Glossary

TERM	DEFINITION
5-Whys	A technique used to determine an issue's root causes. It involves asking the question "Why?" repeatedly until the root causes are identified.
A/B testing	A statistical way of comparing two (or more) techniques, typically an incumbent against a new rival. A/B testing aims to determine not only which technique performs better but also whether the difference is statistically significant. A/B testing usually considers only two techniques using one measurement but can be applied to any finite number of techniques and measures.
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 (AIW)	The maximum period of time that a system can be unavailable before compromising the achievement of the enterprise's business objectives
Acceptable use policy (AUP)	A policy that establishes an agreement between users and the enterprise that defines, for all parties, the ranges of use that are approved before gaining access to a network or the Internet
Acceptance criteria	Criteria that a solution must satisfy to be accepted by customers
Acceptance testing	Testing performed to determine whether a customer, acquirer, user, or their designee should accept a solution
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 table
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 point	A point that accesses the network
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 risk	The risk that information may be divulged or made available to recipients without authorized access from the information owner, reflecting a loss of confidentiality
Access server	The centralized access control system for managing remote access dial-up services

TERM	DEFINITION
Accountability	The ability to map a given activity or event back to the responsible party
Accountability of governance	The ability of governance to ensure 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 and COBIT 2019 perspective
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."
Accuracy	The fraction of predictions that a classification model predicted correctly. In multiclass classification, accuracy is defined as correct predictions divided by total number of examples. In binary classification, accuracy is defined as true positives plus true negatives divided by total number of examples.
Acknowledgment (ACK)	A flag set in a packet to indicate to the sender that the previously sent packet was accepted correctly by the receiver without error or that the receiver is now ready to accept a transmission
Acquirer	The stakeholder who obtains a solution from a supplier See Affected stakeholder.
Acquisition	The process of obtaining solutions by establishing and executing supplier agreements See Supplier agreement.
Action	The mechanism by which the agent transitions between states of the environment in reinforcement learning. The agent chooses the action by using a policy.
Action plan reappraisal (APR)	A bounded set of appraisal activities performed to address nonsystemic weaknesses that lead to a limited set of unsatisfied practice groups in an appraisal. The APR includes: • Conducting an eligibility analysis • Gaining authorization from ISACA • Reviewing and obtaining approval to proceed from the Appraisal Sponsor • Modifying the existing appraisal plan • Conducting a reappraisal of unsatisfied practice groups • Reporting the results to ISACA
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
Actuator	A device component responsible for enacting physical changes within an environment, e.g., relays, solenoids, switches
AdaGrad	A sophisticated gradient descent algorithm that rescales the gradients of each parameter, effectively giving each parameter an independent learning rate

TERM	DEFINITION
Address	**1.** A number, character or group of characters that identifies a given device or a storage location, which may contain data or a program step **2.** A device or storage location referred to by an identifying number, character or group of characters
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)
Addressing exception	An exception that occurs when a program calculates an address that is outside the bounds of the storage that is available to the program See Unhandled exception.
Adjusting period	A calendar containing "real" and adjusting accounting periods without overlap or gaps between the "real" periods. 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 access	Elevated or increased privileges granted to an account for that account to manage systems, networks and/or applications. Administrative access can be assigned to an individual's account or a built-in system account.
Administrative control	The rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies
Administrative distance	A metric used by routers to select the best network traffic path when multiple routes exist
Advanced Encryption Standard (AES)	A public algorithm that supports keys from 128 bits to 256 bits in size
Advanced Message Queueing Protocol (AMQP)	A messaging protocol on the application layer usually used with middleware
Advanced persistent threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources, which allow them to create opportunities to achieve their objectives by using multiple attack vectors, e.g., cyber, physical and deception. These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission themselves to carry out these objectives in the future. An advanced persistent threat (APT): • Pursues its objectives repeatedly over an extended period of time • Adapts to defenders' efforts to resist it • Is determined to maintain the level of interaction needed to execute its objectives Source: CMMC-NIST SP800-39
Adversary	A threat agent

TERM	DEFINITION
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.
Affected stakeholders	People impacted by a process, activity, work product, or decision
Affirmation	A written or oral statement confirming implementation, or lack of implementation, of processes that meet the intent and value of one or more model practices. Affirmations must be provided: • By people who have a process role that involves implementing, following, or supporting processes • In an interactive forum where the appraisal team has control over the interaction Examples of affirmations: • Oral affirmations include: interview responses, presentations, and demonstrations, and can include responses to questions on white boards, Skype/Instant Message chat boards, etc. • Written affirmations include: emails, instant messages, and data contained in systems, documents See Process role and Appraisal participant
Agent	In artificial intelligence (AI), an autonomous program or system designed to perceive and interact with its environment to make decisions and take actions to achieve specific goals. Also referred to as an intelligent agent.
Agile	**1.** A methodology of adopting flexible, adaptable and iterative processes (ISACA) **2.** An approach to project management or delivery methodology in which the customer is intimately involved in the project, tasks are divided into short phases of work, and there is frequent reassessment and adaptation of plans (CMMI)
Agile with Scrum	This is a CMMI context-specific tag is reserved for identifying unique information for agile projects using Scrum. It is a framework for managing work with an emphasis on software development. It is designed for small teams of developers who break their work into actions that can be completed within time-boxed iterations—called sprints—(e.g., two weeks) and track progress and replan in 15-minute stand-up meetings called daily scrums. See Agile
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.
Alerting system	Provides real-time information about security issues, including vulnerabilities and exploits that are currently happening
Algorithm	A finite set of well-defined, unambiguous rules for the solution of a problem in a finite number of steps. It is a sequence of operational actions that lead to a desired goal and is the basic building block of a program
Algorithm analysis	A software verification and validation (V&V) task to ensure that the algorithms selected are correct, appropriate and stable, and meet all accuracy, timing and sizing requirements
Algorithmic justice	Actively identifying and dismantling harmful biases within algorithms, promoting fairer development and deployment, and promoting accountability and transparency

TERM	DEFINITION
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
Alignment goals	Goals that emphasize the alignment of all IT efforts with business objectives
Allocated requirement	Requirement that results from levying all or part of a higher-level requirement on a solution's lower-level design component. Requirements can be assigned to logical or physical components, including people, consumables, delivery increments and architecture.
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
Altcoin	Have no formal definition but are widely considered to be alternative digital currencies; can also be all cryptocurrencies other than bitcoin
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	An 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 National Standards Institute (ANSI)	The organization that coordinates the development of US voluntary national standards for nearly all industries. It is the US member body to the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Information-technology industry standards pertain to programming languages, electronic data interchange, telecommunications and physical properties of diskettes, cartridges and magnetic tapes.
American Standard Code for Information Interchange (ASCII)	See ASCII
Amortization	The process of cost allocation that assigns the original cost of an intangible asset to the periods benefited. This is calculated in the same way as depreciation.
Amplitude	The strength of a radio signal
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.
Analysis	**1.** To separate into elemental parts or basic principles to determine the nature of the whole **2.** A course of reasoning showing that a certain result is a consequence of assumed premises **3.** The methodical investigation of a problem and the separation of that problem into smaller related units for further detailed study (Source: ANSI)

TERM	DEFINITION
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
AngularJS	An open-source JavaScript library maintained by Google and the AngularJS community that lets developers create what are known as Single [web] Page Applications. AngularJS is popular with data scientists, as a way to show the results of their analysis.
Annotation	The process of labeling or tagging data to provide examples from which a machine learning (ML) algorithm can develop a model
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
Anonymization	Irreversible severance of a data set from the identity of the data contributor to prevent any future reidentification, even by the organization collecting the data under any condition
Antimalware	A widely used technology to prevent, detect and remove many categories of malware, including computer viruses, worms, Trojans, keyloggers, malicious browser plug-ins, adware and spyware
Antiphishing	Software that identifies phishing content and attempts to block the content or warn the user about the suspicious nature of the content
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	The behavior that is appropriate of an IS auditor 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. 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:* Applications contrast 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 matters such as: appropriate controls being designed into the system, the processing of information in a complete, accurate and reliable manner; the application will function as intended; the application will application functionality in compliance with any applicable statutory provisions and compliance with the established system acquisition process.

TERM	DEFINITION
Application architecture	A 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 and COBIT 2019 perspective
Application benchmarking	The process of establishing the design and operation of automated controls within an application
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.
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 and in compliance with the established system development life cycle process.
Application development sandbox	A standalone computer, virtual machine or virtual environment used to conduct software development removed from production infrastructure
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	The application layer provides services for an application program to ensure that effective communication with another application program in a network is possible in the Open Systems Interconnection (OSI) communications model
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
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	The security aspects supported by the application, primarily with regard to the roles or responsibilities and audit trails within the applications

TERM	DEFINITION
Application service provider (ASP)	A managed service provider (MSP) that 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	A software designed to fill the specific needs of a user; for example, software for navigation, payroll or process control. Contrasts with support software and system software.
Application software tracing and mapping	A specialized tool 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.
Application-specific integrated circuits (ASIC)	A solid-state device designed to perform a single or small group of functions
Applistructure	An amalgamation of applications and technical infrastructure
Appraisal	An examination of one or more processes by a trained team using an appraisal reference model as the basis for determining, at a minimum, strengths and weaknesses See Action plan reappraisal, Benchmark appraisal, Evaluation appraisal and Sustainment appraisal
Appraisal Disclosure Statement (ADS)	A summary statement describing the ratings generated as outputs of the appraisal, and the conditions and constraints under which the appraisal was performed. The ADS may be used for public disclosure of maturity level or capability level profile ratings so they can be reported accurately and consistently.
Appraisal final findings	The results of an appraisal that identify, at a minimum, any strengths and weaknesses within the appraisal scope. Appraisal findings are inferences drawn from corroborated objective evidence. See Objective evidence
Appraisal method	A group of appraisal activities that satisfy a defined subset of requirements, as defined by ISACA in the CMMI V2.0 Appraisal Method Definition Document
Appraisal objectives	The outcomes desired from an appraisal
Appraisal output	The results of an appraisal See Appraisal results package
Appraisal participant	The members of the organizational unit who must perform a process role and are identified in the appraisal plan as someone who will provide information used by an appraisal team See process role.
Appraisal rating	A value an appraisal team assigns to a CMMI practice group, practice area or the maturity level or capability level target profile of an organizational unit during a benchmark appraisal, sustainment appraisal or action plan reappraisal. Ratings are determined by following the requirements in the appraisal method.
Appraisal results package	A package consisting of all the items required to be updated, within the CMMI Appraisal System or retained by the Appraisal Sponsor, during the entire appraisal validity period. For a detailed list, refer to Activity 2.3.4 Record Appraisal Results.

TERM	DEFINITION
Appraisal scope	The definition of the boundaries of the appraisal that encompass and describe the organizational unit transparently and in detail. The appraisal scope includes the organizational unit and model scope. See model scope, and Organizational unit
Appraisal sponsor	An individual, internal or external to the organization being appraised, who requires the appraisal to be performed, and who provides funding, the contract or other resources to conduct the appraisal. The appraisal sponsor also typically can commit the organization, e.g., approvals for purchases.
Appraisal tailoring	An appraisal method selected for use in a specific appraisal. Tailoring helps an organization adapt the appraisal method to meet its business needs and objectives.
Appraisal team member (ATM)	The role of the person(s) responsible for performing the activities as assigned and identified in the appraisal plan. ATMs must meet the minimum requirements for experience and training/certification as defined by ISACA in the CMMI V2.0 Appraisal Method Definition Document.
Appraisal teamleader (ATL)	The role of the individual who leads the activities of an appraisal and has satisfied the qualification criteria for experience, knowledge and skills as defined by ISACA in the CMMI V2.0 Appraisal Method Definition Document. The appraisal teamleader should also be an active Certified CMMI Lead Appraiser and listed on the CMMI website as sponsored by a CMMI Partner.
Appropriate evidence	The measure of the quality of the evidence
Architectural design	**1.** The process of defining a collection of hardware and software components and their interfaces to establish the framework for the development of a computer system See Functional design. **2.** The result of the process outlined in definition 1 See Software engineering.
Architecture	**1.** 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 (ISACA) **2.** The set of structures that need to be considered to establish a solution. These structures are comprised of smaller components or elements, relationships among those structures and elements and the properties of both (CMMI). See Functional architecture.
Architecture board	A group of stakeholders and experts who provide guidance on enterprise-architecture-related matters and decisions and for setting architectural policies and standards *Scope Notes:* COBIT 5 and COBIT 2019 perspective
Archive	A lasting collection of computer system data or other records that are in long-term storage
Arithmetic logic unit (ALU)	The area of the central processing unit that performs mathematical and analytical operations
Array	An n-dimensional ordered set of data items identified by a single name and one or more indices so that each element of the set is individually addressable (e.g., a matrix, table or vector)
Artifact	A form of objective evidence that is an output of the work being performed and the process being followed. It must demonstrate the extent of implementing, performing or supporting the organizational or project processes that can be mapped to one or more model practices. Artifacts must be provided by people with a process role to implement, perform, follow or support processes. See Document, Process role and Appraisal participant

TERM	DEFINITION
Artificial intelligence (AI)	An advanced computer system that can simulate human capabilities, such as analysis, based on a predetermined set of rules
ASCII	The American Standard Code for Information Interchange (ASCII). It uses 7 or 8 bits to represent an alphanumeric symbol or special character.
Assembler	A computer program that translates programs (source-code files) that are written in assembly language into their machine language equivalents (object-code files). This is in contrast to other programs, including Compiler and Interpreter. See Cross-assembler, Cross-compiler
Assembly language	A low-level programming language that corresponds closely to the instruction set of a computer, allows symbolic naming of operations and addresses, and usually results in, a one-to-one translation of program instructions (mnemonics) into machine instructions
Assertion	Any formal declaration, or set of declarations, about a subject matter made by management *Scope Notes:* Assertions should usually be made in writing and commonly contain a list of specific attributes about the subject matter or about a process involving the subject matter.
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 of 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
Asset inventory	A register used to record all relevant assets
Asset value (AV)	The value of an asset to both the business and to competitors
Assignable cause of process variation	An extraordinary event outside the bounds of the usual steps following the process
Assurance	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 regarding 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 engagement	An objective examination of evidence for the purpose of providing an assessment of risk management, control or governance processes for the enterprise *Scope Notes:* Examples may include financial, performance, compliance and system security engagements.
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 cipher	A type of cipher that combines 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 its mathematically related counterpart.

TERM	DEFINITION
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, video and data. It is a data-link layer protocol. *Scope Notes:* ATM is a protocol-independent transport mechanism. It allows high-speed data transfer rates of 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	A transmission method where characters are sent one at a time
Atomic	A condition of smart contracts where one or more conditions defined by the smart contract must be met for the transaction to execute in its entirety
Atomic swaps	A peer-to-peer exchange of assets across separate blockchains triggered by predetermined rules, without the use of a third-party service and through the use of self-enforced smart contracts. It requires an exchange of assets on both sides or the transaction will not occur.
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) *Scope Notes:* There are two types of attack vectors: ingress and egress (also known as data exfiltration).
Attention mechanism	In artificial intelligence (AI), a powerful feature used in machine learning (ML) and deep learning (DL) that weights the importance of different inputs, thus enhancing the model's ability to process and interpret complex data patterns, leading to more accurate and relevant outcomes
Attenuation	A reduction of signal strength during 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 audit report should express an opinion about whether, in all material respects, the design and/or operation of control procedures in relation to an area of activity were effective. The report should also include a description of the scope (identification or description of the audit subject or activity, the period under review and the period when the audit was performed, the nature and extent of the work performed, and any qualifications or limitations in scope).
Attestation	An engagement in which an IT auditor is engaged to either examine management's assertion regarding a particular subject matter or the subject matter directly
Attitude	A way of thinking, behaving, feeling, etc.
Attribute sampling	A method to select a portion of a population based on the presence or absence of a certain characteristic
Audit	A 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	A performance measurement of service delivery including cost, timeliness and quality against agreed service levels
Audit authority	A statement of an employee's position within the enterprise, including lines of reporting and the rights of access

TERM	DEFINITION
Audit charter	A document approved by those charged with governance that defines the purpose, authority and responsibility of the internal audit activity *Scope Notes:* The charter should: - Establish the internal audit function's position within the enterprise - Authorize access to records, personnel and physical properties relevant to the performance of IS audit and assurance engagements - Define the scope of the audit function's activities
Audit engagement	A specific audit assignment, task or review activity, such as an audit, control self-assessment review, fraud examination or consultancy. An audit engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.
Audit evidence	The information used to support the audit opinion
Audit expert systems	The 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 log	See Audit trail
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. It also includes 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 *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 evidence about a particular characteristic of the population.

TERM	DEFINITION
Audit subject matter risk	The 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.). *Scope Notes:* See inherent risk
Audit trail	A logical path linking a sequence of events, in the form of data, used to trace the transactions that have affected the contents of a record Source : ISO
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 and 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	The 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
Auditor	An individual assigned by ISACA to evaluate, audit or review an appraisal team leader or an appraisal
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 *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

TERM	DEFINITION
Augmented reality	A computer-generated simulation that adds enhancements to existing reality enabling a user to interact with reality in a more meaningful way. It is often accessed through mobile applications that blend digital enhancements with the real world while ensuring that the user can easily distinguish between the two.
Authentication	**1.** The act of verifying identity, i.e., user, system *Scope Notes:* Can also refer to the verification of the correctness of a piece of data. **2.** The act of verifying the identity of a user or the user's eligibility to access computerized information *Scope Notes:* Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.
Authentication Header (AH)	The protocol used to provide connectionless integrity and data-origin authentication for Internet Protocol (IP) datagrams and to provide protection against replays (RFC 4302) *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.
Authenticity	The concept of undisputed authorship
Authorization	The process of determining if the end user is permitted to have access to an information asset or the information system containing the asset
Automated application controls	The controls that have been programmed and embedded within an application
Autoregressive model	A model that predicts the probability distribution of each element in a sequence based on previous elements
Auxiliary storage	A storage device other than main memory (RAM), e.g., disks and tapes
Availability	The ability to ensure timely and reliable access to, and use of, information
Availability risk	The risk that service may be lost or data are not accessible when needed
Average precision	A metric for summarizing the performance of a ranked sequence of results. Average precision is calculated by taking the average of the precision values for each relevant result in a ranked list (each result in the ranked list where the recall increases relative to the previous result).
Awareness	The idea of being acquainted with, mindful of, conscious of and well informed on a specific subject, which implies knowing and understanding a subject and acting accordingly
Backbone	The main communication channel of a digital network. It is the part of a network that handles 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.
Backdoor	A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions
Backpropagation	An algorithm for iteratively adjusting the weights used in a neural network system. Backpropagation is often used to implement gradient descent.
Backup	The 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

TERM	DEFINITION
Backup center	An alternate facility used to continue IT/IS operations when the primary data processing (DP) center is unavailable
Bad actor	A term for a cybercriminal or hacker
Bad actor	An individual, group, country or entity who intentionally causes harm
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 a simple means of identification *Scope Notes:* Also used in advertising and publicity
Balanced scorecard (BSC)	A coherent set of performance measures organized into four categories that include traditional financial measures and customer, internal business process and learning and growth perspectives. Developed by Robert S. Kaplan and David P. Norton.
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.
Base measure	A measure that is functionally independent of other measures and cannot be expressed in other terms. A base measure is defined in terms of an attribute and the method for quantifying it. See Derived measure
Base58 Encoding	A binary-to-text encoding process that converts long bit sequences into alphanumeric text, which is easier for users
Base64 Encoding	A binary-to-text encoding process that converts long bit sequences into alphanumeric text
Baseband	A form of modulation in which data signals are pulsed directly on the transmission medium without frequency division and usually utilizes a transceiver *Scope Notes:* The entire bandwidth of the transmission medium (e.g., coaxial cable) is utilized for a single channel.
Baseline	**1.** A specification or product that has been formally reviewed and agreed on, serves as the basis for further development and can only be changed through formal change control procedures (ISACA) **2.** A set of specifications or work products that: • Has been formally reviewed and agreed on, • Serves as the basis for further work or change, and • Can be changed only through change control procedures (CMMI) See Configuration baseline and Product baseline
Baseline architecture	The existing description of the underlying design of the components of a business system before entering a cycle of architecture review and redesign *Scope Notes:* COBIT 5 and COBIT 2019 perspective
BASIC	Beginners All-purpose Symbolic Instruction Code (BASIC) is a high-level programming language intended to facilitate learning to program in an interactive environment
Bastion	A system heavily fortified against attacks

