (IDS)	Inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack.
Intrusive monitoring	In vulnerability analysis, gaining information by performing checks that affect the normal operation of the system, and even by crashing the system.
IP Security (IPSec)	A set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets.
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.
ISO 9001:2000	Code of practice for quality management from the International Organization for Standardization (ISO). ISO 9001:2000 specifies requirements for a quality management system for any enterprise that needs to demonstrate its ability to consistently provide products or services that meet particular quality targets.
ISO/IEC 17799	This standard defines information's confidentiality, integrity and availability controls in a comprehensive information security management system. Scope Notes: Originally released as part of the British Standard for Information Security in 1999 and then as the Code of Practice for Information Security Management in October 2000, it was elevated by the International Organization for Standardization (ISO) to an international code of practice for information security management. The latest version is ISO/IEC 17799:2005.
ISO/IEC 27001	Information Security Management--Specification with Guidance for Use; the replacement for BS7799-2. It is intended to provide the foundation for third-party audit and is harmonized with other management standards, such as ISO/IEC 9001 and 14001.
IT architecture	Description of the fundamental underlying design of the IT components of the business, the relationships among them, and the manner in which they support the enterprise's objectives.
IT governance	The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives.
IT governance framework	A model that integrates a set of guidelines, policies and methods that represent the organizational approach to IT governance. Scope Notes: 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 Governance Institute® (ITGI®)	Founded in 1998 by the Information Systems Audit and Control Association (now known as ISACA). ITGI strives to assist enterprise leadership in ensuring long-term, sustainable enterprise success and to increase stakeholder value by expanding awareness.
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 Notes: 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 investment dashboard	A tool for setting expectations for an enterprise at each level and continuous monitoring of the performance against set targets for expenditures on, and returns from, IT-enabled investment projects in terms of business values.
IT risk	The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

IT risk issue	1. An instance of IT risk. 2. A combination of control, value and threat conditions that impose a noteworthy level of IT risk.
IT risk profile	A description of the overall (identified) IT risk to which the enterprise is exposed.
IT risk register	A repository of the key attributes of potential and known IT risk issues. Attributes may include name, description, owner, expected/actual frequency, potential/actual magnitude, potential/actual business impact, disposition.
IT risk scenario	The description of an IT-related event that can lead to a business impact.
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 Notes: 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.
IT tactical plan	A medium-term plan (i.e., six- to 18-month horizon) that translates the IT strategic plan direction into required initiatives, resource requirements and ways in which resources and benefits will be monitored and managed.
IT user	A person who uses IT to support or achieve a business objective.
ITIL (IT Infrastructure Library)	The UK Office of Government Commerce (OGC) IT Infrastructure Library. A set of guides on the management and provision of operational IT services.
IT-related incident	An IT-related event that causes an operational, developmental and/or strategic business impact.
Information	An asset that, like other important business assets, is essential to an enterprise's business. It can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Scope Notes: COBIT 5 perspective
Inputs and outputs	The process work products/artifacts considered necessary to support operation of the process Scope Notes: Inputs and outputs enable key decisions, provide a record and audit trail of process activities, and enable follow-up in the event of an incident. They are defined at the key management practice level, may include some work products used only within the process and are often essential inputs to other processes. The illustrative COBIT 5 inputs and outputs should not be regarded as an exhaustive list since additional information flows could be defined depending on a particular enterprise's environment and process framework. COBIT 5 perspective
Investment portfolio	The collection of investments being considered and/or being made Scope Notes: COBIT 5 perspective
IT application	Electronic functionality that constitutes parts of business processes undertaken by, or with the assistance of, IT Scope Notes: COBIT 5 perspective
IT goal	A statement describing a desired outcome of enterprise IT in support of enterprise goals. An outcome can be an artifact, a significant change of a state or a significant capability improvement. Scope Notes: COBIT 5 perspective
IT service	The day-to-day provision to customers of IT infrastructure and applications and support for their use—e.g., service desk, equipment supply and moves, and security authorizations Scope Notes: COBIT 5 perspective
IEEE 802.11	A family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area network (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.
Imaging	A process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be performed.. </br/>Scope Notes: The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.
Impact	Magnitude of loss resulting from a threat exploiting a vulnerability
Impairment	A condition that causes a weakness or diminished ability to execute audit objectives. </br/>Scope Notes: Impairment to organisational independence and individual objectivity may include personal conflict of interest; scope limitations; restrictions on access to records, personnel, equipment, or facilities; and resource limitations (such as funding or staffing).
Incident response plan	The operational component of incident management. </br/>Scope Notes: The plan includes documented procedures and guidelines for defining the criticality of incidents, reporting and escalation process, and recovery procedures.
Inconsequential deficiency	A deficiency is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected deficiencies, that the deficiencies, either individually or when aggregated with other deficiencies, would clearly be trivial to the subject matter. If a reasonable person could not reach such a conclusion regarding a particular deficiency, that deficiency is more than inconsequential.
Independence of mind	The state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgement, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.
Ingestion	A process to convert information extracted to a format that can be understood by investigators. </br/>Scope Notes: See also Normalization.
Ingress	Network communications coming in
Injection	A general term for attack types which consist of injecting code that is then interpreted/executed by the application. (OWASP)

Intangible asset	An asset that is not physical in nature. </br/>Scope Notes: Examples include: intellectual property (patents, trademarks, copyrights, processes), goodwill, and brand recognition
Intellectual property	Intangible assets that belong to an enterprise for its exclusive use
International Standards Organization (ISO)	The world's largest developer of voluntary International Standards
Internet Assigned Numbers Authority (IANA)	Responsible for the global coordination of the DNS root, IP addressing, and other Internet protocol resources
Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)	IPX is layer 3 of the open systems interconnect (OSI) model network protocol; SPX is layer 4 transport protocol. The SPX layer sits on top of the IPX layer and provides connection-oriented services between two nodes on the network.
Interrogation	Used to obtain prior indicators or relationships, including telephone numbers, IP addresses and names of individuals, from extracted data
Intruder	Individual or group gaining access to the network and it's resources without permission
Intrusion prevention	A preemptive approach to network security used to identify potential threats and respond to them to stop, or at least limit, damage or disruption
Intrusion prevention system (IPS)	A system designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks
Investigation	The collection and analysis of evidence with the goal to identifying the perpetrator of an attack or unauthorized use or access
IP address	A unique binary number used to identify devices on a TCP/IP network
IP Authentication Header (AH)	Protocol used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just "integrity") and to provide protection against replays. (RFC 4302). </br/>Scope Notes: AH ensures data integrity with a checksum that a message authentication code, such as MD5, generates. To ensure data origin authentication, AH includes a secret shared key in the algorithm that it uses for authentication. To ensure replay protection, AH uses a sequence number field within the IP authentication header.
Irregularity	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.
Job control language (JCL)	Used to control run routines in connection with performing tasks on a computer.
Journal entry	A debit or credit to a general ledger account, in Oracle. See also Manual Journal Entry.
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 Notes: A lead indicator of whether a goal will likely be reached, and a good indicator of capabilities, practices and skills. It measures an activity goal, which is an action that the process owner must take to achieve effective process performance.
Key risk indicator (KRI)	A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk. Scope Notes: See also Risk Indicator.
Knowledge portal	Refers to the repository of a core of information and knowledge for the extended enterprise. Scope Notes: Generally a web-based implementation containing a core repository of information provided for the extended enterprise to resolve any issues
Kernel mode	Used for execution of privileged instructions for the internal operation of the system. In kernel mode, there are no protections from errors or malicious activity and all parts of the system and memory are accessible.
Key length	The size of the encryption key measured in bits
Keylogger	Software used to record all keystrokes on a computer
Latency	The time it takes a system and network delay to respond. Scope Notes:More specifically, system latency is the time a system takes to retrieve data. Network latency is the time it takes for a packet to travel from source to the final destination.
Leadership	The ability and process to translate vision into desired behaviors that are followed at all levels of the extended enterprise.
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.
Level of assurance	Refers to the degree to which the subject matter has been examined or reviewed.
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 Notes: When both high and low values are used, the test may be called a range check.
Link editor (linkage editor)	A utility program that combines several separately compiled modules into one, resolving internal references between them.
Literals	Any notation for representing a value within programming language source code, e.g., a string literal; a chunk of input data that is represented "as is" in compressed data.

Local area network (LAN)	Communication network that serves several users within a specified geographic area. Scope Notes: 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
Logoff	The act of disconnecting from the computer.
Logon	The act of connecting to the computer, which typically requires entry of a user ID and password into a computer terminal.
Logs/log file	Files created specifically to record various actions occurring on the system to be monitored, such as failed login attempts, full disk drives and e-mail delivery failures.
Loss event	Any event during which a threat event results in loss. Scope Notes: From Jones, J.; "FAIR Taxonomy," Risk Management Insight, USA, 2008
Layer 2 switches	Data link level devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks
Layer 3 and 4 switches	Switches with operating capabilities at layer 3 and layer 4 of the open systems interconnect (OSI) model. These switches look at the incoming packet's networking protocol, e.g., IP, and then compare the destination IP address to the list of addresses in their tables, to actively calculate the best way to send a packet to its destination.
Layer 4-7 switches	Used for load balancing among groups of servers. </br/>Scope Notes: Also known as content-switches, content services switches, web-switches or application-switches.
Legacy system	Outdated computer systems
Likelihood	The probability of something happening
Logical access	Ability to interact with computer resources granted using identification, authentication and authorization.
Lag indicator	Metrics for achievement of goals-An indicator relating to the outcome or result of an enabler. Scope Notes: This indicator is only available after the facts or events.
Lead indicator	Metrics for application of good practice-An indicator relating to the functioning of an enabler. Scope Notes: This indicator will provide an indication on possible outcome of the enabler.
Risk owner	The person in whom the organization has invested the authority and accountability for making risk-based decisions and who owns the loss associated with a realized risk scenario. Scope Notes: The risk owner may not be responsible for the implementation of risk treatment.
Machine language	The logical language that a computer understands.
Magnetic card reader	Reads cards with a magnetic surface on which data can be stored and retrieved.
Magnetic ink character recognition (MICR)	Used to electronically input, read and interpret information directly from a source document. Scope Notes: MICR requires the source document to have specially-coded magnetic ink
Magnitude	A measure of the potential severity of loss or the potential gain from realized events/scenarios
Mail relay server	An electronic mail (e-mail) server that relays messages so that neither the sender nor the recipient is a local user.
Malware	Short for malicious software.Designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Scope Notes: 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.
Mandatory access control (MAC)	A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf.
Man-in-the-middle attack	An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system and then replaces the traffic between the two components with the intruder's own, eventually assuming control of the communication.
Manual journal entry	A journal entry entered at a computer terminal. Scope Notes: Manual journal entries can include regular, statistical, inter-company and foreign currency entries. See also Journal Entry.
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 Notes: 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.
Masqueraders	Attackers that penetrate systems by using the identity of legitimate users and their logon credentials.
Master file	A file of semi permanent information that is used frequently for processing data or for more than one purpose.

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 Notes: See Capability Maturity Model (CMM).
Maximum tolerable outages (MTO)	Maximum time that an enterprise can support processing in alternate mode.
Measure	A standard used to evaluate and communicate performance against expected results. Scope Notes: Measures are normally quantitative in nature capturing numbers, dollars, percentages, etc., but can also address qualitative information such as customer satisfaction. Reporting and monitoring measures help an enterprise gauge progress toward effective implementation of strategy.
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 Notes: 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 Notes: 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 authentication code	An American National Standards Institute (ANSI) standard checksum that is computed using Data Encryption Standard (DES).
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.
Metric	A quantifiable entity that allows the measurement of the achievement of a process goal Scope Notes: Metrics should be SMART--specific, measurable, actionable, relevant and timely. Complete metric guidance defines the unit used, measurement frequency, ideal target value (if appropriate) and also the procedure to carry out the measurement and the procedure for the interpretation of the assessment.
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 Notes: 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.
Mirrored site	An alternate site that contains the same information as the original. Scope Notes: Mirrored sites are set up for backup and disaster recovery and to balance the traffic load for numerous download requests. Such download mirrors are often placed in different locations throughout the Internet.
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.
Misuse detection	Detection on the basis of whether the system activity matches that defined as "bad".
Mobile computing	Extends the concept of wireless computing to devices that enable new kinds of applications and expand an enterprise network to reach places in circumstances that could never have been done by other means. Scope Notes: Mobile computing is comprised of personal digital assistants (PDAs), cellular phones, laptops and other technologies of this kind.
Mobile site	The use of a mobile/temporary facility to serve as a business resumption location. The facility can usually be delivered to any site and can house information technology and staff.
MODEM (modulator/demodulator)	Connects a terminal or computer to a communications network via a telephone line. Modems turn digital pulses from the computer into frequencies within the audio range of the telephone system. When acting in the receiver capacity, a modem decodes incoming frequencies.
Modulation	The process of converting a digital computer signal into an analog telecommunications signal.
Monetary unit sampling	A sampling technique that estimates the amount of overstatement in an account balance.
Monitoring policy	Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted.
Multiplexor	A device used for combining several lower-speed channels into a higher-speed channel.
Mutual takeover	A fail-over process, which is basically a two-way idle standby: two servers are configured so that both can take over the other node's resource group. Both must have enough central processing unit (CPU) power to run both applications with sufficient speed, or expected performance losses must be taken into account until the failed node reintegrates.