TERM	DEFINITION
Batch control	The correctness checks built into data processing systems for 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)
Bayes' Theorem	An equation for calculating the probability that something is true if something potentially related to it is true. If P(A) means “the probability that A is true” and P(A|B) means “the probability that A is true if B is true,” then Bayes' Theorem tells us that P(A|B) = (P(B|A)P(A)) / P(B).
Bayesian Analysis	A mathematical model that uses probability to aid in answering theoretical questions about unidentified parameters
Bayesian network	Graphs that compactly represent the relationship between random variables for a given problem. These graphs aid in reasoning or decision-making in the face of uncertainty. These networks are usually represented as graphs in which the link between any two nodes is assigned a value representing the probabilistic relationship between those nodes.
Benchmark	A standard against which measurements or comparisons can be made
Benchmark appraisal	A consistent and reliable assessment method that results in a rating. This includes clear and repeatable process steps, which are capable of achieving high accuracy and reliable appraisal results through the collection of objective evidence from multiple sources. A maturity level profile or capability level profile must be produced as part of this appraisal process and allows Appraisal Sponsors to compare an organization’s or project’s process implementation with others. Like other appraisal methods, benchmark appraisals identify opportunities for improving both process implementation and business performance.
Benchmark model view	A logical grouping of predefined CMMI model components used to define the appraisal model view scope. Benchmark model views are defined in the CMMI V2.0 Model, Appendix B. • **For maturity levels**, the benchmark model view is a set of practice areas and their levels that are predefined for the purpose of conducting benchmark appraisals or sustainment appraisals. • **For capability levels**, the benchmark model view may either be a predefined view or a selection of practice or capability areas and their levels that meet the organization’s business needs and performance objectives.
Benchmarking	A systematic approach to comparing enterprise performance against peers and competitors in an effort to learn the best ways of conducting business *Scope Notes:* Examples include benchmarking of quality, logistic efficiency and various other metrics.
Benefit	An outcome whose nature and value (expressed in various ways) are considered advantageous by an enterprise
Benefits realization	An objective of governance. It involves bringing new benefits to the enterprise, maintaining and extending existing forms of benefits, and eliminating initiatives and assets that are not creating sufficient value. *Scope Notes:* COBIT 5 and COBIT 2019 perspective
Best practice	A proven activity or process that has been successfully used by multiple enterprises

TERM	DEFINITION
Bias	In machine learning (ML), systemic errors or distortions either in algorithms, data, or models that lead to prejudiced results
Bidirectional traceability	An association that enables the ability to trace in either direction between logical entities, e.g., from requirements to design to code to test to the end solution, or from customer requirements to product component requirements See Requirements traceability and Traceability
Big data	Huge and diverse sets of information, encompassing structured and unstructured data, generated at high volume, velocity, and variety (the three Vs)
Big game hunter (BGH)	A cyber big game hunter is a type of cyberattack that usually leverages ransomware to target large, high-value organizations or high-profile entities.
Binary	The base 2 number system (2^n). Permissible digits are 0 and 1.
Binary classification	A type of machine learning (ML) task that categorizes observations into two groups (e.g., positive review/negative review, spam email/nonspam email, healthy patient/diseased patient)
Binary code	A code whose representation is limited to 0 and 1
Binding corporate rules (BCRs)	A set of rules that allow multinational organizations to transfer personal data from the EU to their affiliates outside of the EU
Binomial distribution	A distribution that represents the outcomes of a fixed number of independent events, each with two mutually possible outcomes, a fixed number of trials and a constant probability of success. This is a discrete probability distribution, as opposed to continuous.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data
Biometric locks	Door and entry locks that are activated by biometric features, such as voice, retina, fingerprint or signature
Biometrics	A security technique that verifies an individual's identity by analyzing a unique physical attribute, such as a handprint
BIOS (BIOS)	A basic input/output system
Bit (Bit)	A contraction of the term binary digit, and the most basic and smallest unit of computing information. A bit may be in one of two states, logic 1 or logic 0. It can be thought of as a switch that is either on or off. Bits are usually combined into computer words of various sizes, called "bytes."
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
Block cipher	A public algorithm that operates on plaintext in blocks (strings or groups) of bits
Block height	The number of blocks preceding a specific block in a blockchain ledger. It is typically used to identify a specific block (e.g., block ID).
Block producers	An entity used for proof-of-stake on a blockchain network
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-bearing transaction.

TERM	DEFINITION
Blockchain explorers	Front-end applications or user interfaces that allow a user to view individual records on a blockchain
Blue team	A team of cybersecurity staff (including incident response consultants) charged with defending the enterprise during scheduled assessments called "red team" exercises
Blueprint	An exact or detailed plan or outline
Bluetooth	A wireless communications standard used for communication over short distances
Bomb	A Trojan horse that attacks a computer system when a specific logical event occurs (logic bomb) or when a specific time-related logical event occurs (time bomb). It can also be hidden in electronic mail or data and triggers a computer system attack when read in a certain way (letter bomb). Similar to: Trojan horse, virus and worm
Boolean	A set of principles of mathematical logic developed by George Boole, a nineteenth century mathematician. Boolean algebra is the study of operations carried out on variables that can have only one of two possible values, i.e., 1 (true) and 0 (false). "Add," "subtract," "multiply" and "divide" are the primary operations of arithmetic, while "and," "or" and "not" are the primary operations of Boolean Logic. In Pascal programming language, a Boolean variable is a type of variable that can have one of two possible values: true or false.
Boosting	A machine learning technique that iteratively combines a set of simple and not very accurate classifiers (referred to as "weak" classifiers) into a classifier with high accuracy (a "strong" classifier) by upweighting the examples the model is currently misclassifying
Boot	**1.** To initialize a computer system by clearing memory and reloading the operating system **2.** To cause a computer system to reach a known beginning state. A boot program, in firmware, typically performs the boot function, which includes loading basic instructions that tell the computer how to load programs into memory and how to begin executing those programs. A distinction can be made between a warm boot and a cold boot. A cold boot starts the system from a powered-down state. A warm boot restarts the computer while it is powered up. Important differences between the two procedures are: • A power-up self-test, in which various portions of the hardware, e.g., memory, are tested for proper operation, is performed during a cold boot, while a warm boot does not normally perform such self-tests • A warm boot does not clear all memory
Bootstrap	A short computer program that is permanently resident or easily loaded into a computer, and whose execution brings a larger program, such as an operating system or its loader, into memory
Botnet	A term derived from a robot network; 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 targeted victims
Boundary	Logical and physical controls used to define a perimeter between the organization and the outside world
Boundary value	**1.** A data value that corresponds to a minimum or maximum input, internal or output value specified for a system or component **2.** A value that lies just inside or just outside of a specified range of valid input and output values

TERM	DEFINITION
Boundary value analysis	A selection technique in which test data are chosen to lie along boundaries of the input domain or output range classes, data structures, procedure parameters, etc. Choices often include maximum, minimum and trivial values or parameters. This technique is often called stress testing. See Testing, boundary value. Source: NBS
Branch	An instruction that causes program execution to jump to a new point in the program sequence, rather than execute the next instruction. Contrasts with condition coverage, multiple condition coverage, path coverage and statement coverage. See Decision coverage
Branch analysis	A test case identification technique that produces enough test cases so that each decision has a true and a false outcome at least once
Branch coverage	A test coverage criterion that requires that for each decision point, each possible branch is executed at least once. Branch coverage is synonymous with decision coverage and contrasts with condition coverage, multiple condition coverage, path coverage and statement coverage.
Bridge	A 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) segments from a single segment to reduce collision domains *Scope Notes:* A bridge acts as a store-and-forward device by moving frames toward their destination. This is achieved by analyzing a data packet's MAC header, 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
Broadband	Multiple channels that are formed by dividing the transmission medium into discrete frequency segments *Scope Notes:* Broadband generally requires the use of a modem.
Broadcast	A method to distribute information to multiple recipients simultaneously
Brouter	A device that performs the functions of both a bridge and a router *Scope Notes:* A brouter operates at both the data link and 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, it processes and forwards messages to a different data link type network based on the network protocol address whenever required. When connecting same data link type networks, it is as fast as a bridge.
Browser	A computer program that enables users to retrieve information that has been made publicly available on the Internet and permits multimedia (graphics) applications on the World Wide Web
Browser protection	Software that evaluates the safety of websites
Brute force	A class of algorithms that methodically try all possible combinations until a solution is found
Brute-force attack	An attack that involves methodically 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.

TERM	DEFINITION
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	A device or storage area (memory) used to store data temporarily to compensate for differences in rates of data flow, time of occurrence of events or amounts of data that can be handled by the devices or processes involved in the transfer or use of the data
Buffer overflow	An anomaly that 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:* Because buffers contain a finite amount of data, excess data can overflow into adjacent buffers, corrupting or overwriting their valid data. Although it may occur accidentally through programming error, buffer overflow is also 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, which in effect, send new instructions to the attacked computer that can damage user files, change data or disclose confidential information.
Bug	A fault in a program that causes it to perform in an unintended or unanticipated manner See Anomaly, Defect, Error, Exception and Fault
Bulk data transfer	A data recovery strategy that includes 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	A common path or channel between hardware devices *Scope Notes:* Can be located between internal computer components or between external computers in a communication network
Bus configuration	A configuration in which 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 to allow more computers to join the network. A repeater can also be used to extend a bus configuration.
Bus topology	A network topology in which nodes are connected to a single cable
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 and learning and growth (lead) indicators that are combined to rate the enterprise
Business case	Documentation of the rationale for making a business investment that is 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

TERM	DEFINITION
Business continuity	A term for preventing, mitigating and recovering from disruption *Scope Notes:* The terms 'business resumption planning,' 'disaster recovery planning' and 'contingency planning' may also be used in this context as they focus on recovery aspects of continuity. For that reason, the 'resilience' aspect should also be taken into account. *Scope Notes:* COBIT 5 and COBIT 2019 perspective
Business continuity plan (BCP)	A plan used by an enterprise to respond to the disruption of critical business processes (depends on the contingency plan for the restoration of critical systems)
Business control	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
Business dependency assessment (BDA)	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)	The process of evaluating the criticality and sensitivity of information assets by determining the impact of losing the support of any resource to an enterprise. This establishes the escalation of a loss over time, identifies the minimum resources needed to recover and prioritizes the recovery of processes and the supporting system. *Scope Notes:* This process captures income loss, unexpected expense, legal issues (regulatory compliance or contractual), interdependent processes and loss of public reputation or public confidence.
Business impact analysis/assessment (BIA)	The process of evaluating the criticality and sensitivity of information assets. This exercise determines the impact to an enterprise of losing the support of any resource, 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 addresses: • 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	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 business goals into tactical targets and desired results and outcomes

TERM	DEFINITION
Business performance	The accomplishment of a given capability or task measured against known preset objectives (including, but not limited to, quality, cost, speed, accuracy and completeness) for delivery of a solution to a customer. In the CMMI, the term "business performance" refers to performance at the business or organizational level; it can be both organization-specific or aggregated from the project level. For example, it may involve collecting measurement and performance data at the project level and aggregating data to enable organizational performance analysis at the business level. See Process performance
Business process	An interrelated set of cross-functional activities or events that result in the delivery of a specific product or service to a customer
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 and COBIT 2019 perspective
Business process integrity	Controls over 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 the 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 that is more responsive to the customer base and market conditions while yielding material cost savings
Business risk	The probability that a situation with uncertain frequency and magnitude of loss (or gain) could prevent the enterprise from meeting its business objectives
Business service provider (BSP)	An application service provider (ASP) that also outsources 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 (B-to-B)	Transactions in which the acquirer is an enterprise or individual operating in the scope of their professional activity. In this case, laws and regulations related to consumer protection are not applicable. *Scope Notes:* A contract's general terms should be communicated to the other party and approved. Some companies require the other party to fill out a check-box with a description such as, "I specifically approve the clauses." This is not convincing; the best solution is adopting a digital signature scheme, which allows the approval of clauses and terms with a nonrepudiation condition.
Business-to-consumer (B-to-C)	Selling processes in which the involved parties are an enterprise, which offers goods or services, and a consumer. In this case, there is comprehensive legislation that protects the consumer. *Scope Notes:* Comprehensive legislation can include: • Contracts established outside the merchant's property (such as the right to end a contract for a full refund or a return policy for goods) • Distance contracts (such as rules that establish how a contract should be written, specific clauses or how a contract should be transmitted to the consumer and approved) • An electronic form of contract (such as an Internet contract or the option for the consumer to exit a procedure without having their data recorded)

TERM	DEFINITION
Business-to-consumer ecommerce (B2C)	The processes by which enterprises conduct business electronically with their customers and/or the public at large using the Internet as the enabling technology
Bypass label processing (BLP)	A technique that involves reading a computer file while bypassing the internal file/data set label. This process can result in the bypassing of the security access control system.
Byte	A sequence of adjacent bits, often an octet, operated on as a unit
Byzantine fault tolerance (BFT)	The property of a system that allows it to withstand failures and continue to function even if some of the nodes fail or act maliciously
C	A general-purpose, high-level programming language created for developing computer operating system software. It strives to combine the power of assembly language with the ease of a high-level language.
C++	An object-oriented, high-level programming language
Cadbury	A name associated with the Committee on the Financial Aspects of Corporate Governance (created in May 1991 by the UK Financial Reporting Council, the London Stock Exchange and the UK accountancy profession), which was chaired by Sir Adrian Cadbury. The committee produced a report on the subject commonly known in the UK as the Cadbury Report.
Calibration layer	A post-prediction adjustment typically used to account for prediction bias. The adjusted predictions and probabilities should match the distribution of an observed set of labels.
Candidate generation	The initial set of recommendations chosen by a recommendation system
Capability	**1.** 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 (ISACA) **2.** Organizational-level skills, abilities and knowledge embedded in people, processes, infrastructure and technology. An organization needs capabilities to implement its business model or fulfill its mission and achieve measurable business results. (CMMI)
Capability area (CA)	A group of related practice areas that can improve the performance of the skills and activities of an organization or project. Capability areas are a type of view.
Capability level	A list of practice areas (PAs) and their corresponding capability levels. A capability-level profile represents an organization's progress toward achieving its targeted practice group level for each in-scope PA.
Capability level profile	A list of practice areas (PAs) and their corresponding capability levels. A capability level profile represents an organization’s progress toward achieving its targeted practice group level for each in-scope PA.
Capability Maturity Model (CMM)	**1.** A model that 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.** A model, from the Software Engineering Institute (SEI), used by many enterprises to identify best practices useful in helping them assess and increase the maturity of their software development processes. *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. This maturity model indicates the degree of reliability or dependency a business can place on a process to achieve its desired goals or objectives. It is also a collection of instructions that an enterprise can follow to gain better control over its software development process.

TERM	DEFINITION
Capability Maturity Model Integration (CMMI)	An integrated model of best practices that enable businesses to improve performance by improving their processes. Product teams developed the model with global members from across the industry. The CMMI provides a best-practice framework for building, improving and sustaining process capability. See CMMI product suite
Capable process	A stable process that is able to meet the quality and process performance objectives set for it. The process variation is within set specification limits. See Stable process
Capacity stress testing	A test for testing an application with large quantities of data to evaluate its performance during peak periods. This is 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 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. In this way, the card swipe device prevents unauthorized access and logs all attempts to enter the secured location.
Cartel attack	An attack that involves a group of stakers with a large amount of staked tokens in a blockchain manipulating the blockchain in their favor. Alternatively, it is a type of 51% attack on PoS blockchain.
Category	Logical groups or types of views of related capability areas that address common problems encountered by businesses when producing or delivering solutions
Cathode ray tube (CRT)	A vacuum tube that displays data by means of an electron beam striking the screen. It is coated with suitable phosphor material or a device similar to a television screen where data can be displayed.
Causal analysis	A method of searching for the origin of certain effects See Root cause
Central bank digital currency (CBDC)	A digital form of fiat money
Central processing unit (CPU)	Computer hardware that houses the electronic circuits that control/direct all operations of a computer system
Centralized data processing	A distributed processing configuration formed by one central processor and database
Centroid	The center of a cluster as determined by a k-means or k-median algorithm. For instance, if k is 3, then the k-means or k-median algorithm finds 3 centroids.
Certificate (certification) authority (CA)	A trusted third party that serves authentication infrastructures or enterprises, registers entities and issues entities 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 critical and poses a risk in digital certificate verification.

TERM	DEFINITION
Certification practice statement (CPS)	A detailed set of rules governing the certificate authority's (CA) operations. It provides an understanding of the value and trustworthiness of certificates issued by a given CA. *Scope Notes:* In terms of the controls an enterprise observes, this is the method used to validate the authenticity of certificate applicants and the CA's expectations of how its certificates may be used.
Certified CMMI High Maturity Lead Appraiser (CHMLA)	The ISACA designation for a person who leads high-maturity appraisal activities and has satisfied the qualification criteria for experience, knowledge and skills defined by the Appraisal Method Definition Document. This person also has an active certification for conducting high-maturity appraisals See Appraisal team leader
Chain of custody	The process of evidence handling (from collection to presentation) that is necessary to maintain the validity and integrity of evidence *Scope Notes:* Includes documentation of who had access to the evidence and when and the ability to identify that the evidence is the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on verifying 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 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, protecting it 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	**1.** 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 (ISACA) *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 policies and procedures, executive coaching, change leadership training, team building and communication planning and execution. **2.** A methodical approach for controlling and implementing changes in a planned and structured manner (CMMI)
Change control	The processes, authorities and procedures used for all changes made to a computerized system and/or the system data. Change control is a vital subset of the quality assurance program in an enterprise and should be clearly described in the enterprise standard operating procedures. See Configuration control
Change enablement	A holistic and systemic process of ensuring that relevant stakeholders are prepared and committed to the changes involved in moving from a current state to a desired future state

TERM	DEFINITION
Change management	**1.** 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 (ISACA) *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 policies and procedures, executive coaching, change leadership training, team building and communication planning and execution. **2.** A methodical approach for controlling and implementing changes in a planned and structured manner (CMMI)
Change risk	A change in technology, regulation, business process, functionality, architecture, users or other variables that affect the enterprise business and technical environments and the level of risk associated with systems in operation
Channel service unit/ digital 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.
Channels	Private channels, also called ledger conduits, in a permissioned blockchain network where two or more nodes perform private transactions
Chargeback	The redistribution of expenditures to the units within a company that produced 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.
Chatbot	A software program that interacts with humans through text or voice using natural language processing (NLP) to understand user queries, respond, and engage in dialogue that simulates human conversation
Check digit	A numeric value, calculated mathematically, added to data to ensure that original data have not been altered or that an incorrect but valid match has not 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 used to verify the completeness of a task or goal *Scope Notes:* Used in quality assurance (and, in general, in information systems audits) to check process compliance, code standardization, error prevention and other items for which consistency processes or standards have been defined
Checkpoint restart procedures	A point in a routine where sufficient information can be stored to allow the restart of computation from that point
Checkpointing	The process of storing a block in the history of a blockchain at intervals and refusing to accept divergent blockchain without these blocks
Checksum	A value generated by an 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 later and verify that the input has not been maliciously altered. If a subsequent checksum value no longer matches the initial value, the input may have been altered or corrupted.
Chi-square test	An analysis technique used to estimate whether two variables in a cross-tabulation are correlated. A chi-square distribution varies from normal distribution based on the “degrees of freedom” used to calculate it.

TERM	DEFINITION
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 enterprise official 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). The CKO deals in knowledge, not just information. Also see chief technology officer (CTO).
Chief information security officer (CISO)	The individual in charge of information security in an enterprise
Chief risk officer (CRO)	An executive tasked with assessing and responding to risk to an enterprise's assets
Chief security officer (CSO)	The individual typically responsible for all physical and digital security matters in an enterprise
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)
Chipset	An integrated circuit (IC) or group of ICs that provides input and output for computer processing (e.g., RAM, graphics chips or WiFi chips)
Cipher	An algorithm that performs encryption
Ciphertext	Information generated by an encryption algorithm to protect the plaintext that is unintelligible to the unauthorized reader
Circuit-switched network	A data transmission service that requires establishing 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, 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
Classification	The identification of two or more categories in which an item belongs
Cleartext	Data that is not encrypted. This is also known as plaintext.
Client-server	A term used to broadly describe the relationship between the receiver and provider of a service. Generally, the client-server describes a networked system where front-end applications, like the client, make service requests to another networked system. Client-server relationships are defined primarily by software. In a local area network (LAN), the workstation is the client, and the file server is the server. However, client-server systems are inherently more complex than file-server systems. Two disparate programs must work in tandem, and there are many more decisions to make about separating data and processing between the client workstations and the database server. The database server encapsulates database files and indexes, restricts access, enforces security and provides applications with a consistent interface to data via a data dictionary.
Clipping	A technique for handling outliers. Specifically, clipping includes reducing feature values that are greater than a set maximum value down to that maximum value. It also involves increasing feature values that are less than a specific minimum value up to that minimum value.

TERM	DEFINITION
Cloud access security brokers (CASBs)	Software or appliances that are positioned between an enterprise technology infrastructure and a cloud service provider (CSP)
Cloud computing	Convenient, scalable on-demand network access to a shared pool of resources that can be provisioned rapidly and released with minimal management effort or service provider interaction
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.
Clustering	An algorithm for dividing data instances into groups—not a predetermined set of groups, but groups identified by the execution of the algorithm because of similarities found among the instances. The center of each cluster is known as the "centroid."
CMMI product suite	The integrated set of components that comprise CMMI. The product suite components include the model, appraisal method, training and certification, adoption guidance and systems and tools.
Co-adaptation	A process by which neurons predict patterns in training data by relying almost exclusively on outputs of other specific neurons instead of the network's behavior as a whole
Coaxial cable	A 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 that wraps the second wire *Scope Notes:* Has a greater transmission capacity than standard twisted-pair cables but has a limited range of effective distance

TERM	DEFINITION
COBIT	1. **COBIT 2019**: The current iteration of COBIT, which builds on and integrates more than 25 years of developments in the field of enterprise governance of information and technology (I&T). It not only incorporates new insights from science but also operationalizes these insights as practices. COBIT is a broad and comprehensive I&T governance and management framework that continues to establish itself as a generally accepted framework for I&T governance. *Scope Notes:* Earlier versions of COBIT focused on information and technology (IT), whereas COBIT 2019 focuses on information **and** technology aimed at the whole enterprise, recognizing that I&T has become crucial in the support, sustainability and growth of enterprises. (See www.isaca.org/cobit for more information.) 2. **COBIT 5**: 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 and related IT goals. Formerly known as Control Objectives for Information and related Technology (COBIT), with this iteration used only as the acronym. 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 governance aspects. Adoption and use of the COBIT framework are supported by guidance from a growing family of supporting products. 3. **COBIT 4.1 and earlier**: A complete, internationally accepted process framework for IT that supports business and IT executives and management in their definition and achievement of business and related IT goals by providing a comprehensive IT governance, management, control and assurance model. Formally known as Control Objectives for Information and related Technology (COBIT). 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 frameworks and standards.
COBOL	A high-level programming language used for solving problems in business data processing (stands for Common Business Oriented Language).
CoCo	A framework published by the Canadian Institute of Chartered Accountants in 1995 (stands for Criteria of Control)
Code audit	An independent review of source code by a person, team or tool to verify compliance with software design documentation and programming standards. Correctness and efficiency may also be evaluated. This contrasts with code inspections, code reviews and code walkthroughs.

TERM	DEFINITION
Code of ethics	A document designed to influence employees' individual and organizational behavior 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 in understanding the difference between 'right' and 'wrong' and to apply this understanding to their decisions. COBIT 5 and COBIT 2019 perspective
Coding	**1.** In software engineering, the process of expressing a computer program in a programming language **2.** The transforming of logic and data from design specifications (design descriptions) into a programming language
Coding standards	Written procedures describing coding (programming) style conventions that specify rules governing the use of individual constructs. These are provided by the programming language, naming, formatting and documentation requirements, which prevent programming errors, control complexity and promote the understandability of the source code. They are synonymous with development and programming standards.
Coefficient	A number or algebraic symbol prefixed as a multiplier to a variable or unknown quantity (e.g., x in x(y + z), 6 in 6ab)
Coevolving	Originally a biological term, the way two or more ecologically interdependent species become intertwined over time *Scope Notes:* As species adapt to their environment, they also adapt to one another. Today's multibusiness 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 content) matters. Rather than plan a 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	A term that refers to establishing a potent binding force and sense of direction and purpose for an enterprise; relating different parts of an enterprise to each other and 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 the main computing location to the alternative computer facility.
Collaborative filtering	A technique for making predictions about the interests of one user based on the interests of many other users. Collaborative filtering is often used in recommendation systems.
Collision	The situation that occurs when two or more demands are made simultaneously on equipment that can handle only one at a given time (Federal Standard 1037C)

TERM	DEFINITION
Combined Code on Corporate Governance	The consolidation of the Cadbury, Greenbury and Hampel Reports in 1998 *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. The Combined Code made to address the financial aspects of corporate governance, directors' remuneration and implementation of the Cadbury and Greenbury recommendations.
Comment	**1.** In programming languages, a language construct that allows explanatory text to be inserted into a program and that does not have any effect on the execution of the program **2.** Information embedded within a computer program, job control statements or a set of data that provides clarification to human readers but does not affect machine interpretation (Source: IEEE)
Commercial off-the-shelf (COTS)	Items that can be purchased from a commercial supplier and used without tailoring
Common Attack Pattern Enumeration and Classification (CAPEC)	A catalog of attack patterns that is “an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed” (published by the MITRE Corporation)
Common cause of variation	The variation of a process that exists because of normal and expected interactions among components of a process. This is also referred to as inherent cause of variation. See Special cause of variation
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 cloud	A cloud computing environment in which resources are shared among entities that have common interests or are in shared industries, e.g., healthcare or financial services
Community strings	A string of characters that authenticates access to management information base (MIB) objects and functions as an embedded password *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 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, log messages are generated every time the device is accessed from the management station. The log message records the source IP address of the packet.

TERM	DEFINITION
Compact disc–read-only memory (CD-ROM)	A compact disk used for the permanent storage of text, graphic or sound information. Digital data is represented compactly by tiny holes that can be read by lasers attached to high-resolution sensors. It is capable of storing up to 680 MB of data, equivalent to 250,000 pages of text or 20,000 medium-resolution images. This storage medium is often used for archival purposes and is synonymous with optical disks and write-once read-many times disks.
Comparison program	A program for the examination of data that uses logical or conditional tests to identify similarities or differences
Compartmentalization	A process for protecting very high-value assets or environments where trust is an issue. Access to an asset requires two or more processes, controls or individuals.
Compensating control	An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions
Competence	The ability to perform a specific task, action or function successfully *Scope Notes:* COBIT 5 and COBIT 2019 perspective
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
Compilation	The process of translating a program expressed in a problem-oriented or procedure-oriented language into object code. Compilation contrasts with assembling and interpret.
Compiler	**1.** A computer program that translates programs expressed in a high-level language into their machine-language equivalents **2.** A computer program that takes the finished source-code listing as input and outputs the machine-code instructions that the computer must have to execute the program See Assembler and Interpreter
Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)	A type of challenge-response test used in computing to ensure that a response was not generated by a computer. An example is the site request given to website 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	A term that refers to the 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, standards and procedures that document actions that are required or prohibited. Violations may be subject to disciplinary actions.
Compliance risk	The probability and consequences of an enterprise failing to comply with laws, regulations or the ethical standards and codes of conduct applicable to the enterprise's industry
Compliance testing	Control tests designed to obtain evidence on both the effectiveness of the controls and their operation during the audit period

TERM	DEFINITION
Component	A general term 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 cooperating 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 purposely built. However, the goal of component-based development is to ultimately use as many predeveloped, pretested components as possible.
Comprehensive audit	An audit designed to determine the accuracy of financial records and evaluate the internal controls of a function or department
Computational linguistics	A branch of computer science for parsing the text of spoken languages (e.g., English or Mandarin) to convert it to structured data that can be used to drive program logic
Computationally greedy	A term that means requiring a great deal of computing power; processor intensive
Computer	**1.** A functional unit that can perform substantial computations, including numerous arithmetic operations (or logic operations), without human intervention during a run **2.** A functional programmable unit that consists of one or more associated processing units and peripheral equipment, is controlled by internally stored programs and can perform substantial computations, including numerous arithmetic operations, or logic operations, without human intervention
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 acts as an efficient corrective control and should also be the 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 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 makes it admissible as evidence in a court of law.
Computer instruction set	A complete set of the operators of a computer's instructions together with a description of the different meanings that can be attributed to their operands. This is synonymous with machine instruction set.
Computer language	A language designed to enable humans to communicate with computers See Programming language
Computer science	The branch of science and technology concerned with methods and techniques relating to data processing performed by automatic means
Computer security incident response team (CSIRT)	The technical team responsible for addressing security incidents
Computer sequence checking	A process that verifies that control numbers follow 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)

TERM	DEFINITION
Computer system	A functional unit consisting of one or more computers and associated peripheral input and output devices and software that uses common storage for all or part of a program and all or part of the data necessary for the execution of the program. A computer system executes user-written or user-designated programs; performs user-designated data manipulation, including arithmetic and logic operations; and can execute programs that modify themselves during their execution. A computer system may be a stand-alone unit or may consist of several interconnected units. See Computer
Computer vision	A subfield of artificial intelligence (AI) concerned with enabling computers to interpret and understand visual information such as images and videos
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	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 class of controls implies that only serial and recoverable schedules are permitted and that committed transactions are not discarded when undoing aborted transactions.
Concurrent access	A failover process, in which all nodes run the same resource group and access the external storage concurrently. There can be no Internet Protocol (IP) or mandatory access control (MAC) address in a concurrent resource group.
Concurrent appraisals	Two or more appraisals that have the same appraisal team leader (ATL) performing their conduct appraisal phases at the same time. Concurrent appraisals, also called simultaneous appraisals, are not allowed under any circumstances. Concurrent appraisals typically include: • Appraising one or more organizational units (OUs) with different scopes, or • Using two or more appraisal teams, with the same time frame for their conduct appraisal phase.
Confidence interval	A range specified for an estimate to indicate margin of error, combined with a probability that a value will fall in that range
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 identification	A configuration management activity that involves selecting configuration items for a hardware/software product, assigning them unique identifiers, and recording their functional and physical characteristics in technical documentation See Configuration item and Configuration management

TERM	DEFINITION
Configuration item (CI)	**1.** Component of an infrastructure—or an item, such as a request for change, associated with an infrastructure—that is (or is to be) under the control of configuration management (ISACA) *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 **2.** Work products designated for configuration management and treated as a single entity in the configuration management process (CMMI) See Configuration management
Configuration management	**1.** The control of changes to a set of configuration items over a system life cycle (ISACA) **2.** The process of managing the integrity of work products using configuration identification, version control, change control and audits (CMMI) See Configuration identification, Configuration item, Configuration audit and Version control
Confirmation	The number of blocks added to the blockchain after the network accepts that a particular transaction has been executed
Consensus	A decision-making method that allows team members to develop a common basis of understanding and develop general agreement concerning a decision that all team members are willing to support
Consensus mechanism	A fault-tolerant mechanism used in blockchain/distributed ledger systems to achieve the necessary agreement on data values or the state of the network among distributed processes or multiagent systems
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
Consequence	The result of a realized risk. A consequence can be certain or uncertain and can have positive or negative, direct or indirect effects on objectives. Consequences can be expressed qualitatively or quantitatively.
Consistency	The degree of uniformity, standardization and freedom from contradiction among the documents or parts of a system or component See Traceability
Consistency checker	A software tool used to test requirements in design specifications for consistency and completeness
Console log	An automated detail report of computer system activity
Consolidation	The practice of collecting and summarizing the information provided into a manageable set to: • Determine the extent to which the objective evidence is corroborated and covers the areas being investigated • Determine the objective evidence sufficiency for making judgments • Revise the objective evidence-gathering plan as necessary to achieve this sufficiency See Objective evidence
Consortium blockchain	A subset of private blockchains that provides a unique blend of public and private blockchain
Constant	A value that does not change during processing; contrasts with variable
Constrained Application Protocol (CoAP)	A messaging protocol usually implemented with low-powered devices

TERM	DEFINITION
Consulted	In a RACI (responsible, accountable, consulted, informed) chart, refers to those people whose opinions are sought on an activity (two-way communication)
Consumer	One who utilizes goods
Consumerization	A model in which emerging technologies are first embraced by the consumer market and later spread to the business
Containers	A packaged environment that includes all necessary dependencies, executables and code for particular applications to run separately from the host computing device
Containment	Actions taken to limit exposure after an incident has been identified and confirmed
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 content filtering analyzes the data in the packet and packet filtering analyzes the attributes of the packet itself, e.g., source/target IP address and 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 the ability of an enterprise 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 over intuition) • Strategic context (strategic objectives of the enterprise) COBIT 5 and COBIT 2019 perspective
Contingency plan	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 might 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	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 feature	A floating-point feature with an infinite range of possible values; contrasts with discrete feature
Continuous improvement	The goals of continuous improvement (Kaizen) include elimination of waste (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.

TERM	DEFINITION
Continuous risk and control monitoring	A process that includes: • Developing a strategy to regularly evaluate selected information and technology (I&T)-related controls/metrics • Recording and evaluating I&T-related events and the effectiveness of the enterprise in dealing with those events • Recording changes to I&T-related controls or changes that affect I&T-related risk • Communicating the current risk and control status to enable information-sharing decisions involving the enterprise
Continuous variable	A variable whose value can be any of an infinite number of values, typically within a particular range
Contract account	The account (or address) created when a smart contract is deployed by the smart contract owner. Contract account contains the runtime virtual machine bytecode for a contract.
Contractual requirements	Result of analysis and refinement of customer requirements into a set of requirements suitable for inclusion in solicitation packages or supplier agreements. Contractual requirements include technical and nontechnical requirements necessary to acquire a solution. See Acquirer and Customer requirement
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 Internal control
Control center	Hosts the recovery meetings that manage disaster recovery operations
Control flow diagram	A diagram that depicts the set of all possible sequences in which operations may be performed during the execution of a system or program. Types include box diagram, flowchart, input-process-output chart and state diagram. Contrasts with data flow diagram.
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 presents 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 owner	A person to whom the enterprise has assigned the authority and accountability for making control-related decisions and who is responsible for ensuring that the control is implemented and is operating effectively and efficiently
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	Risk that assets are lost/compromised or that financial statements are materially misstated, due to lack of, or ineffective, design and/or implementation of internal controls

TERM	DEFINITION
Control risk self-assessment	A method/process by which management and staff at all levels collectively identify and evaluate risk and controls within their business areas. This assessment 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 result in risk not being reduced to an acceptable level in the relevant activity area (relevant risk threatens achievement of the objectives that are relevant to the activity area 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.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Convenience sampling	The use of a dataset that is not gathered scientifically in order to run quick experiments. Later on, it is essential to switch to a scientifically gathered dataset.
Convergence	A state reached during training in which training loss and validation loss change very little or not at all with each iteration after a certain number of iterations
Convolutional neural network	A deep learning (DL) method that uses layers of filters to extract features and patterns from data, particularly images
Cookie	A web browser message used 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).
Copyright	The protection of writings, recordings or other ways of expressing an idea. The idea itself may be common, but the way it was expressed is unique, such as a song or book.
Core assets	The assets essential to a solution and may include: • Components • Domain models • Requirements • Performance models • Estimates and plans • Test plans and test descriptions • Process descriptions
Corporate exchange rate	An exchange rate that can be used 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. Corporate governance consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives.
Corporate security officer (CSO)	The person responsible for coordinating the planning, development, implementation, maintenance and monitoring of the information security program

TERM	DEFINITION
Corrective control	A control designed to correct errors, omissions, unauthorized uses and intrusions, once they are detected
Correlation	The degree of relative correspondence between two sets of data. The correlation coefficient is a measure of how closely the two data sets correlate.
Corroboration	The practice of considering multiple pieces of objective evidence in support of a judgment regarding an individual CMMI model practice See Objective evidence
COSO (COSO)	The 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.
Cost-benefit analysis	A net result analysis that relies on the addition of positive factors and the subtraction of negative factors to build a business case supporting a risk response
COTS	Configurable, off-the-shelf software
Countermeasure	The reduction of threats or vulnerabilities through any direct process
Coupling	A measure of interconnectivity among the 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.
Covariant	A measure of the relationship between two variables whose values are observed at the same time. Whereas variance measures how a single variable deviates from its mean, covariance measures how two variables vary in tandem from their means.
Coverage	The proportion of known attacks detected by an intrusion detection system (IDS)
Coverage analysis	The determination and assessment of measures associated with the invocation of program structural elements to determine the adequacy of a test run. Coverage analysis is useful when attempting to execute each statement, branch, path or iterative structure in a program. Tools that capture this data and provide reports summarizing relevant information have this feature. See Testing, branch, Testing, path and Testing, statement.
CPU	See Central processing unit
Crack	To "break into" or "get around" the security of a software program *Scope Notes:* For example, certain newsgroups 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. Crack is commonly used in the case of cracking (unencrypting) a password or other sensitive data.
Crash	The sudden and complete failure of a computer system or component
Crash blossom	A sentence or phrase with an ambiguous meaning
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
Credit risk	The potential that a borrower or creditor will fail to meet financial obligations in accordance with agreed terms

TERM	DEFINITION
Criteria	Standards and benchmarks 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 control point	(QA) A function or an area in a manufacturing process or procedure, the failure of which, or loss of control over, may have an adverse effect on the quality of the finished product and may result in an unacceptable health risk
Critical design review	A review to verify that the detailed design of one or more configuration items satisfies specified requirements; to establish the compatibility among the configuration items and other items of equipment, facilities, software and personnel; to assess risk areas for each configuration item; and, as applicable, to assess the results of producibility analyses, review preliminary hardware product specifications, evaluate preliminary test planning and evaluate the adequacy of preliminary operation and support documents See System design review.
Critical functions	Business activities or information that cannot be interrupted or unavailable for several business days without significantly jeopardizing operation of the enterprise
Critical infrastructure	Systems whose incapacity or destruction will 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	The importance of a particular asset or function to the enterprise, and the impact if that asset or function is not available
Criticality analysis	Evaluation of 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 chain	Interoperability between two independent blockchains that allows blockchains to speak to each another, mainly during an asset swap or asset transfer
Cross-border data transfers	The transfer of personal data to recipients outside of the territory in which the data originate
Cross-border processing	Processing of personal data in the context of the activities of establishments in more than one country of a controller or processor, where the controller or processor is established in more than one country; or processing of personal data in the context of the activities of a single establishment of a controller or processor union but which substantially affects or is likely to substantially affect data subjects in more than one country
Cross-certification	A certificate issued by one certificate authority (CA) to a second CA that allows users of the first certification authority to obtain the public key of the second CA and verify the certificates that the second CA created *Scope Notes:* Often refers to certificates issued to each other by two CAs at the same level in a hierarchy

TERM	DEFINITION
Cross-site request forgery (CSRF)	A type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts (also known as a one-click attack or session riding). CSRF is pronounced sea-surf.
Cross-site scripting (XSS)	Injection of malicious scripts into otherwise benign and trusted websites *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 widespread and occur anywhere a web application uses input from a user within the output that it generates without validating or encoding it. Source: OWASP
Cross-validation	A mechanism for estimating how well a model will generalize to new data by testing the model against one or more nonoverlapping data subsets that are withheld from the training set
Cryptoassets	Decentralized virtual currencies (and their underlying blockchain technology layers) that are meant to achieve something other than the exchange of value
Cryptocurrency	A digital asset designed and created to function as a unit of account and payment method within its particular ecosystem. Cryptocurrency transactions usually take place within a peer-to-peer network and use cryptography to secure transaction records.
Cryptography	The study of mathematical techniques related to aspects of information security, such as confidentiality, data integrity, entity authentication and data origin authentication
Cryptosystem	Set of cryptographic primitives that are used to provide information security services. Most often, the term is used in conjunction with primitives providing confidentiality, i.e., encryption.
Cryptotoken	Unit that is used for any function not related to payments within a blockchain; for example, as a function of a decentralized application or a smart contract. Security tokens or utility tokens are examples of cryptotokens. A cryptotoken can also be considered a cryptoasset.
Culture	A pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things *Scope Notes:* COBIT 5 and COBIT 2019 perspective
Current risk	The risk state that exists in the moment, taking into account those actions that have already been taken but not actions that are anticipated or have been proposed
Customer	The party responsible for buying or accepting a solution or for authorizing payment for a solution. Customers may also be end users.
Customer relationship management (CRM)	Practices and strategies 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.
Customer requirement	The result of eliciting and consolidating needs, and resolving conflicts among those needs, expectations, constraints, and interfaces that clarifies and defines the solutions with affected stakeholders in a way that is acceptable to them See Customer.
Cyber and information security risk	The danger, harm or loss related to the use of, or dependence on, information and communications technology, electronic data, and digital or electronic communications
Cybercop	An investigator of activities related to computer crime
Cybercrime	Category of crime involving technology that may or may not involve the Internet
Cybercriminal	An individual or entity that uses technology with malicious intent
Cyberespionage	Activities conducted for the reason of security, business, politics or technology to find information that ought to remain secret. It is not inherently military.