Management	Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.
Model	A way to describe a given set of components and how those components relate to each other in order to describe the main workings of an object, system, or concept Scope Notes: COBIT 5 perspective
MAC header	Represents the hardware address of an network interface controller (NIC) inside a data packet
Mainframe	A large high-speed computer, especially one supporting numerous workstations or peripherals
Material misstatement	An accidental or intentional untrue statement that affects the results of an audit to a measurable extent
Material weakness	A deficiency or a combination of deficiencies in internal control, such that there is a reasonable possibility that a material misstatement will not be prevented or detected on a timely basis. Weakness in control is considered 'material' if the absence of the control results in failure to provide reasonable assurance that the control objective will be met. A weakness classified as material implies that: - Controls are not in place and/or controls are not in use and/or controls are inadequate - Escalation is warranted There is an inverse relationship between materiality and the level of audit risk acceptable to the IS audit or assurance professional, i.e., the higher the materiality level, the lower the acceptability of the audit risk, and vice versa.
Media access control (MAC) address	A unique identifier assigned to network interfaces for communications on the physical network segment
Message digest	A smaller extrapolated version of the original message created using a message digest algorithm
Message digest algorithm	Message digest algorithms are SHA1, MD2, MD4 and MD5. These algorithms are one-way functions unlike private and public key encryption algorithms. </br/>Scope Notes: All digest algorithms take a message of arbitrary length and produce a 128-bit message digest.
Metropolitan area network (MAN)	A data network intended to serve an area the size of a large city
Miniature fragment attack	Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall, in the hope that only the first of the sequence of fragmented packets would be examined and the others would pass without review.
Mobile device	A small, handheld computing devices, typically having a display screen with touch input and/or a miniature keyboard and weighing less than two pounds
Multifactor authentication	A combination of more than one authentication method, such as token and password (or personal identification number [PIN] or token and biometric device).
Merkle Tree	A datastructure within which all nodes other than "leaf nodes" (nodes to which no subnodes are attached) include the hash values of all subnodes. Use of a cryptographically-strong hashing function (i.e. a message digest) can allow rapid (logorithmic) verification of the integrity of all nodes on the tree.
message digest	A cryptographic hash function takes an input of an arbitrary length and produces an output (also known as a message digest) that is a standard-sized binary string. The output is unique to the input in such a way that even a minor change to the input results in a completely different output. Modern cryptographic hash functions are also resistant to collisions (situations in which different inputs produce identical output); a collision, while possible, is statistically improbable. Cryptographic hash functions are developed so that input cannot be determined readily from the output. See hash
Net present value (NPV)	Calculated by using an after-tax discount rate of an investment and a series of expected incremental cash outflows (the initial investment and operational costs) and cash inflows (cost savings or revenues) that occur at regular periods during the life cycle of the investment. Scope Notes: To arrive at a fair NPV calculation, cash inflows accrued by the business up to about five years after project deployment also should be taken into account.
Net return	The revenue that a project or business makes after tax and other deductions; often also classified as net profit.
Netcat	A simple UNIX utility, which reads and writes data across network connections using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). It is designed to be a reliable back-end tool that can be used directly or is easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, because it can create almost any kind of connection needed and has several interesting built-in capabilities. Netcat is now part of the Red Hat Power Tools collection and comes standard on SuSE Linux, Debian Linux, NetBSD and OpenBSD distributions.
Net-centric technologies	The contents and security of information or objects (software and data) on the network are now of prime importance compared with traditional computer processing that emphasizes the location of hardware and its related software and data. Scope Notes: An example of net-centric technologies is the Internet, where the network is its primary concern.
Netware	A popular local area network (LAN) operating system (OS) developed by the Novell Corp.
Network	A system of interconnected computers and the communication equipment used to connect them.
Network administrator	Responsible for planning, implementing and maintaining the telecommunications infrastructure; also may be responsible for voice networks. Scope Notes: 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 Notes: NA storage devices generally do not provide traditional file/print or application services.
Network hop	An attack strategy in which the attacker successively hacks into a series of connected systems, obscuring his/her identify from the victim of the attack.
Network interface card (NIC)	A communication card that when inserted into a computer, allows it to communicate with other computers on a network. Scope Notes: Most NICs are designed for a particular type of network or protocol.
Node	Point at which terminals are given access to a network.
Noise	Disturbances in data transmissions, such as static, that cause messages to be misinterpreted by the receiver.
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 Notes: 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.
Nonintrusive monitoring	The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities.
Nonrepudiable transaction	Transaction that cannot be denied after the fact.
Nonrepudiation	The assurance that a party cannot later deny originating data; provision of proof of the integrity and origin of the data and that can be verified by a third party. Scope Notes: A digital signature can provide non-repudiation.
Normalization	The elimination of redundant data.
Numeric check	An edit check designed to ensure that the data element in a particular field is numeric.
National Institute for Standards and Technology (NIST)	Develops tests, test methods, reference data, proof-of concept implementations, and technical analyses to advance the development and productive use of information technology. </br/>Scope Notes: NIST is a US government entity that creates mandatory standards that are followed by federal agencies and those doing business with them.
Network address translation (NAT)	A methodology of modifying network address information in IP datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another
Network basic input/output system (NetBIOS)	A program that allows applications on different computers to communicate within a local area network (LAN).
Network news transfer protocol (NNTP)	Used for the distribution, inquiry, retrieval, and posting of Netnews articles using a reliable stream-based mechanism. For news-reading clients, NNTP enables retrieval of news articles that are stored in a central database, giving subscribers the ability to select only those articles they wish to read. (RFC 3977)
Network segmentation	A common technique to implement network security is to segment an organization's network into separate zones that can be separately controlled, monitored and protected.
Network traffic analysis	Identifies patterns in network communications. </br/>Scope Notes: Traffic analysis does not need to have the actual content of the communication but analyzes where traffic is taking place, when and for how long communications occur and the size of information transferred.
Non-statistical sampling	Method of selecting a portion of a population, by means of own judgement and experience, for the purpose of quickly confirming a proposition. This method does not allow drawing mathematical conclusions on the entire population.
nonce	A limited or single-use, typically small value used as an initialization, seed, or other special-purpose value.
Object code	Machine-readable instructions produced from a compiler or assembler program that has accepted and translated the source code.
Object management group (OMG)	A consortium with more than 700 affiliates from the software industry whose purpose is to provide a common framework for developing applications using object-oriented programming techniques. Scope Notes: For example, OMG is known principally for promulgating the Common Object Request Broker Architecture (CORBA) specification.
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 Notes: 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
Object-oriented system development	A system development methodology that is organized around "objects" rather than "actions," and "data" rather than "logic". Scope Notes: Object-oriented analysis is an assessment of a physical system to determine which objects in the real world need to be represented as objects in a software system. Any object-oriented design is software design that is centered around designing the objects that will make up a program. Any object-oriented program is one that is composed of objects or software parts.
Offline files	Computer file storage media that are not physically connected to the computer; typical examples are tapes or tape cartridges used for backup purposes.
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.
Online data processing	Achieved by entering information into the computer via a video display terminal. Scope Notes: With online data processing, the computer immediately accepts or rejects the information as it is entered.
Open Source Security Testing Methodology	An open and freely available methodology and manual for security testing.
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 Notes: 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 Notes: 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.
Operating system audit trail	Record of system events generated by a specialized operating system mechanism.
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.
Operational level agreement (OLA)	An internal agreement covering the delivery of services that support the IT organization in its delivery of services.
Operator console	A special terminal used by computer operations personnel to control computer and systems operations functions. Scope Notes: Operator console terminals typically provide a high level of computer access and should be properly secured.
Optical character recognition (OCR)	Used to electronically scan and input written information from a source document.
Optical scanner	An input device that reads characters and images that are printed or painted on a paper form into the computer.
Organization	The manner in which an enterprise is structured; can also mean the entity.
Organization for Economic Cooperation and Development (OECD)	An international organization helping governments tackle the economic, social and governance challenges of a global economy. Scope Notes: The OECD groups 30 member countries in a unique forum to discuss, develop, and refine economic and social policies.
Outcome	Result
Outcome measure	Represents the consequences of actions previously taken; often referred to as a lag indicator. Scope Notes: Outcome measure frequently focuses on results at the end of a time period and characterize historic performance. They are also referred to as a key goal indicator (KGI) and used to indicate whether goals have been met. These can be measured only after the fact and, therefore, are called "lag indicators."
Output analyzer	Checks the accuracy of the results produced by a test run. Scope Notes: There are three types of checks that an output analyzer can perform. First, if a standard set of test data and test results exist for a program, the output of a test run after program maintenance can be compared with the set of results that should be produced. Second, as programmers prepare test data and calculate the expected results, these results can be stored in a file and the output analyzer compares the actual results of a test run with the expected results. Third, the output analyzer can act as a query language; it accepts queries about whether certain relationships exist in the file of output results and reports compliance or noncompliance.
Outsourcing	A formal agreement with a third party to perform IS or other business functions for an enterprise.
Objective	Statement of a desired outcome Scope Notes: COBIT 5 perspective
Organizational structure	An enabler of governance and of management. Includes the enterprise and its structures, hierarchies and dependencies. Scope Notes: Example: Steering committee COBIT 5 perspective
Owner	Individual or group that holds or possesses the rights of and the responsibilities for an enterprise, entity or asset. Scope Notes: Examples: process owner, system owner COBIT 5 perspective
Obfuscation	The deliberate act of creating source or machine code that is difficult for humans to understand

Open Systems Interconnect (OSI) model	A model for the design of a network. The open systems interconnect (OSI) model defines groups of functionality required to network computers into layers. Each layer implements a standard protocol to implement its functionality. There are seven layers in the OSI model.
Open Web Application Security Project (OWASP)	An open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted
Packet	Data unit that is routed from source to destination in a packet-switched network. Scope Notes: A packet contains both routing information and data. Transmission Control Protocol/Internet Protocol (TCP/IP) is such a packet-switched network.
Packet filtering	Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them, based on a list of rules.
Packet internet groper (PING)	An Internet program (Internet Control Message Protocol [ICMP]) used to determine whether a specific IP address is accessible or online. It is a network application that uses User Datagram Protocol (UDP) to verify reachability of another host on the connected network. Scope Notes: It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections. In addition, PING reports the number of hops required to connect two Internet hosts. There are both freeware and shareware PING utilities available for personal computers (PCs).
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 Notes: Usually used in disaster recovery and contingency testing; team members review and become familiar with the plans and their specific roles and responsibilities
Parallel simulation	Involves an IS auditor writing a program to replicate those application processes that are critical to an audit opinion and using this program to reprocess application system data. Scope Notes: The results produced by parallel simulation are compared with the results generated by the application system and any discrepancies are identified.
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 Notes: 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.
Passive assault	Intruders attempt to learn some characteristic of the data being transmitted. Scope Notes: 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.
Passive response	A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action.
Password	A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system.
Password cracker	A tool that tests the strength of user passwords by searching for passwords that are easy to guess. It repeatedly tries words from specially crafted dictionaries and often also generates thousands (and in some cases, even millions) of permutations of characters, numbers and symbols.
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 Notes: 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.
Payback period	The length of time needed to recoup the cost of capital investment. Scope Notes: Financial amounts in the payback formula are not discounted. Note that the payback period does not take into account cash flows after the payback period and therefore is not a measure of the profitability of an investment project. The scope of the internal rate of return (IRR), net present value (NPV) and payback period is the useful economic life of the project up to a maximum of five years.
Payment system	A financial system that establishes the means for transferring money between suppliers and users of funds, ordinarily by exchanging debits or credits between banks or financial institutions.

Payroll system	An electronic system for processing payroll information and the related electronic (e.g., electronic timekeeping and/or human resources [HR] system), human (e.g., payroll clerk), and external party (e.g., bank) interfaces. In a more limited sense, it is the electronic system that performs the processing for generating payroll checks and/or bank direct deposits to employees.
Penetration testing	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers
Performance	In IT, the actual implementation or achievement of a process.
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 Notes: 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 indicators	A set of metrics designed to measure the extent to which performance objectives are being achieved on an on-going basis. Scope Notes: Performance indicators can include service level agreements (SLAs), critical success factors (CSFs), customer satisfaction ratings, internal or external benchmarks, industry best practices and international standards.
Performance management	In IT, the ability to manage any type of measurement, including employee, team, process, operational or financial measurements. The term connotes closed-loop control and regular monitoring of the measurement.
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 Notes: Examples of peripherals include disk drives and printers.
Personal digital assistant (PDA)	Also called palmtop and pocket computer, PDA is a handheld device that provide computing, Internet, networking and telephone characteristics.
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. </br/>Scope Notes: PINs have been adopted by financial institutions as the primary means of verifying customers in an electronic funds transfer (EFT) system.
Pervasive IS control	General control designed to manage and monitor the IS environment and which, therefore, affects all IS-related activities.
Phase of BCP	A step-by-step approach consisting of various phases Scope Notes: Phase of BCP is usually comprised of the following phases: pre-implementation phase, implementation phase, testing phase, and post-implementation phase.
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 Notes: 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.
Phreakers	Those who crack security, most frequently telephone and other communication networks.
Piggybacking	1. Following an authorized person into a restricted access area. 2. Electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions.
Plaintext	Digital information, such as cleartext, that is intelligible to the reader.
Platform as a Service (PaaS)	Offers the capability to deploy onto the cloud infrastructure customer-created or -acquired applications that are created using programming languages and tools supported by the provider.
PMBOK (Project Management Body of Knowledge)	A project management standard developed by the Project Management Institute (PMI).
Point-of-presence (POP)	A telephone number that represents the area in which the communication provider or Internet service provider (ISP) provides service.
Point-of-sale (POS) systems	Enables the capture of data at the time and place of transaction. Scope Notes: 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.
Point-to-point Protocol (PPP)	A protocol used for transmitting data between two ends of a connection.
Point-to-point Tunneling Protocol (PPTP)	A protocol used to transmit data securely between two end points to create a virtual private network (VPN).
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 Notes: 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 Notes: COBIT 5 perspective
Polymorphism (Objects)	Polymorphism refers to database structures that send the same command to different child objects that can produce different results depending on their family hierarchical tree structure.

Population	The entire set of data from which a sample is selected and about which an IS auditor wishes to draw conclusions.
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.).
Posting	The process of actually entering transactions into computerized or manual files. Scope Notes: Posting transactions might immediately update the master files or may result in memo posting, in which the transactions are accumulated over a period of time and then applied to master file updating.
Preventive application control	Application control that is intended to prevent an error from occurring. Preventive application controls are typically executed at the transaction level, before an action is performed.
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.
PRINCE2 (Projects in a Controlled Environment)	Developed by the Office of Government Commerce (OGC), PRINCE2 is a project management method that covers the management, control and organization of a project.
Privacy	The rights of an individual to trust that others will appropriately and respectfully use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived </br/> Scope Notes: What is appropriate depends on the associated circumstances, laws and the individual's reasonable expectations. An individual also has the right to reasonably control and be aware of the collection, use and disclosure of his\her associated personal and sensitive information.
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.
Private key	A mathematical key (kept secret by the holder) used to create digital signatures and, depending on the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.
Privilege	The level of trust with which a system object is imbued.
Problem	In IT, the unknown underlying cause of one or more incidents.
Problem escalation procedure	The process of escalating a problem up from junior to senior support staff, and ultimately to higher levels of management. Scope Notes: 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 Notes: 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.
Process maturity assessment	A subjective assessment technique derived from the Software Engineering Institute (SEI) capability maturity model integration (CMMI) concepts and developed as a COBIT management tool. It provides management with a profile of how well developed the IT management processes are. Scope Notes: It enables management to easily place itself on a scale and appreciate what is required if improved performance is needed. It is used to set targets, raise awareness, capture broad consensus, identify improvements and positively motivate change.
Process maturity attribute	The different aspects of a process covered in an assurance initiative.
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 Notes: 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.
Professional standards	Refers to standards issued by ISACA. The term may extend to related guidelines and techniques that assist the professional in implementing and complying with authoritative pronouncements of ISACA. In certain instances, standards of other professional organizations may be considered, depending on the circumstances and their relevance and appropriateness.
Program	A structured grouping of interdependent projects that is both necessary and sufficient to achieve a desired business outcome and create value. These projects could include, but are not limited to, changes in the nature of the business, business processes and the work performed by people as well as the competencies required to carry out the work, the enabling technology, and the organizational structure.
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 Notes: 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 management officer (PMO)	The individual function responsible for the implementation of a specified initiative for supporting the project management role and advancing the discipline of project management.
Project portfolio	The set of projects owned by a company. Scope Notes: It usually includes the main guidelines relative to each project, including objectives, costs, time lines and other information specific to the project.
Project team	Group of people responsible for a project, whose terms of reference may include the development, acquisition, implementation or maintenance of an application system. Scope Notes: The project team members may include line management, operational line staff, external contractors and IS auditors.
Promiscuous mode	Allows the network interface to capture all network traffic irrespective of the hardware device to which the packet is addressed.
Protection domain	The area of the system that the intrusion detection system (IDS) is meant to monitor and protect.
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.
Protocol stack	A set of utilities that implement a particular network protocol. Scope Notes: For instance, in Windows machines a Transmission Control Protocol/Internet Protocol (TCP/IP) stack consists of TCP/IP software, sockets software and hardware driver software.
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 Notes: 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 Notes: 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	In an asymmetric cryptographic scheme, the key that may be widely published to enable the operation of the scheme.
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.
Principle	An enabler of governance and of management. Comprises the values and fundamental assumptions held by the enterprise, the beliefs that guide and put boundaries around the enterprise's decision making, communication within and outside the enterprise, and stewardship--caring for assets owned by another. Scope Notes: Examples: Ethics charter, social responsibility charter. COBIT 5 perspective
Process goals	A statement describing the desired outcome of a process. Scope Notes: An outcome can be an artifact, a significant change of a state or a significant capability improvement of other processes. COBIT 5 perspective
Program and project management office (PMO)	The function responsible for supporting program and project managers, and gathering, assessing and reporting information about the conduct of their programs and constituent projects
Patch	Fixes to software programming errors and vulnerabilities
Payload	The section of fundamental data in a transmission. In malicious software this refers to the section containing the harmful data/code.
Plain old telephone service (POTS)	A wired telecommunications system.
Port (Port number)	A process or application-specific software element serving as a communication endpoint for the Transport Layer IP protocols (UDP and TCP)
Port scanning	The act of probing a system to identify open ports
Prime number	A natural number greater than 1 that can only be divided by 1 and itself.
Principle of least privilege/access	Controls used to allow the least privilege access needed to complete a task
Probe	Inspect a network or system to find weak spots
Professional judgement	The application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement
Professional skepticism	An attitude that includes a questioning mind and a critical assessment of audit evidence. </br/>Scope Notes: Source: American Institute of Certified Public Accountants (AICPA) AU 230.07
Public switched telephone network (PSTN)	A communications system that sets up a dedicated channel (or circuit) between two points for the duration of the transmission.
primitive	A primitive is a fundamental interface, block of code or basic functionality that can be deployed and reused within broader systems or interfaces. Primitives can be combined in various ways to accomplish particular tasks. In cryptosystems, primitives form the building blocks of cryptographic algorithms.
private key cryptosystems	Private key cryptosystems involve secret, private keys. The keys are also known as symmetric ciphers because the same key both encrypts message plaintext from the sender and decrypts resulting ciphertext for a recipient. See symmetric cipher.

public key cryptosystem	Public key cryptosystems combine a widely distributed public key and a closely held, protected private key. A message that is encrypted by the public key can only be decrypted by the mathematically related, counterpart private key. Conversely, only the public key can decrypt data that was encrypted by its corresponding private key. See asymmetric cipher.
Quality Assurance (QA)	A planned and systematic patter of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. (ISO/IEC 24765)
Quality management system (QMS)	A system that outlines the policies and procedures necessary to improve and control the various processes that will ultimately lead to improved enterprise performance.
Queue	A group of items that is waiting to be serviced or processed.
Quick ship	A recovery solution provided by recovery and/or hardware vendors and includes a pre-established contract to deliver hardware resources within a specified number amount of hours after a disaster occurs. Scope Notes: The quick ship solution usually provides enterprises with the ability to recover within 72 or more hours.
Quality	Being fit for purpose (achieving intended value) Scope Notes: COBIT 5 perspective
RACI chart	Illustrates who is Responsible, Accountable, Consulted and Informed within an organizational framework.
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 Notes: 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 analysis	Analysis that is performed on a continuous basis, with results gained in time to alter the run-time system.
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.
Reciprocal agreement	Emergency processing agreement between two or more enterprises with similar equipment or applications. Scope Notes: Typically, participants of a reciprocal agreement promise to provide processing time to each other when an emergency arises.
Record	A collection of related information that is treated as a unit. Scope Notes: Separate fields within the record are used for processing of the information.
Record, screen and report layouts	Record layouts provide information regarding the type of record, its size and the type of data contained in the record. Screen and report layouts describe what information is provided and necessary for input.
Recovery action	Execution of a response or task according to a written procedure.
Recovery point objective (RPO)	Determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.
Recovery strategy	An approach by an enterprise that will ensure its recovery and continuity in the face of a disaster or other major outage. Scope Notes: 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 testing	A test to check the system's ability to recover after a software or hardware failure.
Recovery time objective (RTO)	The amount of time allowed for the recovery of a business function or resource after a disaster occurs
Redo logs	Files maintained by a system, primarily a database management system (DBMS), for the purpose of reapplying changes following an error or outage recovery.
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.
Redundant site	A recovery strategy involving the duplication of key IT components, including data or other key business processes, whereby fast recovery can take place.
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 Notes: 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.