TERM	DEFINITION
Cybersecurity	**1.** The protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems (ISACA) **2.** Protection and restoration of products, services, solutions and supply chain, including technology, computers, telecommunications systems and services, and information, to ensure their availability, integrity, authentication, transport, confidentiality and resilience. Cybersecurity is a part of information security. (CMMI)
Cybersecurity architecture	Description of the structure, components and topology (connections and layout) of security controls within the IT infrastructure of an enterprise *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.
Cyberthreat actor (CTA)	See Bad actor
Cyberthreat actor	See Bad actor
Cyberwarfare	Activities supported by military organizations with the purpose of threatening the survival and well-being of society/foreign entity
D3 (Data-driven documents)	A JavaScript library that eases the creation of interactive visualizations embedded in web pages. D3 is popular with data scientists as a way to present the results of their analysis.
Damage evaluation	The determination of the extent of damage to provide an estimate of the recovery time frame and the potential loss to the enterprise
DAP tools	Tools used to help control the data that end users can transmit
DASH7 Alliance Protocol (D7A)	A protocol used to enable wireless communications between actuators and sensors
Dashboard	A tool that is used for setting enterprise expectations at each level of responsibility and for continuous monitoring of the performance against set targets
Data	**1.** Representations of facts, concepts or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means. In the simplest terms, data are pieces of information. (ISACA) **2.** Qualitative or quantitative-based information that can be recorded, communicated and analyzed (CMMI)
Data accuracy	A component of data quality that indicates whether the data values stored for an object are the correct values and are represented in a consistent and unambiguous form
Data analysis	Obtaining an understanding of data by considering samples, measurement and visualization. Data analysis can be particularly useful when a data set is first received, before the first model is built, and is crucial for understanding experiments and debugging problems with the system.
Data anonymization	Protection of private or sensitive information by encrypting or removing personally identifiable information from data sets to keep the people whom the data represent anonymous
Data augmentation	Artificially boosting the range and number of training examples by transforming existing examples to create additional examples
Data breach	See Personal data breach.
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. Classification level is an indication of the value or importance of the data to the enterprise.

TERM	DEFINITION
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 concerning health	Personal data related to the physical or mental health of a natural person, including the provision of healthcare services, that reveal information about his or her health status
Data controller	See controller.
Data custodian	Individual(s) and department(s) responsible for the storage and safeguarding of computerized data
Data destruction	Elimination, erasure or clearing of data
Data dictionary	Repository that stores all the details that correspond to the data flow diagram (DFD) stores, processes and flows. It may be called a database that contains the name, type, range of values, source and authorization for access for each data element in a system. 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.
Data diddling	Changing data with malicious intent before or during input into the system
Data Encryption Standard (DES)	A legacy algorithm for encoding binary data that was deprecated in 2006. DES and its variants were replaced by the Advanced Encryption Standard (AES).
Data exception	An exception that occurs when a program attempts to use or access data incorrectly
Data exfiltration	Unauthorized acquisition of data from any network or endpoint
Data flow	The flow of data from the input (in Internet banking, ordinarily user input at his/her desktop) to the output (in Internet banking, ordinarily data in a bank's central database). Data flow includes travel through communication lines, routers, switches and firewalls, and processing through various applications on servers that process the data.
Data flow analysis	A software verification and validation (V&V) task to ensure that the input and output data and their formats are properly defined, and that the data flows are correct
Data flow diagram (DFD)	A diagram that depicts data sources, data sinks, data storage, processes performed on data (represented as nodes) and logical flow of data (represented as links between the nodes)
Data frame	A popular data type for representing data sets in pandas. A data frame is analogous to a table. Each column of the data frame has a name (a header), and each row is identified by a number.
Data governance	Setting direction on data use through prioritization and decision making, and ensuring alignment with agreed-on direction and objectives
Data integrity	The degree to which a collection of data is complete, consistent and accurate
Data leakage	Unauthorized transmission of data from an organization, either electronically or physically
Data life cycle	The sequence of steps that data go through, beginning with its collection/generation and ending with archiving or deleting data at the end of its useful life
Data loss prevention (DLP)	Detecting and addressing data breaches, exfiltration or unwanted destruction of data
Data minimization	Principle that requires data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Data mining	The use of computers to analyze large data sets to look for patterns that assist people in making business decisions

TERM	DEFINITION
Data normalization	A structured process for organizing data into tables in such a way that it preserves the relationships among the data
Data owner	Individual(s) who has responsibility for the integrity, accurate reporting and use of computerized data
Data portability	The ability to transmit a data subject's data from one controller to another
Data processing	Any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Data processor	A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller
Data protection authority	Independent authority that monitors and supervises the application of a data protection law
Data protection officer (DPO)	Enterprise officer who is responsible for informing and advising the enterprise about its data protection obligations and monitoring its compliance with them. The General Data Protection Regulation (GDPR) requires some enterprises to appoint a data protection officer.
Data recipient	Any person, public authority, agency or another body to which the personal data are disclosed, including third parties
Data retention	The policies that govern data and records management for meeting internal, legal and regulatory data archival requirements
Data science	A new branch of science used to extract knowledge and insights from large and complex data sets. Data science work often requires knowledge of both statistics and software engineering.
Data security	The controls that seek to maintain confidentiality, integrity and availability of information
Data set	A collection of related records
Data structure	A particular arrangement of data units, such as an array or a tree
Data subject	A natural person whose personal data are collected, held or processed
Data validation	**1.** A process used to determine whether data are inaccurate, incomplete or unreasonable. The process may include format checks, completeness checks, check key tests, reasonableness checks and limit checks. **2.** The checking of data for correctness or compliance with applicable standards, rules and conventions
Data warehouse (DW)	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 and advanced filtering
Data wrangling	The conversion of data, often through the use of scripting languages, to make data easier to manage
Data-oriented systems development	The focus on providing *ad hoc*reporting for users by developing a suitable accessible database of information and useable data rather than a function
Database	A collection of data, often with controlled redundancy, organized according to a schema to serve one or more applications. The data are stored so that they can be used by different programs without considering the data structure or organization. A common approach is used to add new data and modify and retrieve existing data. See Archival database.

TERM	DEFINITION
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 analysis	A software verification and validation (V&V) task to ensure that the database structure and access methods are compatible with the logical design
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 others. The beauty of replication is that it enables many users to work with their own local copy of a database while the database updates as if they were working on a single centralized database. For database applications in which users are distributed widely geographically, replication is often the most efficient method of database access.
Database security	The degree to which a database is protected from exposure to accidental or malicious alteration or destruction
Database specifications	The requirements for establishing a database application that include field definitions, field requirements and reporting requirements for the individual information in the database
Datagram	A packet (encapsulated with a frame containing information) transmitted in a packet-switching network from source to destination
Debugging	Determining the exact nature and location of a program error and fixing the error
Decentralization	The process of distributing computer processing to different locations within an enterprise
Decentralized autonomous organization (DAO)	A computer program on a blockchain that uses smart contracts to set organizational rules via decentralized means
Decision boundary	The separator between classes learned by a model in a binary class or multiclass classification problems
Decision coverage	A test coverage criterion requiring enough test cases so that each decision has a true and false result at least once, and each statement is executed at least once. Synonymous with branch coverage. Contrasts with condition coverage, multiple condition coverage, path coverage, statement coverage
Decision support systems (DSS)	An interactive system that provides the user with easy access to decision models and data to support semistructured decision-making tasks
Decision trees	A tree structure to represent a number of possible decision paths and an outcome for each path
Decoder	In sequence-to-sequence models, the part of the architecture that leverages the vectors provided by the encoder and generates an output sequence (e.g., the component that writes Spanish sentences in an English-to-Spanish machine translator)
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
Deep fake	Media manipulated by deep learning and other AI techniques to generate and synthesize convincing yet false representations of faces and facial expressions, sounds, voices, and speech, to depict individuals or scenes falsely, typically to promote misinformation or other malicious reasons.

TERM	DEFINITION
Deep learning	A multilevel algorithm that gradually identifies things at higher levels of abstraction, e.g., image classification
Deep model	A type of neural network containing multiple hidden layers
Deep packet inspection	A type of network packet filtering that evaluates the data and header of a packet transmitted through an inspection point
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. Default accounts 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 or the inverse of default
Default password	The password used to gain access when a system is first installed on a computer or network device *Scope Notes:* A large list published on the Internet and maintained at several locations exists. Failure to change these after the installation leaves the system vulnerable.
Default value	A standard setting or state taken by the program if no alternate setting or state is initiated by the system or the user or a value assigned automatically if one is not given by the user
Defect	Refer to bug, error, exception and fault.
Defect density	Number of defects per unit of solution size (e.g., the number of bugs per thousand lines of code)
Defense in depth	The practice of layering defenses to provide added protection. Defense in depth improves security by increasing the effort needed in an attack by placing multiple barriers between an attacker and enterprise computing and information resources.
Defense-in-depth approach	A systematic means of layering defenses to provide resiliency against exploited security vulnerabilities that can include aspects of physical, personnel, process, mission and cybersecurity needs
Defined process	The essential subset of organizational process assets for any tailored and managed process. A fully defined process has enough detail that it can be consistently performed by trained and skilled people and is both persistent and habitual. A defined process is necessary at the practice group level 3 in the CMMI Practice Areas. See Managed process.
Degauss	The application of variable levels of alternating currents 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 minimal residue of magnetic induction on the media. Degauss generally means to erase.
Deidentification	Information that cannot reasonably identify, relate to, describe, be associated with or linked, directly or indirectly, to a particular consumer
Deliverable	An item provided to an acquirer or other designated recipient as specified in an agreement, including a document, hardware item, software item, service or any type of work product See Acquirer.
Demilitarized zone (DMZ)	A small, isolated network that serves as a buffer zone between trusted and untrusted networks *Scope Notes:* A demilitarized zone is typically used to house systems, such as web servers, that must be accessible from both internal networks and the Internet.
Demodulation	The process of converting an analog telecommunications signal into a digital computer signal

TERM	DEFINITION
Demographic	A fact determined by measuring and analyzing data about a population, relying heavily on survey research and census data
Denial-of-service attack (DoS attack)	An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and either stops completely or operates at a significantly reduced rate
Dependent variable	In artificial intelligence (AI), the outcome predicted by a model, which is influenced by other independent variables
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.
Derived measure	Measure defined as a function of two or more base measures often expressed as ratios, composite indices or other aggregate summary measures See Base measure.
Derived requirements	Requirements not explicitly stated in customer requirements but inferred and developed from: • Contextual requirements, e.g., applicable standards, laws, policies, common practices, management decisions • Requirements needed to specify a solution component Derived requirements can also emerge during the analysis and design of solution components. See Product component requirements.
Design	The process of defining the architecture, components, interfaces and other characteristics of a system or component See Architectural design, Preliminary design and detailed design.
Design effectiveness	Occurring when the enterprise's controls are operated as prescribed by persons possessing the necessary authority and competence to perform the control effectively, satisfy the enterprise's control objectives and effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements
Design factors	Factors that can influence the design of an enterprise's governance system and position it for success in the use of information and technology (I&T). In COBIT® 2019, design factors include: enterprise strategy, enterprise goals, risk profile, I&T-related issues, threat landscape, compliance requirements, role of IT, sourcing model for IT, IT implantation methods, technology adoption strategy and enterprise size.
Design phase	The period of time in the software life cycle during which the designs for architecture, software components, interfaces and data are created, documented and verified to satisfy requirements
Design review	A formal, recorded, comprehensive and systematic examination of a solution or component design to determine whether the design meets applicable requirements, identifies problems and proposes solutions
Designee	A delegated appraisal role responsible for performing some tasks as specified in a defined Appraisal Method Definition Document in place of the appraisal sponsor or appraisal team leader. Designee's tasks performed must be clearly identified in the appraisal plan. Only those tasks not specifically reserved, i.e., via a "must" or "shall" statement, for the appraisal team leader or appraisal sponsor may be delegated.
Detailed IS controls	Controls over the acquisition, implementation, delivery and support of IS systems and services comprised of application controls and those general controls not included in pervasive controls
Detection risk	Risk that assets are lost or compromised or financial statements are materially misstated due to failure of an enterprise's internal controls to detect errors or fraud in a timely manner

TERM	DEFINITION
Detective application controls	Controls designed to detect errors that may have occurred based on predefined logic or business rules and usually executed after an action has taken place and often include a group of transactions
Detective control	Controls designed to detect and report when errors, omissions and unauthorized uses or entries occur
Develop, use and keep updated	A fundamental principle in CMMI denoting that work products resulting from projects and organizational processes must be used and useful to the work and enable performance. The work products should be kept current to reflect how work is performed or improved.
Developer	A person or group that designs and/or builds, and/or documents and/or configures the hardware and/or software of computerized systems
Development (Dev)	Creating a solution by deliberate effort. In some contexts, development can include maintenance of the developed product or service system. In the CMMI product suite, when this term is used with the phrase "development context specific," it is referring to this definition.
Development methodology	A systematic approach to software creation that defines development phases and specifies the activities, products, verification procedures and completion criteria for each phase See Incremental development, Rapid prototyping, Spiral model and Waterfall model.
Device	A generic term for a computer subsystem, such as a printer, serial port or disk drive that frequently requires its own controlling software termed a device driver
Device identity	Uniquely identifies a specific device
Device management provision tools	Tools that help in device provisioning (the process of attaching a certificate to the device identity)
DevOps	A combination of the terms: "development" and "operations." An enterprise software development phrase used to denote a type of agile relationship between development and Information Technology (IT) operations. The goal of DevOps is to change and improve the relationship between development and operations by advocating better communication and collaboration between these two business units.
Diagnostic	Pertaining to the detection and isolation of faults or failures (e.g., a diagnostic message and a diagnostic manual)
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 call is coming 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 dial-back control to remote user authentication.
Dialogue system	A system that simulates conversations with humans through text or speech using natural language processing (NLP) to understand user input, generate responses, and maintain a coherent flow of conversation when powering various applications like chatbots, virtual assistants, and customer service agents
Differential privacy	Achieved by adding randomly generated noise to obfuscate personal identifiability. Computations performed on altered data are only statistically/directionally correct (i.e., not accurate).
DigiCash	An electronic money corporation and the private, secure digital money it delivers
Digital asset	Any token—whether created in a peer-to-peer and/or cryptographic environment—that exists in a digital format with the token holder having the ability and right to use or transfer the digital asset. All cryptocurrencies and cryptotokens are subsets of digital assets.

TERM	DEFINITION
Digital certificate	An electronic credential that permits an entity to exchange information securely via the Internet using the public key infrastructure (PKI)
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 forensics	The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings
Digital signal processor (DSP)	Special processing unit specific to audio and telecommunication needs
Digital signature	An electronic identification of a person or entity using a public key algorithm that serves as a way for the recipient to verify the identity of the sender, integrity of the data and proof of transaction
Digital signature processor	Special processing unit specific to audio and telecommunication needs
Dimension reduction	A technique to extract one or more dimensions that capture as much of the variation in the data as possible
Dimensionality	In statistics, it refers to how many attributes a dataset has
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	An emergency event of such great magnitude that it overwhelms the capacity to respond and takes considerable time from which to recover
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 (DR)	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 (DRP)	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 (DRP)	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.

TERM	DEFINITION
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.
Discovery-based appraisal	An appraisal in which limited objective evidence is provided by the appraised organization prior to the appraisal, and the appraisal team probes and uncovers a majority of the OE during the onsite period necessary to obtain sufficient coverage of model components See Verification-based appraisal for contrast
Discrete variable	A variable whose potential values must be one of a specific number of values. Also known as discrete feature.
Discretionary access control (DAC)	Logical access control filters that may be configured or modified by the users or data owners
Discriminative model	A model that predicts labels from a set of one or more features. A discriminative model defines the conditional probability of an output based on the features and weights.
Discriminator	A system that determines whether examples are real or fake
Disk	A circular rotating magnetic storage hardware component. Disks can be hard (fixed) or flexible (removable) and can come in different sizes.
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 workstation	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 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

TERM	DEFINITION
Diverse routing	A method of routing traffic through split cable facilities or duplicate cable facilities *Scope Notes:* This can be accomplished with different 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, including dual entrance facilities, from the local carrier. 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, which 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 space with mechanical and electrical systems that can pose great risk due to potential human error and disasters.
DMZ	See demilitarized zone.
Document	A collection of information and data, regardless of the medium, that generally has permanence and can be read by humans or machines. Documents can be work products reflecting the implementation of processes that meet the intent and value of one or more model practices. Documents may be embedded within an automated, robotic or online system. Documents can be physical hard copies or soft copies that are accessible via hyperlinks in a web-based environment or application. Documents are used and kept updated. See Artifact and Record
Documentation	Aids for understanding the structure and intended uses of an information system or its components, such as flowcharts, textual material and user manuals
Documentation, software	Human-readable technical data or information, including computer listings and printouts, that describe or specify design features or other details, explain capabilities, or provide operating instructions to help users obtain desired results from a software system See Specification; Specification, requirements; Specification, design; Software design description; Test plan, Test report and User's guide.
Domain	In COBIT, the grouping of control objectives into four logical stages in the life cycle of investments involving IT (Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate).
Domain name system (DNS)	A hierarchical database distributed across the Internet, which allows names to be resolved into IP addresses (and vice versa) to locate services, such as web and email servers
Domain name system (DNS) exfiltration	A technique of tunneling over DNS to gain network access; a lower-level attack vector for simple to complex data transmission, slow but difficult to detect
Domain name system (DNS) poisoning	Corrupts the table of an Internet server's DNS, replacing an Internet address with the address of a 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 email 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's 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 spending	A potential blockchain flaw in which the native digital token or currency can be spent more than once

TERM	DEFINITION
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 permits corrective actions to be taken as required
Downfade	Wi-Fi signal condition that occurs when signals combine and produce lower signal strength—the inverse of upfade
Downloading	The act of transferring computerized information from one computer to another computer
Downsampling	Reducing the amount of information in a feature to train a model more efficiently
Downtime report	A report of the time that elapses when a computer is not operating correctly because of machine failure
Driver	A program that links a peripheral device or internal function to the operating system and provides for activation of all device functions; contrasts with test driver
Driver (value and risk)	An event or other activity that results in the identification of an assurance/audit need
Dry-pipe fire extinguisher system	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 in which two or more entities (usually persons) operate 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 actions generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review or analysis
Due professional care	The diligence that a person with a special skill would exercise under a given set of circumstances
Dumb terminal	A display terminal without processing capability *Scope Notes:* A dumb terminal is dependent on the main computer for processing. All entered data are accepted without further editing or validation.
Duplex routing	A method or communication mode of routing data over a 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 from DHCP servers, and parameters such as default gateways, subnet masks and domain name system (DNS) server IP addresses *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 model	A model that is trained online in a continuously updating fashion—that is, data are continuously entering the model
Dynamic partitioning	The variable allocation of central processing unit (CPU) processing and memory to multiple applications and data on a server
Dynamic ports	Dynamic, or private, ports in the range 49152 through 65535; not listed by IANA because of their dynamic nature

TERM	DEFINITION
E-commerce	The processes by which enterprises conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology *Scope Notes:* E-commerce encompasses both business-to-business (B2B) and business-to-consumer (B2C) e-commerce models but does not include existing nonInternet e-commerce methods based on private networks such as the electronic data interchange (EDI) and the Society for Worldwide Interbank Financial Telecommunication (SWIFT).
Early stopping	A method for regularization whereby model training ends before training loss finishes decreasing
Eavesdropping	Listening to a private communication without permission
Echo checks	The detection of line errors by retransmitting data to the sending device for comparison with the original transmission
Econometrics	The use of mathematical and statistical methods in the field of economics to verify and develop economic theories
Economic value added (EVA)	A 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) and more traditional capital investments such as physical property and equipment are measured against what shareholders could earn elsewhere
Edit control	The manual or automated detection of errors in the input portion of information sent to the computer for processing, allowing the user to edit data errors before processing
Editing	The process of ensuring that data conform to predetermined criteria and enable early identification of potential errors
Egress	The exiting of network communications
Electronic data interchange (EDI)	The electronic transmission of transactions (information) between two enterprises, promoting a more efficient paperless environment and often replacing 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 contain the data or information used as evidence of a contract or transaction between parties is considered together with the software program capable of reading 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, referring 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 (e.g., digital signatures)
Electronic vaulting	A data recovery strategy that allows enterprises to recover data within hours after a disaster *Scope Notes:* Electronic vaulting is typically used for batch/journal updates to critical files to supplement full backups taken periodically, including recovery of data from offsite storage media that mirror data via a communication link.