Relational database management system (RDBMS)	The general purpose of a database is to store and retrieve related information. Scope Notes: Database management systems have evolved from hierarchal to network to relational models. Today, the most widely accepted database model is the relational model. The relational model has three major aspects: structures, operations and integrity rules. An Oracle database is a collection of data that is treated as a unit.
Relevant audit evidence	Audit evidence is relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support.
Reliable audit evidence	Audit evidence is reliable if, in the IS auditor's opinion, it is valid, factual, objective and supportable.
Remote access service (RAS)	Refers to any combination of hardware and software to enable the remote access to tools or information that typically reside on a network of IT devices. Scope Notes: Originally coined by Microsoft when referring to their built-in NT remote access tools, RAS was a service provided by Windows NT which allowed most of the services that would be available on a network to be accessed over a modem link. Over the years, many vendors have provided both hardware and software solutions to gain remote access to various types of networked information. In fact, most modern routers include a basic RAS capability that can be enabled for any dial-up interface.
Remote Authentication Dial-in User Service (RADIUS)	A type of service providing an authentication and accounting system often used for dial-up and remote access security.
Remote job entry (RJE)	The transmission of job control language (JCL) and batches of transactions from a remote terminal location.
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 Notes: 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.
Repeaters	A physical layer device that regenerates and propagates electrical signals between two network segments. Scope Notes: Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) distorted by transmission loss due to reduction of signal strength during transmission (i.e., attenuation)
Replication	In its broad computing sense, involves the use of redundant software or hardware elements to provide availability and fault-tolerant capabilities. In a database context, replication involves the sharing of data between databases to reduce workload among database servers, thereby improving client performance while maintaining consistency among all systems.
Repository	An enterprise database that stores and organizes data.
Repudiation	The denial by one of the parties to a transaction, or participation in all or part of that transaction, or of the content of communication related to that transaction.
Reputation risk	The current and prospective effect on earnings and capital arising from negative public opinion. Scope Notes: Reputation risk affects a bank's ability to establish new relationships or services, or to continue servicing existing relationships. It may expose the bank to litigation, financial loss or a decline in its customer base. A bank's reputation can be damaged by Internet banking services that are executed poorly or otherwise alienate customers and the public. An Internet bank has a greater reputation risk as compared to a traditional brick-and-mortar bank, because it is easier for its customers to leave and go to a different Internet bank and since it cannot discuss any problems in person with the customer.
Request for comments (RFC)	A document that has been approved by the Internet Engineering Task Force (IETF) becomes an RFC and is assigned a unique number once published. Scope Notes: If the RFC gains enough interest, it may evolve into an Internet standard.
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 Notes: Some of these are business-, regulatory-, and security-related requirements as well as development-related requirements.
Residual risk	The remaining risk after management has implemented a risk response.
Resilience	The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect
Responsible	In a Responsible, Accountable, Consulted, Informed (RACI) chart, refers to the person who must ensure that activities are completed successfully.
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 Notes: 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 Notes: 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 impact.
Risk aggregation	The process of integrating risk assessments at a corporate level to obtain a complete view on the overall risk for the enterprise.
Risk analysis	1. A process by which frequency and magnitude of IT risk scenarios are estimated. 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 Notes: It often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of that event.
Risk appetite	The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission.
Risk assessment	A process used to identify and evaluate risk and its potential effects. </br/>Scope Notes: Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan. Risk assessments are also used to manage the project delivery and project benefit risk.
Risk avoidance	The process for systematically avoiding risk, constituting one approach to managing risk
Risk culture	The set of shared values and beliefs that governs attitudes toward risk-taking, care and integrity, and determines how openly risk and losses are reported and discussed.
Risk evaluation	The process of comparing the estimated risk against given risk criteria to determine the significance of the risk. [ISO/IEC Guide 73:2002].
Risk factor	A condition that can influence the frequency and/or magnitude and, ultimately, the business impact of IT-related events/scenarios
Risk indicator	A metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite
Risk management	1. The coordinated activities to direct and control an enterprise with regard to risk Scope Notes: 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 Notes: COBIT 5 perspective
Risk map	A (graphic) tool for ranking and displaying risk by defined ranges for frequency and magnitude.
Risk mitigation	The management of risk through the use of countermeasures and controls
Risk portfolio view	1. A method to identify interdependencies and interconnections among risk, as well as the effect of risk responses on multiple types of risk. 2. A method to estimate the aggregate impact of multiple types of risk (e.g., cascading and coincidental threat types/scenarios, risk concentration/correlation across silos) and the potential effect of risk response across multiple types of risk.
Risk tolerance	The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives.
Risk transfer	The process of assigning risk to another enterprise, usually through the purchase of an insurance policy or by outsourcing the service. Scope Notes: Also known as risk sharing
Risk treatment	The process of selection and implementation of measures to modify risk (ISO/IEC Guide 73:2002).
Root cause analysis	A process of diagnosis to establish the origins of events, which can be used for learning from consequences, typically from errors and problems.
Rootkit	A software suite designed to aid an intruder in gaining unauthorized administrative access to a computer system.
Rotating standby	A fail-over process in which there are two nodes (as in idle standby but without priority). Scope Notes: The node that enters the cluster first owns the resource group, and the second will join as a standby node.
Rounding down	A method of computer fraud involving a computer code that instructs the computer to remove small amounts of money from an authorized computer transaction by rounding down to the nearest whole value denomination and rerouting the rounded off amount to the perpetrator’s account.
Router	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 Notes: 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).
RS-232 interface	An interface between data terminal equipment and data communications equipment employing serial binary data interchange.

RSA	A public key cryptosystem developed by R. Rivest, A. Shamir and L. Adleman used for both encryption and digital signatures. Scope Notes: The RSA has two different keys, the public encryption key and the secret decryption key. The strength of the RSA depends on the difficulty of the prime number factorization. For applications with high-level security, the number of the decryption key bits should be greater than 512 bits.
Rulebase	The list of rules and/or guidance that is used to analyze event data.
Run instructions	Computer operating instructions which detail the step-by-step processes that are to occur so an application system can be properly executed; also identifies how to address problems that occur during processing.
Run-to-run totals	Provide evidence that a program processes all input data and that it processed the data correctly.
Resource	Any enterprise asset that can help the organization achieve its objectives Scope Notes: COBIT 5 perspective
Resource optimization	One of the governance objectives. Involves effective, efficient and responsible use of all resources—human, financial, equipment, facilities, etc. Scope Notes: COBIT 5 perspective
Ransomware	Malware that restricts access to the compromised systems until a ransom demand is satisfied
Recovery	The phase in the incident response plan that ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDOs) or business continuity plan (BCP)
Registered ports	Registered ports--1024 through 49151: Listed by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users
Regulation	Rules or laws defined and enforced by an authority to regulate conduct
Regulatory requirements	Rules or laws that regulate conduct and that the enterprise must obey to become compliant
Relevant information	Relating to controls, tells the evaluator something meaningful about the operation of the underlying controls or control component. Information that directly confirms the operation of controls is most relevant. Information that relates indirectly to the operation of controls can also be relevant, but is less relevant than direct information. </br/>Scope Notes: Refer to COBIT 5 information quality goals
Reliable information	Information that is accurate, verifiable and from an objective source. </br/>Scope Notes: Refer to COBIT 5 information quality goals
Remediation	After vulnerabilities are identified and assessed, appropriate remediation can take place to mitigate or eliminate the vulnerability
Removable media	Any type of storage device that can be removed from the system while is running
Replay	The ability to copy a message or stream of messages between two parties and replay (retransmit) them to one or more of the parties
Representation	A signed or oral statement issued by management to professionals, where management declares that a current or future fact (e.g., process, system, procedure, policy) is or will be in a certain state, to the best of management's knowledge.
Return-oriented attacks	An exploit technique in which the attacker uses control of the call stack to indirectly execute cherry-picked machine instructions immediately prior to the return instruction in subroutines within the existing program code
Risk acceptance	If the risk is within the enterprise's risk tolerance or if the cost of otherwise mitigating the risk is higher than the potential loss, the enterprise can assume the risk and absorb any losses
Risk reduction	The implementation of controls or countermeasures to reduce the likelihood or impact of a risk to a level within the organization's risk tolerance.
Risk response	Risk avoidance, risk acceptance, risk sharing/transfer, risk mitigation, leading to a situation that as much future residual risk (current risk with the risk response defined and implemented) as possible (usually depending on budgets available) falls within risk appetite limits.
Risk scenario	The tangible and assessable representation of risk. Scope Notes: One of the key information items needed to identify, analyze and respond to risk (COBIT 5 Process APO12)
Risk sharing	Scope Notes: See Risk transfer
Risk statement	A description of the current conditions that may lead to the loss; and a description of the loss Source: Software Engineering Institute (SEI) Scope Notes: For a risk to be understandable, it must be expressed clearly. Such a treatment must include a description of the current conditions that may lead to the loss; and a description of the loss.
randomness	Randomness or entropy is an important concept in many cryptographic implementations. It is used to create keys; generate initialization vectors (i.e., random values that â€œseedâ€ or initialize an algorithm); generate nonces (i.e., single-use, disposable values); and supply padding (additional data completing a block of fixed length).
Safeguard	A practice, procedure or mechanism that reduces risk.
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.
Sampling risk	The probability that an IS auditor has reached an incorrect conclusion because an audit sample, rather than the entire population, was tested. Scope Notes: While sampling risk can be reduced to an acceptably low level by using an appropriate sample size and selection method, it can never be eliminated.

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 Notes: 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.
Scoping process	Identifying the boundary or extent to which a process, procedure, certification, contract, etc., applies.
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 Notes: 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 Notes: 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 awareness campaign	A predefined, organized number of actions aimed at improving the security awareness of a special target audience about a specific security problem. Each security awareness program consists of a number of security awareness campaigns.
Security awareness coordinator	The individual responsible for setting up and maintaining the security awareness program and coordinating the different campaigns and efforts of the various groups involved in the program. He/she is also responsible for making sure that all materials are prepared, advocates/trainers are trained, campaigns are scheduled, events are publicized and the program as a whole moves forward.
Security awareness program	A clearly and formally defined plan, structured approach, and set of related activities and procedures with the objective of realizing and maintaining a security-aware culture. Scope Notes: This definition clearly states that it is about realizing and maintaining a security-aware culture, meaning attaining and sustaining security awareness at all times. This implies that a security awareness program is not a one-time effort, but a continuous process.
Security forum	Responsible for information security governance within the enterprise. Scope Notes: A security forum can be part of an existing management body. Because information security is a business responsibility shared by all members of the executive management team, the forum needs to involve executives from all significant parts of the enterprise. Typically, a security forum has the following tasks and responsibilities: - Defining a security strategy in line with the business strategy - Identifying security requirements - Establishing a security policy - Drawing up an overall security program or plan - Approving major initiatives to enhance information security - Reviewing and monitoring information security incidents - Monitoring significant changes in the exposure of information assets to major threats
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 management	The process of establishing and maintaining security for a computer or network system. Scope Notes: The stages of the process of security management include prevention of security problems, detection of intrusions, and investigation of intrusions and resolution. In network management, the stages are: controlling access to the network and resources, finding intrusions, identifying entry points for intruders and repairing or otherwise closing those avenues of access.
Security metrics	A standard of measurement used in management of security-related activities.
Security perimeter	The boundary that defines the area of security concern and security policy coverage.
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.
Security software	Software used to administer security, which usually includes authentication of users, access granting according to predefined rules, monitoring and reporting functions.
Security standards	Practices, directives, guidelines, principles or baselines that state what needs to be done and focus areas of current relevance and concern; they are a translation of issues already mentioned in the security policy.
Security testing	Ensuring that the modified or new system includes appropriate controls and does not introduce any security holes that might compromise other systems or misuses of the system or its information.

Security/transaction risk	The current and prospective risk to earnings and capital arising from fraud, error and the inability to deliver products or services, maintain a competitive position, and manage information. Scope Notes: Security risk is evident in each product and service offered, and it encompasses product development and delivery, transaction processing, systems development, computing systems, complexity of products and services and the internal control environment. A high level of security risk may exist with Internet banking products, particularly if those lines of business are not adequately planned, implemented and monitored.
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 Notes: 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.
Sensitivity	A measure of the impact that improper disclosure of information may have on an enterprise.
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 Notes: Can be alpha or numeric and usually utilizes a key field
Sequential fle	A computer file storage format in which one record follows another. Scope Notes: 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 delivery objective (SDO)	Directly related to the business needs, SDO is the level of services to be reached during the alternate process mode until the normal situation is restored.
Service desk	The point of contact within the IT organization for users of IT services.
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.
Service provider	An organization supplying services to one or more (internal or external) customers.
Service Set Identifier (SSID)	A 32-character unique identifier attached to the header of packets sent over a wireless local area network (WLAN) that acts as a password when a mobile device tries to connect to the base station subsystem (BSS). Scope Notes: The SSID differentiates one WLAN from another so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plaintext from a packet, it does not supply any security to the network. An SSID is also referred to as a network name, because it is a name that identifies a wireless network.
Service user	The organization using the outsourced service.
Service-oriented architecture (SOA)	A cloud-based library of proven, functional software applets that are able to be connected together to become a useful online application.
Servlet	A Java applet or a small program that runs within a web server environment. Scope Notes: 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.
Session border controller (SBC)	Provide security features for voice-over IP (VoIP) traffic similar to that provided by firewalls. Scope Notes: SBCs can be configured to filter specific VoIP protocols, monitor for denial-of-service (DOS) attacks, and provide network address and protocol translation features.
Shell	The interface between the user and the system.
Shell programming	A script written for the shell, or command line interpreter, of an operating system; it is often considered a simple domain-specific programming language. Scope Notes: Typical operations performed by shell scripts include file manipulation, program execution and printing text. Usually, shell script refers to scripts written for a UNIX shell, while command.com (DOS) and cmd.exe (Windows) command line scripts are usually called batch files. Many shell script interpreters double as a command line interface such as the various UNIX shells, Windows PowerShell or the MS-DOS command.com. Others, such as AppleScript, add scripting capability to computing environments lacking a command line interface. Other examples of programming languages primarily intended for shell scripting include digital command language (DCL) and job control language (JCL).
Sign-on procedure	The procedure performed by a user to gain access to an application or operating system. Scope Notes: If the user is properly identified and authenticated by the system's security, they will be able to access the software.
Simple fail-over	A fail-over process in which the primary node owns the resource group. Scope Notes: The backup node runs a non-critical application (e.g., a development or test environment) and takes over the critical resource group, but not vice versa.
Simple Mail Transport Protocol (SMTP)	The standard electronic mail (e-mail) protocol on the Internet

Simple Object Access Protocol (SOAP)	A platform-independent formatted protocol based on extensible markup language (XML) enabling applications to communicate with each other over the Internet. Scope Notes: Use of SOAP may provide a significant security risk to web application operations because use of SOAP piggybacks onto a web-based document object model and is transmitted via HyperText Transfer Protocol (HTTP) (port 80) to penetrate server firewalls, which are usually configured to accept port 80 and port 21 File Transfer Protocol (FTP) requests. Web-based document models define how objects on a web page are associated with each other and how they can be manipulated while being sent from a server to a client browser. SOAP typically relies on XML for presentation formatting and also adds appropriate HTTP-based headers to send it. SOAP forms the foundation layer of the web services stack, providing a basic messaging framework on which more abstract layers can build. There are several different types of messaging patterns in SOAP, but by far the most common is the Remote Procedure Call (RPC) pattern, in which one network node (the client) sends a request message to another node (the server), and the server immediately sends a response message to the client.
Single point of failure	A resource whose loss will result in the loss of service or production.
Slack time (float)	Time in the project schedule, the use of which does not affect the project's critical path; the minimum time to complete the project based on the estimated time for each project segment and their relationships. Scope Notes: Slack time is commonly referred to as "float" and generally is not "owned" by either party to the transaction.
SMART	Specific, measurable, attainable, realistic and timely, generally used to describe appropriately set goals
Smart card	A small electronic device that contains electronic memory, and possibly an embedded integrated circuit. Scope Notes: 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.
Sniff	The act of capturing network packets, including those not necessarily destined for the computer running the sniffing software.
Sniffing	The process by which data traversing a network are captured or monitored.
Social engineering	An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information.
Software	Programs and supporting documentation that enable and facilitate use of the computer. Scope Notes: Software controls the operation of the hardware and the processing of data.
Software as a service (SaaS)	Offers the capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).
Software as a service, platform as a service and infrastructure as a service (SPI)	The acronym used to refer to the three cloud delivery models.
Source code	The language in which a program is written. Scope Notes: 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.
Source code compare program	Provides assurance that the software being audited is the correct version of the software, by providing a meaningful listing of any discrepancies between the two versions of the program.
Source document	The form used to record data that have been captured. Scope Notes: A source document may be a piece of paper, a turnaround document or an image displayed for online data input.
Source lines of code (SLOC)	Often used in deriving single-point software-size estimations.
Spanning port	A port configured on a network switch to receive copies of traffic from one or more other ports on the switch.
Split data systems	A condition in which each of an enterprise's regional locations maintains its own financial and operational data while sharing processing with an enterprisewide, centralized database. Scope Notes: Split data systems permit easy sharing of data while maintaining a certain level of autonomy.
Split domain name system (DNS)	An implementation of DNS that is intended to secure responses provided by the server such that different responses are given to internal vs. external users.
Split knowledge/split key	A security technique in which two or more entities separately hold data items that individually convey no knowledge of the information that results from combining the items; a condition under which two or more entities separately have key components that individually convey no knowledge of the plain text key that will be produced when the key components are combined in the cryptographic module.
Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system.
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 Notes: 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.