TERM	DEFINITION
Eligibility analysis	The description of the required criteria and analysis for determining and recording when an Action Plan Reappraisal can be conducted following a benchmark appraisal or sustainment appraisal See Action Plan Reappraisal.
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 *Scope Notes:* Smaller keys are more suitable to mobile devices.
Embedded audit module (EAM)	An integral part of an application system designed to identify and report specific transactions or other information based on predetermined criteria. Identification of reportable items occurs as part of real-time processing. Reporting may be real-time online or use store and forward methods. It is also known as an integrated test facility or a continuous auditing module.
Embedded software	Software part of a larger system that performs some of the requirements of that system, e.g., software used in an aircraft or rapid transit system. Such software does not provide an interface with the user. See firmware
Empowerment	Authority given to a person or group to perform a specific task
Encapsulation	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. In software development, it is a technique that isolates a system function or a set of data and the operations on those data within a module and provides precise specifications for the module. See abstraction, information hiding and software engineering
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
Encapsulation Security Payload (ESP)	A protocol 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 antireplay service (a form of partial sequence integrity) and (limited) traffic flow confidentiality. (RFC 4303). *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).
Encoder	In sequence-to-sequence models, the part of the architecture that processes the input sequence to provide the vectors that are leveraged by the decoder (e.g., the component that processes English sentences in an English-to-Spanish machine translator)
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 algorithm	A mathematically based function or calculation that encrypts/decrypts data, including block or stream ciphers
Encryption key	A piece of information in a digitized form used by an encryption algorithm to convert the plaintext to the ciphertext
Encryption tools	Tools used to encrypt data
End point	A device that can communicate with a connected network
End user	**1.** A person, device, program or computer system that uses an information system for the purpose of data processing in information exchange **2.** A person whose occupation requires the use of an information system but does not require any knowledge of computers or computer programming See user

TERM	DEFINITION
End-user computing	The ability of end users to design and implement their own information system using computer software products
Endpoint detection and response systems	Systems focused on detecting and investigating suspicious activities on end points
Engagement letter	Formal document that 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)	A description of the fundamental underlying design of the business system components or 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 (EA)	A 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 goal	*Scope Notes:* See business goal.
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 governance of information and technology (EGIT)	A concern for the value delivery from digital transformation and the mitigation of business risk that results from digital transformation. Three main outcomes can be expected after successful adoption of EGIT: benefits realization, risk optimization and resource optimization.
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
Entity relationship diagram (ERD)	A diagram that depicts a set of real-world entities and the logical relationships among them
Entry criteria	Conditions that must be met before an effort can begin successfully See exit criteria.
Environment	**1.** Everything that supports a system or the performance of a function **2.** The conditions that affect the performance of a system or function
Environmental risk	Threats to natural resources, human health and wildlife
Episode	Each of the repeated attempts by the agent to learn an environment in reinforcement learning
Epoch	A full training review of the entire dataset such that each example has been seen once. Thus, an epoch represents N/batch size training iterations where N is the total number of examples.
Epsilon greedy policy	A policy that either follows a random policy with Epsilon probability or a greedy policy otherwise in reinforcement learning
Eradication	The process of identifying and removing the root cause of an incident from the network when containment measures have been deployed after the incident occurs
Erasure	The data subject's ability to obtain the erasure of personal data from the controller; also known as the right to be forgotten
ERP (enterprise resource planning) system (ERP)	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®.

TERM	DEFINITION
Error	A deviation between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition See anomaly, bug, defect, exception and fault.
Error detection	Techniques used to identify errors in data transfers
Escrow agent	A person, agency or enterprise authorized to act on behalf of another to create a legal relationship with a third party regarding an escrow agreement; also known as 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, website, software source code or a cryptographic key) is delivered to a third party (named an escrow agent) to be held in trust or otherwise pending a contingency or the fulfillment of a condition(s) in a contract *Scope Notes:* Upon the occurrence of the escrow agreement, escrow agents will deliver the asset to the proper recipient; otherwise, the escrow agents are bound by their fiduciary duty to maintain the escrow account. Source code escrow signifies a 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.
Ethereum	An open source blockchain system enabling smart contracts and producing Ether as its native cryptocurrency
Ethereum request for comments (ERC)	Ethereum blockchain standards designed to enable Layer 2 tokens
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 attempt to access the network simultaneously
Evaluation	An examination of products, processes, services or environments to identify strengths and weaknesses
Evaluation appraisal	A consistent and reliable assessment method typically used to identify improvement opportunities or business performance without a rating. This includes clear and repeatable process steps used to conduct an initial gap analysis, performance improvement progress monitoring or readiness for benchmark appraisals or sustainment appraisals
Evaluation metric	A measure used to assess how well models perform their tasks like accuracy, precision, or recall
Event	Something that happens at a specific place and/or time
Event table	A table that lists events and the corresponding specified effect(s) of or reaction(s) to each event
Event type	One of three possible types of events for the purpose of IT risk management: threat event, loss event and vulnerability event *Scope Notes:* The ability to consistently and effectively discern 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.

TERM	DEFINITION
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 *Scope Notes:* Audit perspective
Example activities	Possible actions that may be taken when implementing processes that meet the intent of a practice. The intent of "Example Activities" is to serve as guidance and suggestions, not as required activities; it is not intended to be a comprehensive list.
Example work products	Possible outputs of implementing processes that meet the intent of a practice. The intent of "Example Work Products" is to serve as guidance and suggestions, not as required work products; it is not intended to be a comprehensive list.
Exception	An event that causes suspension of normal program execution. Types include addressing exception, data exception, operation exception, overflow exception, protection exception and underflow exception.
Exception reports	Reports generated by a program that identifies transactions or data that appear to be incorrect *Scope Notes:* Exception reports contain items that may be outside a predetermined range or may not conform to specified criteria.
Exclusive-OR (XOR)	An operator that 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 generally referred to as the object or load module
Exit criteria	Conditions that must be met before successful completion of an effort
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.
Explainable artificial intelligence (AI)	Artificial intelligence (AI) systems that provide transparent and understandable explanations for decisions or predictions, enabling users to comprehend the reasoning behind AI-generated outcomes
Exploding gradient problem	The tendency for gradients in deep neural networks (especially recurrent neural networks) to become surprisingly steep (high)
Exploit	A method used to take advantage of a vulnerability
Exposure (EF)	The potential loss to an area due to the occurrence of an adverse event
Extended Binary Coded Decimal Interchange Code (EBCDIC)	An 8-bit code representing 256 characters; used in most large computer systems
Extended enterprise	An enterprise that extends outside its traditional boundaries. Such enterprises 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)

TERM	DEFINITION
eXtensible Markup Language (XML)	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; promulgated through the World Wide Web Consortium
External router	A 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 a border router
External storage	The location that contains backup copies to be used in case recovery or restoration is required in the event of a disaster
Externally owned account (EOA)	An address generated from a user's public key. An EOA is typically owned by an individual
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.
Fail-over	The transfer of service from an incapacitated primary component to its backup component
Fail-safe	A system or component that automatically places itself in a safe operational mode in the event of a failure Source: IEEE
Failure	The inability of a system or component to perform its functions within specified performance requirements Source: IEEE See Bug, Crash, Exception and Fault.
Failure analysis	Determining the exact nature and location of a program error to fix the error, to identify and fix other similar errors and to initiate corrective action to prevent future occurrences of this type of error. Contrasts with debugging.
Fall-through logic	An optimized code, based on a branch prediction, that predicts which way a program will branch when an application is presented
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.
False authorization	Also called false acceptance, occurs when an unauthorized person is identified as an authorized person by the biometric system
False negative (FN)	An example in which the model mistakenly predicted the negative class
False positive (FP)	An example in which the model mistakenly predicted the positive class
Fault tolerance	A system's level of resilience to seamlessly react to hardware and/or software failure
Feasibility study	Analysis of the known or anticipated need for a product, system or component to assess the degree to which the requirements, designs or plans can be implemented
Feature	The machine-learning expression for a piece of measurable information about something. For example, if researchers store the age, annual income and weight of a set of people, they are storing three features about them.

TERM	DEFINITION
Feature cross	A synthetic feature formed by crossing (i.e., taking a Cartesian product of) individual binary features obtained from categorical data or from continuous features via bucketing. Feature crosses help represent nonlinear relationships.
Feature engineering	The process of extrapolating features from raw data. Depending on the task, this step might involve the selection, manipulation, and transformation of data.
Federated learning	A distributed machine-learning approach that trains machine-learning models using decentralized examples residing on devices such as smartphones
Feedforward neural network (FFN)	A neural network without cyclic or recursive connections. For example, traditional deep neural networks are feedforward neural networks.
Few-shot learning	A machine-learning approach, often used for object classification, designed to learn effective classifiers from only a small number of training examples
Fiber-optic cable	A cable made of glass fibers that transmits 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	**1.** On a data medium or in storage, a specified area used for a particular class of data, e.g., a group of character positions used to enter or display wage rates on a screen **2.** Defined logical data that is part of a record **3.** The elementary unit of a record that may contain a data item, a data aggregate, a pointer or a link **4.** A discrete location in a database that contains a unique piece of information. A field is a component of a record. A record is a component of a database.
File	**1.** A set of related records treated as a unit, e.g., in stock control, a file can consist of a set of invoices **2.** The largest unit of storage structure that consists of a named collection of all occurrences in a database of records of a particular record type
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.)
File-integrity monitoring	Detecting changes to files and configurations to determine any changes to a baseline
Filing system	Structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.
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.

TERM	DEFINITION
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.
Fine-tuning pretrained models	The process of training only a small portion of a large pretrained model so that it can learn how to perform a task for which it had not been originally trained
Finger	A protocol and program that allows the remote identification of users logged into a system.
Fire protection system	Systems that help to mitigate the unwanted effects of a fire
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	The combination of a hardware device, e.g., an IC, and computer instructions and data that reside as read only software on that device. Such software cannot be modified by the computer during processing. See Embedded software.
First responder interfaces	Systems used to document and communicate information about a breach or other security incident by those first responding to the breach or incident
Fiscal year	Any yearly accounting period without regard to its relationship to a calendar year.
Flat file	A data file that does not physically interconnect with or point to other files. Any relationship between two flat files is logical, e.g., matching account numbers.
Flowchart or flow diagram	**1.** Graphical representation in which symbols are used to represent such things as operations, data, flow direction and equipment, for the definition, analysis or solution of a problem **2.** A control flow diagram in which suitably annotated geometrical figures are used to represent operations, data or equipment, and arrows are used to indicate the sequential flow from one to another. Synonymous with flow diagram. See Block diagram, Box diagram, Bubble chart, Graph, Input-Process-output chart and Structure chart.
Focus area	An area that describes a certain governance topic, domain or issue that can be addressed by a collection of governance and management objectives and their components.
Fog computing	Computing architecture that conducts a large portion of data computations on edge devices
Follow-up activity	Activity that determines whether management has taken appropriate corrective actions to resolve deficiencies.
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.
FORTRAN	An acronym for FORmula TRANslator, the first widely used high-level programming language. Intended primarily for use in solving technical problems in mathematics, engineering and science

TERM	DEFINITION
Forward error correction (FEC)	Error controlling mechanism for channels with a large amount of interference
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	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 among the entities involved, the roles of those involved and the boundaries (what is and is not included in the governance system). See Control framework and IT governance framework.
Fraud	Any act involving the use of deception to obtain illegal advantage
Freeware	A type of software available free of charge
Frequency	A measure of the rate by which events occur over a certain period of time
Frequency analysis	An analysis that determines how often a particular risk scenario might be expected to occur during a specified period of time
Full economic life cycle	The period of time during which material business benefits are expected to arise, 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
Full node	A critical network device that supports and provides security for the blockchain and is capable of validating and relaying new blocks into the chain
Function	**1.** A mathematical entity whose value (the value of the dependent variable) depends on the values of one or more independent variables, with not more than one value of the dependent variable corresponding to each permissible combination of values from the respective ranges of the independent variables **2.** A specific purpose of an entity, or its characteristic action **3.** In data communication, a machine action, such as carriage return or line feed
Function point analysis (FPA)	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.
Functional analysis	**1.** A type of analysis that verifies whether or not each safety-critical software requirement is covered and that an appropriate criticality level is assigned to each software element (ISACA) **2.** An examination of solution components to broaden and deepen understanding (CMMI)
Functional architecture	The conceptual structure and logical arrangement of functions. This may include internal and external interface functions. See Architecture and Functional Analysis
Functional design	**1.** The process of defining the working relationships among the components of a system. See Architectural Design **2.** The result of the process in definition 1

TERM	DEFINITION
Functional requirement	A requirement that specifies the function(s) that a system or system component must be able to perform
Functional safety	The detection of a potentially dangerous condition resulting in the activation of a protective or corrective solution to prevent hazardous events from arising, or the act of providing mitigation to reduce the consequence of the hazardous event. The aspect of the overall safety of a solution, solution component or piece of equipment that depends on the automatic protection mechanisms operating correctly in response to its inputs or failure in a predictable manner (fail-safe). An automatic protection system may be designed to properly handle likely human errors, hardware, solution or solution component failures and operational/environmental stress.
Garbage in, garbage out (GIGO)	The concept of data that is nonsensical, or flawed, especially as it relates to the computational sciences
Gas	A unit/fee that measures the amount of computational effort required to execute certain operations related to a function or smart contract on a blockchain. Best known in relation to the Ethereum blockchain/network.
Gas fee	The cost required to process a transaction on the network (specific to the Ethereum blockchain). Miners can set the price of gas and decline to process a transaction if it does not meet the price threshold that they determine.
Gateway	A physical or logical device on a network that serves as an entrance to another network (e.g., router, firewall or software)
GB	Gigabyte
Gemba walk	The term used to describe personal observation of work; where the work is happening. The original Japanese term comes from *gembutsu*, which means “real thing." It also known as “genba walk.”
General Architecture for Text Engineering (GATE)	An open-source, Java-based framework for natural language processing tasks. The framework lets developers pipeline other tools designed to be plugged into it. The project is based at the UK University of Sheffield.
General computer control	A control, other than an application control, that relates to the environment in which computer-based application systems are developed, maintained and operated and 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 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 security policy, the organization of IS staff to separate conflicting duties and the development of a disaster prevention and recovery plan.
Generalization	The ability of a model to make correct predictions on new, previously unseen data, as opposed to the data used to train the model
Generalized audit software (GAS)	Multipurpose audit software that can be used for general processes, such as record selection, matching, recalculation and reporting
Generative adversarial network	An architecture consisting of two neural networks, the generator and the discriminator, competing as adversaries in a zero-sum game, with the generator creating new data and the discriminator iteratively refining its ability to distinguish real data from generated data
Generative artificial intelligence (AI)	A branch of artificial intelligence (AI) that, by using models to learn underlying patterns and relationships within data, addresses the creation of new and diverse content, such as images, text, audio, or code
Generic process control	A control that applies to all processes of the enterprise

TERM	DEFINITION
Generic Routing Encapsulation (GRE)	An IP encapsulation protocol for transmitting network traffic between network nodes
Genetic data	Personal data that relates to the inherited or acquired genetic characteristics of a natural person and gives unique information about the physiology or health of that natural person. Genetic data results, in particular, from an analysis of a biological sample from the natural person in question.
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.
Gigabyte (GB)	A unit of data storage that equals approximately one-billion bytes (or precisely 2^{30} or 1,073,741,824 bytes)
Good practice	A proven activity or process that has been successfully used by multiple enterprises and shown to produce reliable results
Governance	The method by which an enterprise evaluates stakeholder needs, conditions and options to determine balanced, agreed-upon enterprise objectives to be achieved. It involves setting direction through prioritization, decision making and monitoring performance and compliance against the agreed-upon direction and objectives.
Governance component	Factors that, individually and collectively, contribute to the successful operation of the enterprise's governance system over information and technology (I&T). Components interact with each other resulting in a holistic governance system for I&T. Components include processes; organizational structures; principles, policies and procedures; information; culture, ethics and behavior; people, skills and competencies; and services, infrastructure and applications.
Governance enabler	Something (tangible or intangible) that assists in the realization of effective governance *Scope Notes:* COBIT 5 perspective (this term was updated to "governance component" in COBIT 2019)
Governance framework	A basic conceptual structure used to solve or address complex issues. In the governance context, a framework is used to build a governance system for the enterprise. In COBIT 2019, a governance framework should: **1.** be based on a conceptual model, identifying the key components and relationships among components to maximize consistency and allow automation. **2.** be open and flexible, allowing for the addition of new content and the ability to address new issues in the most flexible way while maintaining integrity and consistency. **3.** align to relevant major standards, frameworks and regulations.
Governance of enterprise IT	A governance view that ensures that information and related technology support and enable the enterprise strategy and 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

TERM	DEFINITION
Governance system	The core requirements that underlie the governance over enterprise information and technology. In COBIT 2019, the six principles for a governance system are: **1.** Providing stakeholder value **2.** Holistic approach **3.** Dynamic governance system **4.** Governance distinct from management **5.** Tailored to enterprise needs **6.** End-to-end governance system
Governance, risk management and compliance (GRC)	A business term used to group the three closely related disciplines responsible for operations and the protection of assets
Governance/ management objective	The outcomes (objectives) for achieving enterprise goals for information and technology. In COBIT 2019, a governance or management objective always relates to one process, a governance objective relates to a governance process and a management objective relates to a management process. Boards and executive management are typically accountable for governance processes, while management processes are the domain of senior and middle management.
Governance/ management practice	For each COBIT 5 process, practices that 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
Gradient boosting	A machine-learning technique for regression and classification problems that produces a prediction model in the form of an ensemble of weak prediction models, typically decision trees. It builds the model in a stage-wise fashion, like other boosting methods, and generalizes them by allowing the optimization of an arbitrary differentiable loss function.
Gradient descent	An optimization algorithm for finding the input to a function that produces the largest (or smallest) possible value
Graph	A diagram or other representation consisting of a finite set of nodes and internode connections called edges or arcs. Contrasts with blueprint. See Block diagram, Box diagram, Bubble chart, Call graph, Cause-effect graph, Control flow diagram, Data flow diagram, Directed graph, Flowchart, Input-process-output chart, Structure chart and Transaction flowgraph.
Graphic software specifications	The documents, such as charts, diagrams and graphs, that depict program structure, states of data, control, transaction flow, HIPO and cause-effect relationships. Tables, including truth, decision, event, state-transition, module interface, and exception conditions/responses are necessary to establish design integrity.
Graphics processing unit	A special processing unit made to render high-quality images and video files
Greedy policy	A policy in reinforcement learning that always chooses the action with the highest expected return
Ground truth	The correct answer; reality. Since reality is often subjective, expert raters typically are the proxy for ground truth.
Guideline	A description of a particular way of accomplishing something that is less prescriptive than a procedure
Habit and persistence	The routine way of doing business and following and improving processes that an enterprise demonstrates as part of its culture

TERM	DEFINITION
Hacker	An individual who attempts to gain unauthorized access to a computer system
Hallucination	In generative artificial intelligence (AI), the generation of false or misleading information presented as fact
Handprint scanner	A biometric device used to authenticate a user through palm scans
Haptic technology	A technology feature that renders an event of physical contact to a user through the application of vibrations
Hard disk drive	Hardware used to read from or write to a hard disk See Disk and Disk drive
Hard fork	A change to blockchain software that make its so any nodes validating according to the old software will see all blocks produced after the new software as invalid. For blockchain nodes to work in alignment with the new software, each will be required to upgrade. If a group of nodes does not upgrade and perpetuate the use of the old version of the software, a permanent split in the blockchain can occur.
Harden	The process of configuring a computer or other network device to resist attacks
Hardware	Physical equipment, as opposed to programs, procedures, rules and associated documentation; contrasts with software
Hardware engineering	The application of a systematic, disciplined and measurable approach to transforming a set of requirements using documented techniques and technology to design, implement and maintain a tangible solution. In CMMI, hardware engineering represents all technical fields, e.g., electrical and mechanical, that transform requirements and ideas into tangible solutions. See Software engineering and Systems engineering
Hash	A cryptographic 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.
Hash function	**1.** 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 **2.** Fixed values derived mathematically from a text message
Hash power	The individual unit of power contributed by a single miner or worker to the proof-of-work (PoW) hash rate
Hash rate	A measure of computational power. The proof-of-work (PoW) blockchain network measures the security profile using the total hash rate provided by all full nodes in supporting the consensus algorithm. Generally, the higher the total hash rate, the more secure the PoW blockchain network.
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 the accuracy of processing.
Hashed timelocks	A technical approach that involves a type of smart contract utilized in cryptoasset transactions and designed to remove counterparty risk, which is the risk that the other party to a transaction cannot participate in the trade

TERM	DEFINITION
Hashing	**1.** A technique involving using a hash function (algorithm) to create hash valued or checksums that validate message integrity **2.** In data processing and machine learning, a mechanism for bucketing categorical data, particularly when the number of categories is large, but the number of categories actually appearing in the dataset is comparatively small
Hazard	A condition or event that poses a risk to safety. Hazards can be internal or external.
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	A quick solution to a problem, which may or may not be the best solution
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	The base-16 number system. Digits are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F. This is a convenient form in which to examine binary data because it collects four binary digits per hexadecimal digit, e.g., decimal 15 is 1111 in binary and F in hexadecimal.
Hidden layer	A synthetic layer in a neural network between the input layer (the features) and the output layer (the prediction). Hidden layers typically contain an activation function (e.g., ReLU) for training. A deep neural network contains more than one hidden layer.
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.
High maturity	A classification based on the Capability Maturity Model Integration (CMMI) model for processes. CMMI model practice group levels (and their associated practices) of 4 or 5 are considered high maturity. High maturity organizations and projects use quantitative and statistical analysis to determine, identify and manage central tendency and dispersion and understand and address process stability and capability and how these impact the achievement quality and process performance objectives.
High-level language	A programming language that requires little knowledge of the target computer; can be translated into several different machine languages; allows symbolic naming of operations and addresses; provides features designed to facilitate the expression of data structures and program logic; and usually results in several machine instructions for each program statement. Examples are PL/1, COBOL, BASIC, FORTRAN, Ada, Pascal and C. This term contrasts with assembly language.
Hijacking	An exploitation of a valid network session for unauthorized purposes
Histogram	A graphical representation of the distribution of a set of numeric data, usually a vertical bar graph
Homomorphic encryption	A type of encryption that supports two primitive operations in the ciphertext/encrypted space—multiplication and addition of two homomorphically encrypted values—wherein the decrypted product or sum provides a meaningful (i.e., when decrypted, the result would be the same as if performed on unencrypted values) value (only category of encryption wherein operations of encrypted yield meaningful result[s])

TERM	DEFINITION
Honeypot	A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner so that their actions do not affect production systems
Horizontal defense in depth	The controls that are in place to access an asset (this is functionally equivalent to the concentric ring model)
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.
Human firewall	A person prepared to act as a network layer of defense through education and awareness
Hurdle rate	A 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	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
Hybrid blockchain	A blockchain that attempts to use optimal parts of private and public blockchain solutions; hybrid blockchains are not open to all parties, but still maintain the immutability, transparency and integrity features of public chains
Hybrid cloud	A cloud computing environment that combines services and resources from both private and public clouds
Hypercall	A stopgap between a hypervisor and the host to filter and control privileged operations
Hyperledger	An umbrella project started by the Linux Foundation, with participation by IBM, Intel and SAP, to build open source blockchains and related tools
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
Hyperparameter	A parameter that specifies the details of the learning process
Hyperparameter tuning	The parameters that are tweaked during successive runs of training a model
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 such as headings, paragraphs and lists–and can be used to describe, to some degree, the appearance and semantics of a document
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.
Hypertext Transfer Protocol Secure (HTTPS)	A protocol for accessing a secure web server, whereby all data transferred are encrypted. A standard port number is 443.
Hyperthreading	The intel propriety implementation of simultaneous multithreading

TERM	DEFINITION
Hypervisors	A type of software that allows multiple virtual machines to be run on a host machine or group of host machines
I/O	The acronym for input/output
Identifiability	A condition that results in a personally identifiable information (PII) principal being identified, directly or indirectly, on the basis of a given set of PII
Identifiable natural person	Someone who can be identified, directly or indirectly, from an identifier, such as a name, identification number, location data, online identifier or from one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Identifier	A set of attribute values that unambiguously distinguishes one entity from another. The total list of an entity's attribute values allows it to be unambiguously distinguished from all other entities within a given context and also recognized as a single identity in that context.
Identity and access management (IAM)	A framework that encapsulates people, processes and products to identify and manage the data used in an information system, 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) (IEEE)	An organization composed of engineers, scientists and students. IEEE is pronounced "I-triple-E." *Scope Notes:* Best known for developing standards for the computer and electronics industry
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.
Image processing	The process of electronically inputting source documents by taking an image of the document, thereby eliminating the need for key entry
Image recognition	A process that classifies objects, patterns or concepts in an image. Image recognition is also known as image classification.
Image synthesis	The process of creating new images that share characteristics with existing data. Generative adversarial networks excel at generating images.
Imaging	A process that allows one to obtain a bit-for-bit copy of data to avoid damaging the original data or information when multiple analyses are performed *Scope Notes:* The imaging process helps in obtaining 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.
Immutable	A term that describes something that is unable to be modified after creation
Impact	A magnitude of loss resulting from a threat exploiting a vulnerability
Impact analysis	A study to prioritize the criticality of information resources for the enterprise based on the costs (or consequences) of adverse events. In an impact analysis, threats to assets are identified and potential business losses are determined for different time periods. This assessment is used to justify the safeguards required and recovery time frames. This analysis is the basis for establishing the recovery strategy.

TERM	DEFINITION
Impact assessment	A review of the possible consequences of a risk See Impact analysis
Impairment	A condition that causes a weakness or diminished ability to execute audit objectives *Scope Notes:* Impairment to organizational independence and individual objectivity may include a personal conflict of interest; scope limitations; restrictions on access to records, personnel, equipment or facilities; and resource limitations (such as funding or staffing).
Impersonation	An entity that mimics a system, process or person in an attempt to manipulate the user into an action that can cause an unexpected or unwanted event to a system
Implement	In business, the full economic life cycle of an 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	The process of translating a design into hardware components, software components or both See Coding
Implementation life cycle review	The controls that support the process of transforming an 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
Implementation phase	The period of time in the software life cycle during which a software product is created from design documentation and debugged
Improvement in progress	A type of preliminary or final finding statement that reflects the current state of a practice area or practice newly implemented for a project(s) or organizational unit and shows promise of helping to achieve further improvement. Due to the recent nature of process implementation, artifacts may be limited.
Improvement opportunity	A type of preliminary or final finding about a particular practice area or practice which typically meets the intent and value of a model practice but represents an opportunity for the process to be improved
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, guidelines or standard security practices
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. Incident response may include evacuation of a facility, initiating a disaster recovery plan (DRP), performing a damage assessment or any other measures necessary to bring an enterprise to a more stable status.
Incident response plan (IRP)	The operational component of incident management (also called IRP) *Scope Notes:* The plan includes documented procedures and guidelines for defining the criticality of incidents, reporting and escalation processes and recovery procedures.
Incident response tools	Tools used to identify and address cyberattacks or other digital security threats
Inconsequential deficiency	A deficiency wherein a reasonable person would conclude, after considering the possibility of further undetected deficiencies, that the deficiency, either individually or when aggregated with others, would 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.

TERM	DEFINITION
Incremental development	A software development technique in which requirements definition, design, implementation and testing occur in an overlapping, iterative (rather than sequential) manner, resulting in incremental completion of the overall software product. Contrasts with rapid prototyping, the spiral model and the waterfall model.
Incremental integration	A structured reformation of the program, module by module or function by function, with an integration test being performed following each addition. Methods include top-down, breadth-first, depth-first and bottom-up.
Incremental testing	The deliberate testing of only the value-added functionality of a software component
Independence	A type of self-governance that includes freedom from conflict of interest and undue influence. An IT auditor should be free to make his/her own decisions and not be influenced by the organization being audited and its people (managers and employees).
Independent attitude	An attitude with an impartial point of view. This attitude allows an IS auditor to act objectively and with fairness.
Independently and identically distributed (i.i.d.)	Data from a distribution that does not change, and where each value drawn does not depend on values that have been drawn previously. An i.i.d. is the ideal gas of machine learning—a useful mathematical construct but almost never exactly found in the real world.
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
Individual data sovereignty	The capability of data subjects (owners of personal data) to manage and/or delimit the use of their personal data, according to applicable laws and regulations
Industry standard	The procedures and criteria recognized as acceptable practices by peer professionals, credentialing or accrediting organizations
Inference	The process of making predictions by applying the trained model to unlabeled examples in machine learning
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 and COBIT 2019 perspective
Information and technology (I&T) operations and service delivery risk (I&T)	Risk related to the performance of IT systems and services. A poorly performing IT operation can bring destruction or reduction of value to the enterprise.
Information and technology (I&T)-related risk	A part of overall business risk associated with the use, ownership, operation, involvement, influence and adoption of information and technology (I&T) within an enterprise
Information architecture	One component of IT architecture (together with applications and technology)
Information criteria	Information attributes that must be satisfied to meet business requirements
Information engineering	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

TERM	DEFINITION
Information hiding	The practice of hiding the details of a function or structure, making them inaccessible to other parts of the program See Abstraction, Encapsulation and Software engineering.
Information processing facility (IPF)	The computer room and support areas
Information security	The assurance that information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and nonaccess when required (availability). Information security deals with all formats of information—paper documents, digital assets, intellectual property in people's minds and verbal and visual communications.
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 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 information security resources are used responsibly.
Information security program	The 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 security testing tools	ools used to test the accuracy and completeness of an enterprise's cybersecurity practices and controls
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
Informative material	A type of material that includes everything other than the required information. Explanatory information in practice are part of the informative material. Informative material also includes the overview and appendices, e.g., glossary and index. Informative material must not be ignored, as it is needed to correctly understand and adopt the model. External links can be added to the informative material. These are links to external assets such as: • Additional informative material • Adoption examples • Transition and adoption guidance from one model or standard to others • Templates • Training materials • Inherent security risk • The risk level or exposure without taking into account the actions that management has taken or might take
Informed	Refers to those people who are kept up to date on the progress of an activity (one-way communication) in a RACI (Responsible, Accountable, Consulted, Informed) chart.
Infrastructure as a Service (IaaS)	A form of cloud computing that offers the capability to provision processing, storage, networks and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, including operating systems and applications

TERM	DEFINITION
Infrastructure risk	The risk that information and technology (I&T) infrastructure and systems may be unable to effectively support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion
Ingestion	A process to convert extracted information to a format that can be understood by investigators See Normalization
Ingress	Traffic that comes into a network
Inherent risk	The level of risk or exposure that does not account for the actions management has taken or might take (e.g., implementing controls)
Inherent security risk	The level of risk or exposure that does not account for the actions management has taken or might take
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 type of attack involving initialization vectors (IVs). Wired equivalent privacy (WEP) can allocate the RC4 IVs used to create the keys that can drive a pseudo-random number generator, which 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 key reuse. The WEP standard also fails to specify how these IVs are assigned. Many wireless network cards reset the 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 that result in key reuse can create a susceptibility to attacks. These attacks require a large number of packets (5-6 million) to fully derive the WEP key; on a large, busy network, this can occur in a short time, sometimes as quickly as 10 minutes (however, some of the largest corporate networks will likely require much more time to gather enough packets). In WEP-protected wireless networks, often multiple, or all, stations use the same shared key. This increases the chances of IV collisions greatly. The result is that the network becomes insecure if the WEP keys are not frequently changed, which furthers the need for a WEP key management protocol.
Injection	A general term for attack types that inject code that is then interpreted/executed by the application *Source Notes*: OWASP
Input control	Techniques and procedures used to verify, validate and edit data to ensure that only correct data are entered into the computer
Input-processing-output	A structured software design technique. Identification of the steps involved in each process is performed, including the inputs and outputs in each step. A refinement called hierarchical input-process-output identifies the steps, inputs and outputs for both general and detailed levels.
Input/output (I/O)	A way for microprocessors and computers to communicate with the outside world to get the data needed for programs and communicate the results of its data manipulations. This is accomplished through I/0 ports and devices.
Insider threat software	Software designed to detect and mitigate actions by insiders who may pose a threat to an enterprise
Insider threats	Threats to an enterprise that come from individuals within the enterprise, such as employees or contractors
Installation	The phase in the system life cycle that includes assembly and testing of the hardware and software of a computerized system. Installation includes installing a new computer system, software or hardware or otherwise modifying the current system.

TERM	DEFINITION
Installation and checkout phase	The period of time in the software life cycle during which a software product is integrated into its operational environment and tested to ensure that it performs as required
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) and connected over a network, such as the Internet.
Institute of Electrical and Electronic Engineers (IEEE)	An organization involved in the generation and promulgation of standards. IEEE standards represent the formalization of current norms of professional practice through the process of obtaining the consensus of concerned practicing professionals in a given field.
Instruction	**1.** A program statement that causes a computer to perform a particular operation or set of operations **2.** In a programming language, a meaningful expression that specifies one operation and identifies its operands, if any
Instruction set	**1.** The complete set of instructions recognized by a given computer or provided by a given programming language **2.** The set of the instructions of a computer, a programming language or the programming languages in a programming system See Computer instruction set
Intangible asset	An asset that is not physical in nature *Scope Notes:* Examples include intellectual property (patents, trademarks, copyrights and processes), goodwill and brand recognition.
Integrated circuit (IC)	An electronic circuit comprised of capacitors, transistors and resistors that is the building block of most electronic devices and equipment. It is also referred to as a chip or microchip.
Integrated services digital network (ISDN)	A public end-to-end digital telecommunications network with signaling, switching and transport capabilities that support a wide range of services 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.
Integration environment	The configuration of processes, systems, tools, people and associated infrastructure used when combining components to develop a solution
Integrity	The guarding against improper information modification or destruction. This includes ensuring information nonrepudiation and authenticity.
Integrity risk	The risk that data may be unavailable due to incompleteness or inaccuracy
Intellectual property	Intangible assets that belong to an enterprise for its exclusive use. Examples include patents, copyrights, trademarks, ideas and trade secrets.
Intent and value	A statement for the purposes of characterization and rating. When the phrases “intent and value” or “meet the intent and value” are used in the Medical Definition Document (MDD), it means the appraisal team must review and analyze Objective Evidence (OE) for the practice area intent, practice statement intent *and* their corresponding value statements. They must also present any additional required Practice information in order to characterize and rate accurately.
Intent-based networking (IBN)	A form of network administration that incorporates artificial intelligence (AI), network orchestration and machine learning (ML) to automate administrative tasks across a network

TERM	DEFINITION
Interactive	A system or mode of operation in which each user entry causes a response from or action by the system. This is in contrast to batch processing. See Conversational, Online and Real time.
Interface	**1.** A shared boundary between two functional units, defined by functional characteristics, common physical interconnection characteristics, signal characteristics and other characteristics, as appropriate. The concept involves the specification of the connection of two devices having different functions. **2.** A point of communication between two or more processes, persons or other physical entities. **3.** A peripheral device that permits two or more devices to communicate.
Interface data	Information describing interfaces or connections
Interface or connection	A shared boundary across components, humans, services, hardware or software that needs or exchanges information or data. Either the term “interface” or “connection” may be used to describe this boundary.
Interface or connection description	A description of the functional and physical characteristics of a component and its boundaries, e.g., user, system, that describes its interaction with another component
Interface testing	A testing technique 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 an 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 the preparation of financial statements in accordance with generally accepted accounting principles and that receipts and expenditures of the registrant are made only in accordance with authorizations of management and directors of the registrant • Provide reasonable assurance regarding the 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

TERM	DEFINITION
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	An 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 an investment project.
Internal storage	The main memory of the computer's central processing unit (CPU)
International Organization for Standardization (ISO)	An organization that sets international standards. It deals with all fields except electrical and electronics, which are governed by the International Electrotechnical Commission (IEC). Synonymous with the International Standards Organization.
International Standards Organization (ISO)	The world's largest developer of voluntary International Standards
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 Assigned Numbers Authority (IANA)	Responsible for the global coordination of the DNS root, IP addressing and other Internet protocol resources
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 and 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)	A protocol 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. The 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 of Things (IoT)	A collection of sensors, actuators and computing capabilities that work together to solve a problem or provide a service over the Internet
Internet Protocol (IP)	Specifies the format of packets and the addressing scheme

TERM	DEFINITION
Internet Protocol (IP) packet spoofing (IP)	An attack using packets with spoofed source Internet packet (IP) addresses *Scope Notes:* This technique exploits applications that use authentication based on IP addresses. This technique may enable an unauthorized user to gain root access to the target system.
Internet proxy system	A server that acts as a gateway between an individual and the internet
Internet service provider (ISP)	A third party that provides individuals and enterprises access to the Internet and a variety of other Internet-related services
Internetwork Packet Exchange/Sequenced Packet Exchange (IPX)	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.
Interoperability	The ability to exchange, access and make use of information across different systems and/or networks without the need for intermediaries and the capacity to transfer an asset between two or more networks or systems without changing the state of the asset
Interpret	To translate and execute each statement or construct of a computer program before translating and executing the next. Contrasts with assemble and compile.
Interpretability	In artificial intelligence (AI), interpretability allows humans to understand the internal mechanisms and reasoning behind a model's decisions, moving beyond simply observing the outputs to provide transparency into the underlying logic and relationships that produced the results
Interpreter	A computer program that translates and executes each statement or construct of a computer program before translating and executing the next. The interpreter must be a resident in the computer each time a program [source code file] written in an interpreted language is executed. Contrasts with assembler and compiler.
Interrogation	Used to obtain prior indicators or relationships from extracted data, including telephone numbers, IP addresses and names of individuals
Interrupt	A hardware or software signal stemming from an event that requires immediate attention
Interruption window	The time that the company can wait from the point of failure to the restoration of the minimum critical services or applications. After this time, the progressive losses caused by the interruption are excessive for the enterprise.
Interview	A meeting (virtual or face-to-face) that includes an interactive discussion between appraisal team members and those who have a process role, e.g., implementing, using, or following the processes, within the organizational unit or project
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
Intruder	An individual or group that gains access to the network and its resources without permission
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)	A system that inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack
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 prevent the intended victim hosts from being affected by the attacks

TERM	DEFINITION
Intrusive monitoring	In vulnerability analysis, the process of gaining information by performing checks that affect the normal operation of a system or by crashing the system
Invalid inputs	**1.** Test data that lie outside the domain of the function the program represents **2.** Not only inputs outside the valid range for data to be input, i.e., when the specified input range is 50 to 100, but also unexpected inputs, especially when these unexpected inputs may easily occur, e.g., the entry of alpha characters or special keyboard characters when only numeric data is valid or the input of abnormal command sequences to a program
Investigation	The collection and analysis of evidence with the goal to identify the perpetrator of an attack or unauthorized use or access
Investment (or expense) risk	The risk that I&T investment fails to provide value commensurate with its cost or is otherwise excessive or wasteful, including the overall I&T investment portfolio
Investment portfolio	The collection of investments being considered and/or made *Scope Notes:* COBIT 5 perspective
IP address	A unique binary number used to identify devices on a TCP/IP network. May be IP version 4 or 6.
IP Authentication Header (AH)	Protocol used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays (RFC 4302) *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 it uses for authentication. To ensure replay protection, AH uses a sequence number field within the IP authentication header.
IP Security (IPSec)	A set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets
Irregularity	Violation of an established management policy or regulatory requirement. It may consist of deliberate misstatements or omissions of information concerning the area under audit or the enterprise as a whole, gross negligence or unintentional illegal acts.
ISO	International Organization for Standardization
ISO 9001:2000	The 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 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	A standard for 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 application	Electronic functionality that constitutes parts of business processes undertaken by, or with the assistance of, IT *Scope Notes:* COBIT 5 perspective
IT architecture	A 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