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 Notes: 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.
Stage-gate	A point in time when a program is reviewed and a decision is made to commit expenditures to the next set of activities on a program or project, to stop the work altogether, or to put a hold on execution of further work.
Standard	A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as International Organization for Standardization (ISO).
Standing data	Permanent reference data used in transaction processing. Scope Notes: These data are changed infrequently, such as a product price file or a name and address file.
Star topology	A type of local area network (LAN) architecture that utilizes a central controller to which all nodes are directly connected. Scope Notes: 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.
Static analysis	Analysis of information that occurs on a non-continuous basis; also known as interval-based analysis.
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 Notes: SANs centralize the process for the storage and administration of data.
Strategic planning	The process of deciding on the enterprise's objectives, on changes in these objectives, and the policies to govern their acquisition and use.
Strengths, weaknesses, opportunities and threats (SWOT)	A combination of an organizational audit listing the enterprise's strengths and weaknesses and an environmental scan or analysis of external opportunities and threats.
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.
Subject matter	The specific information subject to an IS auditor's report and related procedures, which can include things such as the design or operation of internal controls and compliance with privacy practices or standards or specified laws and regulations (area of activity).
Substantive testing	Obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period.
Sufficient audit evidence	Audit evidence is sufficient if it is adequate, convincing and would lead another IS auditor to form the same conclusions.
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 Notes: 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.
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.
Symmetric key encryption	System in which a different key (or set of keys) is used by each pair of trading partners to ensure that no one else can read their messages. The same key is used for encryption and decryption. See also Private Key Cryptosystem.
Synchronize (SYN)	A flag set in the initial setup packets to indicate that the communicating parties are synchronizing the sequence numbers used for the data transmission.
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. </br/>Scope Notes: 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 Notes: 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 Notes: 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.
System narrative	Provides an overview explanation of system flowcharts, with explanation of key control points and system interfaces.
System software	A collection of computer programs used in the design, processing and control of all applications. Scope Notes: The programs and processing routines that control the computer hardware, including the operating system and utility programs
System testing	Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. Scope Notes: System test procedures typically are performed by the system maintenance staff in their development library.
Systems acquisition process	Procedures established to purchase application software, or an upgrade, including evaluation of the supplier's financial stability, track record, resources and references from existing customers.
Systems analysis	The systems development phase in which systems specifications and conceptual designs are developed based on end-user needs and requirements.
Service catalogue	Structured information on all IT services available to customers Scope Notes: COBIT 5 perspective
Skill	The learned capacity to achieve pre-determined results Scope Notes: COBIT 5 perspective
Stakeholder	Anyone who has a responsibility for, an expectation from or some other interest in the enterprise. Scope Notes: Examples: shareholders, users, government, suppliers, customers and the public
System of internal control	The policies, standards, plans and procedures, and organizational structures designed to provide reasonable assurance that enterprise objectives will be achieved and undesired events will be prevented or detected and corrected Scope Notes: COBIT 5 perspective
Sampling stratification	The process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum
Secure Electronic Transaction (SET)	A standard that will ensure that credit card and associated payment order information travels safely and securely between the various involved parties on the Internet.
Secure Multipurpose Internet Mail Extensions (S/MIME)	Provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption) to provide a consistent way to send and receive MIME data. (RFC 2311)
Secure Shell (SSH)	Network protocol that uses cryptography to secure communication, remote command line login and remote command execution between two networked computers
Security as a Service (SecaaS)	The next generation of managed security services dedicated to the delivery, over the Internet, of specialized information-security services.
Significant deficiency	A deficiency or a combination of deficiencies, in internal control, that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight. </br/>Scope Notes: A material weakness is a significant deficiency or a combination of significant deficiencies that results in more than a remote likelihood of an undesirable event(s) not being prevented or detected.
Single factor authentication (SFA)	Authentication process that requires only the user ID and password to grant access
Source routing specification	A transmission technique where the sender of a packet can specify the route that packet should follow through the network
Spam	Computer-generated messages sent as unsolicited advertising
Spear phishing	A targeted attack where social engineering techniques are used to masquerade as a trusted party to obtain sensitive information (personal, financial, intellectual property, etc.) or install malware.
SQL injection	Results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design. (MITRE)
Stateful inspection	A firewall architecture that tracks each connection traversing all interfaces of the firewall and makes sure they are valid.
Statutory requirements	Laws created by government institutions
Sufficient evidence	The measure of the quantity of audit evidence; supports all material questions to the audit objective and scope. </br/>Scope Notes: See evidence
Sufficient information	Information is sufficient when evaluators have gathered enough of it to form a reasonable conclusion. For information to be sufficient, however, it must first be suitable. </br/>Scope Notes: Refer to COBIT 5 information quality goals
Suitable information	Relevant (i.e., fit for its intended purpose), reliable (i.e., accurate, verifiable and from an objective source) and timely (i.e., produced and used in an appropriate time frame)information. </br/>Scope Notes: Refer to COBIT 5 information quality goals
Supervisory control and data acquisition (SCADA)	Systems used to control and monitor industrial and manufacturing processes, and utility facilities
System hardening	A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services and utilities from the system
Secure Shell (SSH)	A secure, remote-access protocol used typically for system administration.
Secure Shell (SSH)	A secure, remote-access protocol used typically for system administration.

Systems thinking	A means of helping people to see overall structures, patterns and cycles in systems, rather than seeing only specific events or elements. It allows the identification of solutions that simultaneously address different problem areas and leverage improvement throughout the wider system.
symmetric cipher	A symmetric cipher is an algorithm that encrypts data using a single key. In symmetric cryptographic algorithms, a single key is used for encipherment (encrypting) and decipherment (decrypting).
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.
Taps	Wiring devices that may be inserted into communication links for use with analysis probes, local area network (LAN) analyzers and intrusion detection security systems.
Tcpdump	A network monitoring and data acquisition tool that performs filter translation, packet acquisition and packet display.
Technical infrastructure security	Refers to the security of the infrastructure that supports the enterprise resource planning (ERP) networking and telecommunications, operating systems, and databases.
Technology infrastructure	Technology, human resources (HR) and facilities that enable the processing and use of applications.
Technology infrastructure plan	A plan for the technology, human resources and facilities that enable the current and future processing and use of applications.
Telecommunications	Electronic communication by special devices over distances or around devices that preclude direct interpersonal exchange.
Teleprocessing	Using telecommunications facilities for handling and processing of computerized information.
Telnet	Network protocol used to enable remote access to a server computer. Scope Notes: Commands typed are run on the remote server.
Terminal Access Controller Access Control System Plus (TACACS+)	An authentication protocol, often used by remote-access servers.
Terms of reference	A document that confirms a client's and an IS auditor's acceptance of a review assignment.
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 Notes: 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 Notes: Test programs, through a series of change control moves, migrate from the test environment to the production environment and become production programs.
Test types	Test types include: - Checklist test--Copies of the business continuity plan (BCP) are distributed to appropriate personnel for review - Structured walk through--Identified key personnel walk through the plan to ensure that the plan accurately reflects the enterprise's ability to recover successfully - Simulation test--All operational and support personnel are expected to perform a simulated emergency as a practice session - Parallel Test--Critical systems are run at alternate site (hot, cold, warm or reciprocal) - Complete interruption test--Disaster is replicated, normal production is shut down with real time recovery process
Testing	The examination of a sample from a population to estimate characteristics of the population.
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 Notes: A potential cause of an unwanted incident (ISO/IEC 13335)
Threat agent	Methods and things used to exploit a vulnerability. Scope Notes: Examples include determination, capability, motive and resources.
Threat analysis	An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against enterprise assets Scope Notes: The threat analysis usually defines the level of threat and the likelihood of it materializing.
Threat event	Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm.
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
Token	A device that is used to authenticate a user, typically in addition to a username and password. Scope Notes: 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 Notes: 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.
Top-level management	The highest level of management in the enterprise, responsible for direction and control of the enterprise as a whole (such as director, general manager, partner, chief officer and executive manager).
Topology	The physical layout of how computers are linked together. Scope Notes: Examples of topology include ring, star and bus.

Total cost of ownership (TCO)	Includes the original cost of the computer plus the cost of: software, hardware and software upgrades, maintenance, technical support, training, and certain activities performed by users.
Transaction	Business events or information grouped together because they have a single or similar purpose. Scope Notes: Typically, a transaction is applied to a calculation or event that then results in the updating of a holding or master file.
Transaction log	A manual or automated log of all updates to data files and databases.
Transaction protection	Also known as "automated remote journaling of redo logs," a data recovery strategy that is similar to electronic vaulting except that instead of transmitting several transaction batches daily, the archive logs are shipped as they are created.
Transmission Control Protocol (TCP)	A connection-based Internet protocol that supports reliable data transfer connections. Scope Notes: Packet data are verified using checksums and retransmitted if they are missing or corrupted. The application plays no part in validating the transfer.
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.
Transparency	Refers to an enterprise's openness about its activities and is based on the following concepts: - How the mechanism functions is clear to those who are affected by or want to challenge governance decisions - A common vocabulary has been established - Relevant information is readily available Scope Notes: Transparency and stakeholder trust are directly related; the more transparency in the governance process, the more confidence in the governance.
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 Notes: Unlike viruses, they do not replicate themselves, but they can be just as destructive to a single computer.
Trusted process	A process certified as supporting a security goal.
Trusted system	A system that employs sufficient hardware and software assurance measures to allow their use for processing a range of sensitive or classified information.
Tunnel	The paths that the encapsulated packets follow in an Internet virtual private network (VPN).
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 Notes: 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).
Tuple	A row or record consisting of a set of attribute value pairs (column or field) in a relational data structure.
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.
Two-factor authentication	The use of two independent mechanisms for authentication, (e.g., requiring a smart card and a password) typically the combination of something you know, are or have.
Tangible asset	Any assets that has physical form
Target	Person or asset selected as the aim of an attack
Threat vector	The path or route used by the adversary to gain access to the target
Timelines	Chronological graphs where events related to an incident can be mapped to look for relationships in complex cases. </br/>Scope Notes: Timelines can provide simplified visualization for presentation to management and other non-technical audiences.
Timely information	Produced and used in a time frame that makes it possible to prevent or detect control deficiencies before they become material to an enterprise. </br/>Scope Notes: Refer to COBIT 5 information quality goals
Tolerable error	The maximum error in the population that professionals are willing to accept and still conclude that the test objective has been achieved. For substantive tests, tolerable error is related to professionals' judgement about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the professionals are willing to accept
Transport Layer Security (TLS)	A protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. (RFC 2246). </br/>Scope Notes: Transport Layer Security (TLS) is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol allows
Triple DES (3DES)	A block cipher created from the Data Encryption Standard (DES) cipher by using it three times
Tunnel mode	Used to protect traffic between different networks when traffic must travel through intermediate or untrusted networks. Tunnel mode encapsulates the entire IP packet with and AH or ESP header and an additional IP header.
Unicode	A standard for representing characters as integers. Scope Notes: Unicode uses 16 bits, which means that it can represent more than 65,000 unique characters; this is necessary for languages such as Chinese and Japanese.
Uninterruptible power supply (UPS)	Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level.