TERM	DEFINITION
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. Note: This was renamed "alignment goal" in COBIT 2019. *Scope Notes:* COBIT 5 perspective
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. See also "governance framework." *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 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 integrate 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 continuously monitoring 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 and disposition.
IT risk scenario	The description of an IT-related event that can lead to a business impact
IT service	The day-to-day provision to customers of information and technology infrastructure and applications and support for their use—e.g., service desk, equipment supply and moves, and security authorizations *Scope Notes:* COBIT 2019 perspective
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

TERM	DEFINITION
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 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
IT-related incident	An IT-related event that causes an operational, developmental and/or strategic business impact
ITIL (IT Infrastructure Library) (ITIL)	The UK Office of Government Commerce (OGC) IT Infrastructure Library, which is a set of guides on the management and provision of operational IT services
JavaScript	A scripting language originally designed in the mid-1990s for embedding logic in web pages, but which later evolved into a more general-purpose development language. JavaScript continues to be very popular for embedding logic in web pages.
Job	A user-defined unit of work to be accomplished by a computer. For example: the compilation, loading and execution of a computer program See Job control language.
Job control language (JCL)	Used to control run routines in connection with performing tasks on a computer
Joint PII controller	A PII controller that determines the purposes and means of the processing of PII with one or more other PII controllers
Journal entry	A debit or credit to a general ledger account See 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
K-means clustering	A data-mining algorithm to cluster, classify or group N objects based on their attributes or features into K number of groups (so-called clusters)
K-nearest neighbors	A machine-learning algorithm that classifies things based on their similarity to nearby neighbors. The algorithm execution is refined by picking how many neighbors to examine (k) and some notion of distance to indicate how near the neighbors are.
KB	Kilobyte
Keras	A popular Python machine-learning API
Kernel	Primary (of three) component of an operating system
Kernel mode	Used for execution of privileged instructions for the internal operation of the operating system. In kernel mode, there are no protections from errors or malicious activity, and all parts of the system and memory are accessible.
Key control indicator (KCI)	A measure of the effectiveness of controls to indicate a failure or weakness which may result in the increased likelihood or impact of risk events
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

TERM	DEFINITION
Key length	The size of an encryption key measured in bits
Key management	The generation, exchange, storage, use, destruction and replacement of keys in a cryptosystem
Key management practice	A management practice that is required to successfully execute business processes
Key performance indicator (KPI)	A type of performance measurement
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.
Keylogger	Software used to record all keystrokes on a computer
Keypoints	The coordinates of particular features in an image
Kilobyte (KB)	Approximately one thousand bytes. This term is used to describe the size of computer memory or disk storage space. Because computers use a binary number system, a kilobyte is precisely 2^{10} or 1024 bytes.
Knowledge engineering	The process of capturing, representing, and utilizing human knowledge within computer systems to help artificial intelligence (AI) models reason, solve problems, and make informed decisions, often in specific domains
Knowledge portal	A repository of core information and knowledge for an extended enterprise *Scope Notes:* Generally a web-based implementation containing a core repository of information provided for the extended enterprise to resolve any issues
Label	In supervised learning, the answer or result portion of an example
Lag indicator	A metric for the achievement of a goal; an indicator relating to the outcome or result of an enabler *Scope Notes:* This indicator is available only after the fact or event.
Lag risk indicator	A backward-looking metric that indicates risk has been realized after an event has occurred
Language model	A statistical model that analyzes text to understand the probabilities of words appearing together, enabling tasks like predicting the next word, generating text, translating languages, and summarizing information
Large language model (LLM)	A language model trained on massive amounts of text data to generate human-like text, analyze information, translate languages, and output code, among other types of content
Latency	The time it takes a system or network 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 destination.
Latent variable	A variable that is not directly observed, but rather inferred (through a mathematical model) from other variables that are observed (directly measured)
Layer 2 switches	Data link layer devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks
Layer 2 tokens	A secondary coding on top of the original blockchain coding structure that allows for the evolution of a decentralized blockchain to address limitations, i.e., scaling and smart contracts
Layer 3 and 4 switches	Switches with operating capabilities at layer 3 and layer 4 of the open systems interconnect (OSI) model. These switches examine 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.

TERM	DEFINITION
Layer 4–7 switches	Used for load balancing among groups of servers *Scope Notes:* Also known as content switches, content services switches, web switches or application switches
Lead indicator	A metric for the application of good practices; an indicator relating to the functioning of an enabler *Scope Notes:* This indicator will provide an indication of the possible outcome of the enabler.
Lead risk indicator	A forward-looking metric that provides an early warning that risk may soon be realized before an event has occurred
Leadership	The ability and process to translate organizational vision into desired behaviors that are followed at all levels of the extended enterprise
Lean	A business methodology for optimizing efficiency in a process and minimizing economic waste
Learning rate	In machine learning (ML), a hyperparameter that defines the update size for model weights during training, controlling the speed and direction of optimization
Leased line	A communication line permanently assigned to connect two points, as opposed to a dial-up line that is available and open only when a connection is made by dialing the target machine or network. Also known as a dedicated line.
Legacy system	An outdated computer system
Legitimate interest	The basis for lawful processing of data
Level of assurance	The degree to which the subject matter has been examined or reviewed
Librarian	The individual responsible for the safeguarding 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)
Life cycle methodology	The use of any one of several structured methods to plan, design, implement, test and operate a system from its conception to the termination of its use See Waterfall model.
Life cycle model	A representation or description of the steps and activities for the development and updating of a solution communicated to stakeholders and followed by a project or organization. This description may include: • Phases • Sequences • Interrelationships • Inputs • Outputs • Decision points • Roles and responsibilities
Lift	Compares the frequency of an observed pattern with how often one expects to see that pattern just by chance
Likelihood	The probability of something happening
Limit check	A test that measures 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.

TERM	DEFINITION
Linear algebra	A branch of mathematics dealing with vector spaces and operations on them, such as addition and multiplication. It is designed to represent systems of linear equations.
Linear regression	A mathematical technique to look for a linear relationship when starting with a set of data points that do not necessarily line up nicely. A linear relationship is one in which the relationship between two varying amounts, such as price and sales, can be expressed with an equation that can be represented as a straight line on a graph.
Link editor (linkage editor)	A utility program that combines several separately compiled modules into one, resolving internal references between them
Linux	Linux is a Unix-like, open-source and community-developed operating system (OS) for computers, servers, mainframes, mobile devices and embedded devices. https://www.techtarget.com/searchdatacenter/definition/Linux-operating-system
Listening nodes	A publicly visible blockchain network device whose main function is to communicate and share data or information with any other node that connects with it
Litecoin	A peer-to-peer cryptocurrency and open-source software project
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)	A communication network that serves several users within a specified limited geographic area
Lock	A mechanism for keeping something secure or restricting access to functionality or data
Log	**1.** To record details of information or events in an organized record-keeping system, usually sequenced in the order in which they occurred **2.** An electronic record of activity (e.g., authentication, authorization and accounting)
Log analyzer	A tool used to track and analyze logs
Logical access	The ability to interact with computer resources granted using identification, authentication and authorization
Logical access controls	The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files
Logistic regression	A model similar to linear regression but where the potential results are a specific set of categories, instead of being continuous
Logoff	The act of disconnecting from a a network or system
Logon	The act of connecting to a network or system, which typically requires entry of a user ID and password
Logs/log file	Files created specifically to record various actions occurring on a system being monitored, such as failed login attempts, full disk drives and email delivery failures
LoRa/LoRaWAN	A proprietary member of the family of low-power wide area network (LPWAN) protocols designed for low-bandwidth, battery-powered devices requiring extended range
Loss event	Any event during which a threat event results in loss *Scope Notes:* From Jones, J.; "FAIR Taxonomy," Risk Management Insight, USA, 2008
Low-level language	See Assembly language. A programming language, wuch as assembly language or machine code, that provides little or no abstraction from a computer's instruction set architecture, i.e., in which commands or functions are structurally similar to the processor's instructions

TERM	DEFINITION
LTE for Machine-Type Communications (LTE-M)	A low-power wide area network (LPWAN) standard from the 3GPP, based on typical Long Term Evolution (LTE)
MAC header	The hardware address of a network interface controller (NIC) inside a data packet
Machine code	Computer instructions and definitions expressed in a form (binary code) that can be recognized by the CPU of a computer. All source code, regardless of programming language, is eventually converted to machine code.
Machine language	The logical language a computer understands
Machine learning (ML)	A program or system that builds (i.e., trains) a predictive model from input data
Machine learning model	The model artifact created by the machine learning training process. The process of training a machine learning model involves providing a machine learning model algorithm (that is, the learning algorithm) with training data.
Machine learning overfitting (ML overfitting)	A complex machine learning model that tends to "memorize" noise in a large data set while failing to capture the overall trend
Machine learning underfitting (ML underfitting)	A machine learning model that is too simple to model complex data
Machine translation	The systematic translation of text from one language to another using statistical or neural network models to analyze the source language and generate the most likely equivalent text in the target language
Magnetic card reader	A hardware device used to read cards with a magnetic surface on which data can be stored and retrieved
Magnetic ink character recognition (MICR)	A technology 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 (email) server that relays messages so that neither the sender or recipient is a local user
Main establishment	The place of central administration for a controller with establishments in more than one country
Main memory	A nonmoving storage device that uses one of a number of types of electronic circuitry to store information
Main program	A software component that is called by the operating system of a computer and that usually calls other software components See Routine and Subprogram.
Mainframe	A large high-speed computer, especially one supporting numerous workstations or peripherals
Maintainability	The ease with which a software system or component can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment; synonymous with modifiability

TERM	DEFINITION
Maintenance	Quality assurance (QA) activities, such as adjusting, cleaning, modifying and overhauling equipment to assure performance in accordance with requirements. Maintenance of a software system includes correcting software errors, adapting software to a new environment and making enhancements to software. See Adaptive maintenance, Corrective maintenance and Perfective maintenance.
Malicious software	See Malware.
Malignant threat	Malignant threats are threats that are unintentional. There is no motive, good or bad, for causing the losses associated with malignant threats
Malware	Malicious software designed to infiltrate or damage a computer system or obtain information from it without the owner's consent. Examples of malware include computer viruses, worms, Trojan horses, spyware and adware.
Malware analysis tools	Tools used to analyze malware
Man-in-the-middle attack (MitM)	A strategy in which the attacker intercepts the communication stream between two components of the target system and then replaces the traffic with the intruder's own, eventually assuming control of the communication
Managed discovery	A phased objective evidence collection approach beginning with an initial call by the appraisal team for a predetermined set of artifacts, followed by a set of iterative calls based on the appraisal team's evaluation of those artifacts and remaining evidence gaps See Discovery-based appraisal and Verification-based appraisal.
Managed process	A performed process that is recorded, followed, updated and made persistent and habitual for consistency. A managed process is necessary at the practice group level 2 in the CMMI Practice Areas. See Performed process.
Management	The planning, building, running and monitoring of activities in alignment with the direction set by the governance body to achieve the enterprise objectives
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)	Logical access control filters used to validate access credentials that cannot be controlled or modified by normal users or data owners
Mapping	Diagramming data that are to be exchanged electronically, including specifications on how they are to be used and what business management systems need them See Application tracing and Mapping. *Scope Notes:* Mapping is a preliminary step for developing an applications link.
Market risk	Pressures on an asset class
Markov Chain	An algorithm for working with a series of events (for example, a system being in particular states) to predict the possibility of a certain event based on which other events have occurred and to identify probabilistic relationships between the different events
Markov decision process (MDP)	A graph representing the decision-making model wherein which decisions (or actions) are taken to navigate a sequence of states, under the assumption that the Markov property holds. In reinforcement learning, these transitions between states return a numerical reward.
Masking	A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report

TERM	DEFINITION
Masqueraders	Attackers that penetrate systems by using the identities and logon credentials of legitimate users
Master file	A file of semi-permanent information that is used frequently for processing data or for more than one purpose
Masternode	A blockchain network device that can process all the functions of a full node or miner and is also able to facilitate other processes
Material misstatement	An untrue statement, whether accidental or intentional, that affects the results of an audit to a measurable extent
Material weakness	A deficiency or a combination of deficiencies in internal control resulting in a reasonable possibility that a material misstatement will not be prevented or detected in a timely way. 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, are not in use or are inadequate • Escalation is warranted • There is an inverse relationship between materiality and the level of audit risk acceptable to the information security (IS) audit or assurance professional—that is, the higher the materiality level, the lower the acceptability of the audit risk and vice versa
Materiality	An auditing concept that considers the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. Materiality is also an expression of the relative significance or importance of a particular matter in the context of the enterprise as a whole.
MATLAB	A commercial computer language and environment popular for visualization and algorithm development
Matrix	A set of numbers or terms arranged in rows and columns between parentheses or double lines. For purposes of manipulating a matrix with software, think of it as a two-dimensional array. As with its one-dimensional equivalent, a vector, this mathematical representation of the two-dimensional array makes it easier to take advantage of software libraries that apply advanced mathematical operations to the data—including libraries that can distribute the processing across multiple processors for scalability.
Maturity	The degree of reliability or dependency a business can place on a process to achieve desired goals or objectives
Maturity level	A rating that describes the degree to which organizational unit processes meet the intentions and values articulated in a predefined set of practice areas. The rating is based on the achievement of a specified set of practice group levels within the predefined set of practice areas.
Maturity model	*Scope Notes:* See Capability Maturity Model (CMM).
Maximum tolerable outage (MTO)	Maximum time an enterprise can support processing in alternate mode
MB	Megabyte
Mean	The average value, also known as arithmetic mean
Mean absolute error	The average error of all predicted values when compared with observed values
Mean squared error	The average of the squares of all the errors found when comparing predicted values with observed values

TERM	DEFINITION
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 they can also address qualitative information such as customer satisfaction. Reporting and monitoring measures help an enterprise gauge progress toward effective implementation of strategy.
Measure (IEEE)	A quantitative assessment of the degree to which a software product or process possesses a given attribute
Measurement and performance objectives	Statements that describe quantitative or qualitative objectives without requiring the additional rigor of statistical or quantitative analysis
Measurement-based	A type of numerical data obtained by performing measurements but not based on statistical and quantitative management
Media access control (MAC)	Lower sublayer of the OSI Model Data Link layer
Media access control (MAC) address (MAC)	A 48-bit unique identifier assigned to network interfaces for communications on the physical network segment
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.
Median	The value in the middle of a sorted list of values or, if the number of values is even, the average of the two in the middle
Meet the intent and value	See Intent and value
Megabit	Approximately 1 million bits. Precisely 1024 K bits, 2^{20} bits or 1,048,576 bits.
Megabyte	Approximately 1 million bytes. Precisely 1024 K Bytes, 2^{20} bytes or 1,048,576 bytes See Kilobyte.
Memorandum of agreement	A record of expectations and arrangements between two or more parties; also known as a “memorandum of understanding” See Statement of Work.
Memory	Any device or recording medium that can hold and store binary data, and from which the entire original data set can be retrieved. Two types of memory are main, e.g., ROM and RAM, and auxiliary, e.g., tape and disk. See Storage device.
Memory dump	Raw data copied from one place to another with little or no formatting for readability *Scope Notes:* Usually, dump refers to data copied from the main memory to a display screen or a printer. Dumps are useful for diagnosing bugs. After a program fails, it is possible to study a 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).
Memory inspection tools	Tools used to detect memory leaks, memory accesses and a variety of memory misuses

TERM	DEFINITION
Merkle tree	A data structure 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 (logarithmic) verification of the integrity of all nodes on the tree.
Mesh topology	A fault-tolerant topology in which network nodes and endpoints are mostly, if not fully, interconnected
Message authentication code (MAC)	An American National Standards Institute (ANSI) standard checksum that is computed using Data Encryption Standard (DES).
Message digest	The result of a cryptographic hash function taking an input of an arbitrary length and producing an output that is a standard-sized binary string. The output is unique to the input and 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 outputs). A collision, while possible, is statistically improbable. Cryptographic hash functions are developed so that the input cannot be determined readily from the output. See Hash.
Message digest algorithm	A one-way function that serves as a way for a recipient to verify data integrity and sender identity. Common message digest algorithms are MD5, SHA256 and SHA512.
Message Queue Telemetry Transport (MQTT)	An ultra-lightweight communication protocol widely used in the Internet of Things
Message switching	A telecommunications methodology that controls traffic by sending a complete message to a concentration point where it is stored until the communications path is established
Meta-learning	A process that involves training models across varied tasks to acquire generalizable strategies, enabling them to adapt and learn efficiently on new, often data-scarce tasks
Metering	The monitoring and tracking of resource usage within a cloud environment, e.g., data, memory and storage
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), the procedure to carry out the measurement and the procedure to interpret the assessment.
Metric, software quality	A quantitative measure of the degree to which software possesses a given attribute that affects its quality
Metropolitan area network (MAN)	A data network intended to serve an area the size of a large city
Microcontroller	Special processing unit useful in embedded systems, such as fleet vehicles and process control applications
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 programming 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.

TERM	DEFINITION
Milestone	A terminal element that marks the completion of a work package or phase *Scope Notes:* A milestone is 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.
Mini-team	A subset of the appraisal team members with primary responsibility for collecting sufficient appraisal data and objective evidence to ensure coverage of assigned model practice areas or sampled projects and organizational support functions; may also perform other tasks, e.g., project-level characterizations
Miniature fragment attack	An attack method that involves fragmenting the IP packet into smaller ones before pushing it through the firewall, in the hope that only the first in the sequence of fragmented packets will be examined and the others will pass without review
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 day-to-day business operations.
Misuse detection	Detection based on whether a system activity matches an activity defined as "bad"
Mnemonic	A symbol chosen to assist human memory and understanding, e.g., an abbreviation such as "MPY" for multiply
Mobile computing	A technology that extends wireless computing to small devices that run specifically designed applications and is capable of expanding an enterprise network to reach remote places under circumstances that would not permit connectivity by other means *Scope Notes:* Mobile computing is comprised of smartphones, tablets and wearable devices
Mobile device	portable electronic equipment that can connect to the Internet
Mobile site	A mobile/temporary facility that serves as a business resumption location. The facility is typically delivered to an alternative site and can house information technology and staff.
Mode	The value that occurs most often in a sample of data. Like the median, the mode cannot be directly calculated.
Model	**1.** A method to describe a given set of components and how those components relate to each other to describe the main workings of an object, system, or concept **2.** In machine learning (ML), the outcome of a training process. A trained model can automatically process data that was not used for its training to perform a specific set of tasks.
Model component	Any of the five main architectural elements or parts that compose the CMMI model. These include the view, practice area, practice group, practice and informative material. See Informative material, Practice, Practice area, Practice group and View.
Model scope	The practice areas or model components to be appraised, defined in benchmark model views predefined by ISACA or customized for the organization’s needs. See Appraisal scope and Organizational unit.
Modeling	Constructing programs that model the effects of a postulated environment to investigate the dimensions of a problem and observe the effects of algorithmic processes on responsive targets

TERM	DEFINITION
MODEM (modulator/ demodulator)	A device that connects a terminal or computer to a communications network via a telephone line. A modem turns digital pulses from a computer into frequencies within the audio range of a telephone system. When acting in the receiver capacity, a modem decodes incoming frequencies.
Modular software	Software composed of discrete parts
Modularity	The degree to which a system or computer program is composed of discrete components so that a change to one component has minimal impact on other components
Modulation	The process of converting a digital computer signal into an analog telecommunications signal
Module	**1.** In programming languages, a self-contained subdivision of a program that may be separately compiled **2.** A discrete set of instructions, usually processed as a unit by an assembler, a compiler, a linkage editor, or a similar routine or subroutine **3.** A packaged functional hardware unit suitable for use with other components See Unit.
Monetary unit sampling	A sampling technique that estimates the amount of overstatement in an account balance
Monitoring policy	A set of rules outlining or delineating the way information about the use of computers, networks, applications and information is captured and interpreted
Monte Carlo method	The use of randomly generated numbers as part of an algorithm
Moving average	The mean (or average) of time series data (observations equally spaced in time, such as per hour or per day) from several consecutive periods
Multifactor authentication (MFA)	A combination of more than one authentication method, such as token and password (or personal identification number [PIN]) or token and biometric device
Multiplexor	A device used for combining several lower-speed channels into a higher-speed channel
Multiprocessing	A mode of operation in which two or more processes (programs) are executed concurrently (simultaneously) by separate CPUs that have access to a common main memory. Contrasts with multiprogramming. See Multitasking and Time sharing.
Must	A word used in a statement of a method requirement to indicate that it is not tailorable. “Must” may be used interchangeably with “shall.” See Shall.
Mutex	A lock set by a smart contract code before access is permitted to a shared resource or function, and released after its use, to prevent multiple threads from simultaneously gaining access to the locked region of the code
Mutual authentication	A form of authentication in which a device sends a certificate to a server and, in return, is sent authentication of the server
Mutual takeover	A failover process that is basically a two-way idle standby. Two servers are configured so that each can take over the other's node resource group. Both must have enough central processing unit (CPU) power to run both servers' applications with sufficient speed, or expected performance losses must be taken into account until the failed node reintegrates.
N-gram	The analysis of sequences of "n" items (typically, words in natural language) to look for patterns. The value of "n" can be anything. An n-gram is used to construct statistical models of documents (e.g., when automatically classifying them) and to find positive or negative terms associated with a product name.