Unit testing	A testing technique that is used to test program logic within a particular program or module. Scope Notes: 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 description, discovery and integration (UDDI)	A web-based version of the traditional telephone book's yellow and white pages enabling businesses to be publicly listed in promoting greater e-commerce activities.
Universal Serial BUS (USB)	An external bus standard that provides capabilities to transfer data at a rate of 12 Mbps. Scope Notes: A USB port can connect up to 127 peripheral devices.
UNIX	A multi-user, multitasking operating system that is used widely as the master control program in workstations and especially servers.
Untrustworthy host	A host is referred to as untrustworthy because it cannot be protected by the firewall; therefore, hosts on trusted networks can place only limited trust in it. Scope Notes: To the basic border firewall, add a host that resides on an untrusted network where the firewall cannot protect it. That host is minimally configured and carefully managed to be as secure as possible. The firewall is configured to require incoming and outgoing traffic to go through the untrustworthy host.
Uploading	The process of electronically sending computerized information from one computer to another computer. Scope Notes: When uploading, most often the transfer is from a smaller computer to a larger one.
User awareness	A training process in security-specific issues to reduce security problems; users are often the weakest link in the security chain.
User Datagram Protocol (UDP)	A connectionless Internet protocol that is designed for network efficiency and speed at the expense of reliability. Scope Notes: A data request by the client is served by sending packets without testing to verify whether they actually arrive at the destination, not whether they were corrupted in transit. It is up to the application to determine these factors and request retransmissions.
Utility programs	Specialized system software used to perform particular computerized functions and routines that are frequently required during normal processing. Scope Notes: 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 Notes: The utility script is executed, either automatically or manually, to perform the task. In UNIX, these are known as shell scripts.
Utility software	Computer programs provided by a computer hardware manufacturer or software vendor and used in running the system. Scope Notes: This technique can be used to examine processing activities; to test programs, system activities and operational procedures; to evaluate data file activity; and, to analyze job accounting data.
Uncertainty	The difficulty of predicting an outcome due to limited knowledge of all components
Uniform resource locator (URL)	The string of characters that form a web address
User interface impersonation	Can be a pop-up ad that impersonates a system dialog, an ad that impersonates a system warning, or an ad that impersonates an application user interface in a mobile device.
User mode	Used for the execution of normal system activities
User provisioning	A process to create, modify, disable and delete user accounts and their profiles across IT infrastructure and business applications
Vaccine	A program designed to detect computer viruses.
Val IT	The standard framework for enterprises to select and manage IT-related business investments and ITassets by means of investment programs such that they deliver the optimal value to the enterprise. Based on COBIT.
Validity check	Programmed checking of data validity in accordance with predetermined criteria.
Value	The relative worth or importance of an investment for an enterprise, as perceived by its key stakeholders, expressed as total life cycle benefits net of related costs, adjusted for risk and (in the case of financial value) the time value of money.
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.
Virtual organizations	Organization that has no official physical site presence and is made up of diverse, geographically dispersed or mobile employees.
Virtual private network (VPN)	A secure private network that uses the public telecommunications infrastructure to transmit data. Scope Notes: In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.
Virtualization	The process of adding a "guest application" and data onto a "virtual server," recognizing that the guest application will ultimately part company from this physical server.
Virus	A program with the ability to reproduce by modifying other programs to include a copy of itself. Scope Notes: 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.
Virus signature file	The file of virus patterns that are compared with existing files to determine whether they are infected with a virus or worm.
Voice mail	A system of storing messages in a private recording medium which allows the called party to later retrieve the messages.

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.
Vulnerability event	Any event during which a material increase in vulnerability results.Note that this increase in vulnerability can result from changes in control conditions or from changes in threat capability/force. Scope Notes: From Jones, J.; "FAIR Taxonomy," Risk Management Insight, USA, 2008
Value creation	The main governance objective of an enterprise, achieved when the three underlying objectives (benefits realization, risk optimization and resource optimization) are all balanced Scope Notes: COBIT 5 perspective
Vertical defense-in depth	Controls are placed at different system layers – hardware, operating system, application, database or user levels
Virtual local area network (VLAN)	Logical segmentation of a LAN into different broadcast domains. </br/>Scope Notes: A VLAN is set up by configuring ports on a switch, so devices attached to these ports may communicate as if they were attached to the same physical network segment, although the devices are located on different LAN segments. A VLAN is based on logical rather than physical connections.
Virtual private network (VPN) concentrator	A system used to establish VPN tunnels and handle large numbers of simultaneous connections. This system provides authentication, authorization and accounting services.
Volatile data	Data that changes frequently and can be lost when the system's power is shut down
Vulnerability scanning	An automated process to proactively identify security weaknesses in a network or individual system
Walk-through	A thorough demonstration or explanation that details each step of a process.
War dialer	Software packages that sequentially dial telephone numbers, recording any numbers that answer.
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.
Web hosting	The business of providing the equipment and services required to host and maintain files for one or more web sites and provide fast Internet connections to those sites. Scope Notes: Most hosting is "shared," which means that web sites of multiple companies are on the same server to share/reduce costs.
Web page	A viewable screen displaying information, presented through a web browser in a single view, sometimes requiring the user to scroll to review the entire page. Scope Notes: An enterprise's web page may display the enterprise's logo, provide information about the enterprise's products and services, or allow a customer to interact with the enterprise or third parties that have contracted with the enterprise.
Web server	Using the client-server model and the World Wide Web's HyperText Transfer Protocol (HTTP), Web Server is a software program that serves web pages to users.
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).
Web site	Consists of one or more web pages that may originate at one or more web server computers. Scope Notes: A person can view the pages of a web site in any order, as he/she would read a magazine.
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 Notes: 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 Notes: 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.
Windows NT	A version of the Windows operating system that supports preemptive multitasking.

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 Notes: 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.
Wireless computing	The ability of computing devices to communicate in a form to establish a local area network (LAN) without cabling infrastructure (wireless), and involves those technologies converging around IEEE 802.11 and 802.11b and radio band services used by mobile devices.
Wiretapping	The practice of eavesdropping on information being transmitted over telecommunications links.
World Wide Web (WWW)	A sub network of the Internet through which information is exchanged by text, graphics, audio and video.
World Wide Web Consortium (W3C)	An international consortium founded in 1994 of affiliates from public and private organizations involved with the Internet and the web. Scope Notes: The W3C's primary mission is to promulgate open standards to further enhance the economic growth of Internet web services globally.
Worm	A programmed network attack in which a self-replicating program does not attach itself to programs, but rather spreads independently of users' action.
Well-know ports	Well-known ports--0 through 1023: Controlled and assigned by the Internet Assigned Numbers Authority (IANA), and on most systems can be used only by system (or root) processes or by programs executed by privileged users. The assigned ports use the first portion of the possible port numbers. Initially, these assigned ports were in the range 0-255. Currently, the range for assigned ports managed by the IANA has been expanded to the range 0-1023.
Wi-Fi protected access II (WPA2)	Wireless security protocol that supports 802.11i encryption standards to provide greater security. This protocol uses Advanced Encryption Standards (AES) and Temporal Key Integrity Protocol (TKIP) for stronger encryption.
Wireless local area network (WLAN)	Two or more systems networked using a wireless distribution method
Write blocker	A devices that allows the acquisition of information on a drive without creating the possibility of accidentally damaging the drive
Write protect	The use of hardware or software to prevent data to be overwritten or deleted
X.25	A protocol for packet-switching networks.
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.
X.500	A standard that defines how global directories should be structured. Scope Notes: X.500 directories are hierarchical with different levels for each category of information, such as country, state and city.
Zero-day-exploit	A vulnerability that is exploited before the software creator/vendor is even aware of it's existence