TERM	DEFINITION
Naive Bayes classifier	A collection of classification algorithms based on Bayes' Theorem. It is a family of algorithms that share a common principle that every feature being classified is independent of the value of any other feature.
NaN trap	The result of one number in a model becoming a NaN during training, causing many or all other numbers in the model to eventually become a NaN. "NaN" is an abbreviation for "Not a Number."
Narrowband IoT (NB-IoT)	A low-power wide area network (LPWAN) standard developed by the 3rd Generation Project Partnership (3GPP) for indoor devices requiring low cost, low battery usage and high density Source: 3rd Generation Partnership
National Institute for Standards and Technology (NIST)	A US government agency that develops tests, test methods, reference data, proof-of concept implementations and technical analyses to advance the development and productive use of information technology *Scope Notes:* NIST creates mandatory standards that are followed by federal agencies and those doing business with them.
Native tokens	**1.** Created at the genesis block and usually used to reward the successful processing of a transaction or the creation of a blockchain **2.** Unit of account for a blockchain
Natural bounds	The inherent range of variation in a process, as determined by process performance measures. Natural bounds are sometimes referred to as “control limits” or the “voice of the process.”
Natural language processing (NLP)	Enables computers to analyze and manipulate human language using various techniques, such as text analysis, sentiment analysis, machine translation, and speech recognition, to complete tasks like summarizing information, generating human-like text, and translating languages
Need-to-know	Principled approach to controlling what individuals can see. Employees can access only the data, systems and spaces necessary to do their job.
Net present value (NPV)	Calculation based on the after-tax discount rate of an investment and a series of expected incremental cash outflows (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 classified as net profit
Net-centric technologies	Information and objects (software and data) managed or stored on a network, whose contents and security are of prime importance compared to the contents and security of software and data in traditional computer processing, which emphasizes hardware location *Scope Notes:* An example of net-centric technologies is the Internet, where the network is its primary concern.
NetBIOS	A program that allows applications on different computers to communicate within a local area network (LAN)
Netcat	A simple UNIX utility that reads and writes data across network connections using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). Netcat is designed to be a reliable back-end tool that can be used directly or easily driven by other programs and scripts. It is also a feature-rich network debugging and exploration tool, because it can create almost any kind of connection needed. Netcat is part of the Red Hat Power Tools collection and comes standard on SuSE Linux, Debian Linux, NetBSD and OpenBSD distributions.
Network	A system of interconnected computers and the communication equipment used to connect them

TERM	DEFINITION
Network access control systems	Systems that assist in controlling devices and user access to networks
Network address	An identifier for a node or host on a telecommunications network
Network address translation (NAT)	A methodology for 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 administrator	An individual who is 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 analyzer	A tool that creates a signal and characterizes the devices that receive it to help diagnose problems with Internet connectivity, WiFi network setups and issues on remote servers
Network basic input/ output system	See NetBIOS.
Network hop	A strategy in which an attacker whose identity is obscured successively hacks into a series of connected systems
Network interface card (NIC)	A card designed for insertion into a computer to enable it to communicate with other computers on a network *Scope Notes:* Most NICs are designed for a particular type of network or protocol.
Network interoperability	The ability of networks comprised of different topologies, configurations and functionalities to transmit data to and from one another
Network News Transfer Protocol (NNTP)	A protocol that uses a reliable stream-based mechanism for the distribution, inquiry, retrieval and posting of netnews articles. For news-reading clients, NNTP enables retrieval of news articles stored in a central database, enabling subscribers to select only the articles they wish to read. (RFC 3977)
Network segmentation	A common network security implementation technique that segments an enterprise network into zones that can be separately controlled, monitored and protected
Network topology	The basic configuration and architecture of a set of interconnected nodes
Network traffic analysis	A means of identifying patterns in network communications *Scope Notes:* Traffic analysis does not need to have the actual content of the communication but analyzes where traffic occurs, when and for how long communications take place, and the quantity of information transferred.
Network-attached storage (NAS)	An architecture that uses dedicated storage devices to centralize data storage *Scope Notes:* NA storage devices generally do not provide traditional file/print or application services.
Neural network	Networks, inspired by the structure of the human brain, that learn by processing data through three layers (input, hidden, and output). They can be trained to match any input to various outputs, including binary ones, making them versatile tools in deep learning (DL) for tasks like image recognition.
Neuron	A neural network node that typically takes in multiple input values and generates one output value
Nibble	An equivalent of four binary digits or half a byte. Nibble can be represented by one hexadecimal digit.
Node	Point at which terminals are given access to a network

TERM	DEFINITION
Node (neural network)	A neuron in a hidden layer
Noise	Data transmission or data set disturbances, such as static, that cause messages to be misinterpreted by the receiver
Non-model findings	Findings that are not directly traceable to model practices but that may be useful to an organization's business, performance or improvement goals. Non-model findings cannot be used to determine ratings, but they may identify other areas that the team must consider in order to characterize practices.
Nonce	A limited or single-use value, typically small, used for initialization, seed generation or some other special purpose
Nondisclosure agreement (NDA)	A legal contract between at least two parties that outlines confidential materials the parties wish to share with one another for certain purposes but wish to restrict from generalized use; a contract through which the parties agree not to disclose information covered by the agreement *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 must 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	A 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, verifiable by a third party *Scope Notes:* A digital signature can provide nonrepudiation.
Nonstatistical sampling	Method of selecting a portion of a population, based in professional judgment and experience, for the purpose of quickly confirming a proposition. This method does not allow drawing mathematical conclusions regarding the entire population.
Normal distribution	A probability distribution that, when graphed, is a symmetrical bell curve with the mean value at the center. The standard deviation value affects the height and width of the graph. Also known as "Gaussian distribution."
Normalization	**1.** The elimination of redundant data **2.** The process of converting an actual range of values into a standard range of values, typically -1 to +1 or 0 to 1
NoSQL	A database management system that uses any of several alternatives to the relational, table-oriented model used by SQL databases
Null	A value whose definition is to be supplied within the context of a specific operating system. This value is a representation of the set of no numbers or no value for the operating system in use.

TERM	DEFINITION
Null data	Data for which space is allocated but for which no value currently exists
Null hypothesis	If the proposed model for a data set indicates that the value of "x" affects the value of "y," then the null hypothesis—i.e., the model compared against the proposed model to check whether "x" really is affecting "y"—will find that the observations are all based on chance and that there is no effect. The smaller the P-value computed from the sample data, the stronger the evidence is against the null hypothesis.
Null string	A string containing no entries. Note that a null string has a length of zero.
Numeric check	An edit check designed to ensure that the data element in a particular field is numeric
Obfuscation	The deliberate act of creating source or machine code that is difficult for humans to understand
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:* 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 are usually 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.
Object oriented design	A software development technique in which a system or component is expressed in terms of objects and connections between those objects
Object oriented language	A programming language that allows the user to express a program in terms of objects and messages between those objects. Examples include C++, Smalltalk and LOGO.
Object oriented programming	A technology for writing programs that are made up of self-sufficient modules containing all the information needed to manipulate a given data structure. The modules are created in class hierarchies so that the code or methods of a class can be passed to other modules. New object modules can be easily created by inheriting the characteristics of existing classes. See Object and Object-oriented design
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 a software design centered around designing the objects that will make up a program. Any object-oriented program is composed of objects or software parts.
Objective	A statement of a desired outcome
Objective evidence (OE)	Artifacts or affirmations used as indicators of the implementation or habit and persistence of processes to meet the intent and value of one or more model practices See Artifact and Affirmation

TERM	DEFINITION
Objective function	A function that combines decision variables, constraints and the goal value to solve an optimization problem. The objective is the goal to maximize or minimize; the objective function is used to find the optimum result.
Objective in 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, audit function or member of the audit team's integrity, objectivity or professional skepticism has been compromised
Objective of mind	The state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism
Objectively evaluate	To review activities and work products against criteria that minimize subjectivity and bias by the reviewer
Objectivity	The ability to exercise judgment, express opinions and present recommendations with impartiality
Observation	The receipt of messages through electronic, sensory or vibrational signals and the human senses
Observer	An individual assigned by ISACA to evaluate, audit or review an appraisal team leader candidate See Auditor
Octal	The base-8 number system. Digits are 0, 1, 2, 3, 4, 5, 6 and 7.
Offchain	Any blockchain actions that require data outside of the blockchain network
Offline files	Computer file storage media that are not physically connected to a computer. Typical examples include tapes or tape cartridges used for backup purposes.
Offline inference	The process of generating a group of predictions, storing those predictions and then retrieving those predictions on demand
Offsite storage	A facility located away from the building that houses the primary information processing facility (IPF) used for storage of computer media, such as offline backup data and storage files
On-demand self-service	The ability for a customer to self-assign and allocate cloud resources instantaneously without vendor interaction
Onchain	Cryptoasset or token transactions which occur on and within the data records of a blockchain and are perpetually dependent on the state of that blockchain for their validity
One-shot learning	A machine-learning approach often used for object classification that is designed to learn effective classifiers from a single training example
Online Certificate Status Protocol (OCSP)	A protocol used for receiving the status of an X.509 certificate
Online data processing	A type of data processing that involves entering information into a computer via a video display terminal *Scope Notes:* With online data processing, the computer immediately accepts or rejects the information as it is entered.
OOP	The acronym for object-oriented programming
Open Source Security Testing Methodology	An open and freely available methodology and manual for security testing

TERM	DEFINITION
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.
Open Systems Interconnect (OSI) model (OSI)	A seven-layer conceptual model that describes functions of computer network or telecommunication systems
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
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 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 and printer) and the application software (word processor, spreadsheet email) which also controls access to the devices, 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
Operation and maintenance phase	The period of time in the software life cycle during which a software product is employed in its operational environment, monitored for satisfactory performance, and modified as necessary to correct problems or to respond to changing requirements
Operational audit	An audit designed to evaluate the various internal controls, economy and efficiency of a function or department
Operational concept	A general description of the way in which a component or solution is used or operates. An operational concept may also be referred to as a "concept of operations."
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 supports the IT organization in its delivery of services
Operational risk	The potential for losses caused by inadequate systems or controls, human error or mismanagement, and natural disasters
Operational scenario	A description of a potential sequence of events that includes the interaction of a component or solution with its environment and users, and with other solution components. Operational scenarios are used to evaluate the requirements and design of the system and to verify and validate the system.
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.
Opportunity	An uncertain event that may positively impact meeting objectives
Opt-in	A declaration or an active motion in which a data subject agrees to particular data processing. Process or type of policy whereby the personally identifiable information (PII) principal is required to take an action to express explicit, prior consent for their PII to be processed for a particular purpose.

TERM	DEFINITION
Opt-out	A choice that is made on behalf of a data subject, indicating the subject's desire to no longer receive unsolicited information
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
Optimizing process	A quantitatively managed process that is continually improved to increase its capability. These continuous improvements can be made through both incremental and innovative improvements. An optimizing process is necessary at the practice group level 5 in the CMMI Practice Areas. See Quantitatively managed process and Defined process.
Or	In the CMMI model, means either "and" or "or"
Oracle	A relational-database programming system that incorporates the SQL programming language. It is a registered trademark of the Oracle Corp.
Oracle problem	A paradoxical situation where the oracle can become the central point of failure for the smart contract due to decreased security and centralization
Organisation for Economic Co-operation and Development (OECD)	An international organization helping governments tackle the economic, social and governance challenges of the global economy *Scope Notes:* The OECD groups 30 member countries in a unique forum to discuss, develop and refine economic and social policies.
Organization	The manner in which an enterprise is structured. It can also mean the entity.
Organizational directives	Expectations established by senior management that are adopted by an organization to influence and determine decisions. This may also be referred to as "organizational policies."
Organizational structure	A component of a governance system. This includes the enterprise and its structures, hierarchies and dependencies. *Scope Notes:* Another example is a "steering committee." See COBIT 5 perspective
Organizational support function	A team or entity that provides products and/or services for a bounded set of activities needed by other portions of the organization. Examples of organizational support functions include quality assurance, configuration management, training and other process groups. Organizational support functions should be treated as projects in that there should be processes and process roles with plans, infrastructure and organizational boundaries that describe what they do and how they provide support to other projects within the organization.
Organizational unit (OU)	The part of an organization that is the subject of an appraisal and to which the appraisal results are generalized. An organizational unit deploys one or more processes that have a coherent process context and defined set of process roles and operate within a coherent set of business objectives. See Process role
Organizational unit coordinator (OUC)	An appraisal role, designated by the appraisal sponsor and appraisal team leader, that handles logistics and provides technical, administrative and logistical support, such as coordinating schedules, notifying participants, arranging facilities and resources, obtaining requested documentation and arranging catering
Organization's business objectives	A set of objectives developed by senior management to improve performance, build and improve capability and enhance profitability, market share and other factors that influence the organization's success

TERM	DEFINITION
Organization's measurement repository	A specific location or locations where measurement-based information is stored. The purpose is to collect and make measurement results available throughout the organization. This repository contains or references actual measurement results and related information needed to understand and analyze measurement results that are typically described as part of the organizational process assets. See Organization's process assets and Organization's set of standard processes
Organization's process asset library	A specific location or locations where information is stored to make process assets available that are useful to those who are defining, implementing, managing and following processes in the organization See Organization's process assets
Organization's process assets	Process-related documentation, records and information, such as an organization's policies, standard processes, tailoring guidelines, checklists, lessons learned, templates, standards, procedures, plans, training materials, etc. See Process description and Organization's process asset library
Organization's set of standard processes	A collection of process descriptions that guide consistent process implementation across an organization. These process descriptions cover the fundamental process elements and their relationships to each other, such as ordering and interfaces that should be incorporated into the defined processes implemented in work groups across the organization. A standard process is essential for long-term stability and improvement. See Process description and Process element
Organogram	A hierarchy diagram of an organizational structure
Orthogonal Frequency Division Multiple Access (OFDMA)	The OFDM multi-user variant that achieves multiple access by assigning subsets of subcarriers to different users, allowing simultaneous data transmission from several users
Other expert	An individual internal or external to an enterprise that could be an IT auditor from an external firm, a management consultant or an expert in the area of the engagement who has been appointment by top management or the team
Outcome	A result
Outcome measure	A measure that 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 characterizes historic performance. It is 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."
Outlier	Extreme values that might be errors in measurement and recording or accurate reports of rare events
Output analyzer	A tool that 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

TERM	DEFINITION
Over the air (OTA) updates (OTA)	An update to a device's firmware or software that is delivered via wireless communication
Overfitting	A model of training data that, by taking too many of the data quirks and outliers into account, is overly complicated and will not be as useful as it could be to find patterns in test data
Overflow	In a calculator, the state in which the calculator is unable to accept or process the number of digits in the entry or result Source: ISO See Arithmetic overflow
Overflow exception	An exception that occurs when the result of an arithmetic operation exceeds the size of the storage location that is designated to receive it Source: IEEE
Owner	An individual or group that holds or possesses the rights of and the responsibilities for an enterprise, entity or asset *Scope Notes:* Examples include process owners and system owners. See COBIT 5 perspective
P value	The probability, under the assumption of no effect or no difference (the null hypothesis), of obtaining a result equal to or more extreme than what was actually observed
Packet	Protocol data unit that is routed from source to destination in a packet-switched network *Scope Notes:* A packet contains both routing information and data.
Packet analyzers	A tool that captures packets as they travel a network to monitor, intercept and decode data
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
PageRank	An algorithm that determines the importance of something, typically to rank it in a list of search results. PageRank works by counting the number and quality of links to a page to determine a rough estimate of importance of the website. The underlying assumption is that more important websites are likely to receive more links from other websites.
PAN	Acronym for primary account number (also referred to as account number). A unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account
Pandas	A Python library for data manipulation that is popular with data scientists
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

TERM	DEFINITION
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
Parameter	**1.** A constant, variable, or expression that is used to pass values between software modules. Synonymous with argument. **2.** As it relates to neural networks, a variable that determines how a trained model produces a prediction and executes a task. The number of parameters can serve as an indication of the complexity of the model (e.g., a simple Naïve Bayes model can have tens of thousands of parameters, while state-of-the-art large language models [LLMs] have hundreds of billions of parameters).
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
Pascal	A high-level programming language designed to encourage structured programming practices
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	Fixes to software programming errors and vulnerabilities

TERM	DEFINITION
Patch management	**1.** An area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system to maintain up-to-date software and often to address security risk *Scope Notes:* Patch management tasks include 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 noncritical systems prior to installations. Patch management can be viewed as part of change management. **2.** The process to identify, acquire, install, and verify a set of changes to a computer program or its supporting data for solutions and systems. A patch is typically an isolated change of a specified scope and is sometimes referred to as a bug fix. (CMMI)
Patent	Protection of research and ideas that led to the development of a new, unique and useful product to prevent the unauthorized duplication of the patented item
Path	A sequence of instructions that may be performed in the execution of a computer program
Path analysis	Analysis of a computer program (i.e., source code) to identify all possible paths through the program, to detect incomplete paths or discover portions of the program that are not on any path
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.
Payload	A piece of malicious software that lets an attacker control a compromised computer system. The payload is typically attached to and delivered by an exploit.
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.
Peer reviews	The examination of work products performed by similarly skilled personnel during the development of work products to identify defects for removal. Peer reviews are sometimes called work product inspections. See Work product
Penetration testing	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers
Perceptron	Neural network that approximates a single neuron with n binary inputs. It computes a weighted sum of its inputs and fires if that weighted sum is zero or greater.
Performance	In IT, the actual implementation or achievement of a process

TERM	DEFINITION
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 parameters	Measurable criteria used to monitor progress toward quantitative objectives. Collectively, performance parameters provide a metric for determining the success of the business or project.
Performance testing	A test for comparing the system's performance to other equivalent systems using well-defined benchmarks
Performance work statement (PWS)	A statement of work (SOW) for performance-based acquisitions that clearly describes the performance objectives and standards expected of the contractor. When a contract is awarded, the PWS is a legally binding document for the contractor. See SOW
Performed process	A simple approach or set of steps that produces solutions or work products. A performed process is characteristic of Practice Group Level 1 in the CMMI Practice Areas.
Peripheral device	Equipment that is directly connected to a computer. A peripheral device can be used to input data, e.g., a keypad, bar code reader, transducer or laboratory test equipment or to output data, e.g., a printer, disk drive, video system, tape drive, valve controller or motor controller. It is synonymous with "peripheral equipment."
Peripherals	Auxiliary computer hardware equipment used for input, output and data storage *Scope Notes:* Examples of peripherals include disk drives and printers.
Perplexity	One measure of how well a model is accomplishing its task
Persistent and habitual	The routine way of doing business and following and improving a process that an organization follows as part of its culture
Personal computer (PC)	Synonymous with microcomputer, a computer that is functionally similar to large computers but serves only one user
Personal data	Information relating to an identified or identifiable natural person
Personal data breach	Any accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of a subject's data
Personal digital assistant (PDA)	Also called a "palmtop" or "pocket computer," a handheld device that has 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 *Scope Notes:* PINs have been adopted by financial institutions as the primary means of verifying customers in an electronic funds transfer (EFT) system.

TERM	DEFINITION
Personal information	A synonym for "personal data"
Personally identifiable information (PII)	Any information that can be used to establish a link between the information and the natural person to whom such information relates or that is or might be directly or indirectly linked to a natural person
Pervasive IS control	A 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	A type of electronic mail (email) attack that attempts to convince a user that the originator is genuine with the intention of obtaining information for use in social engineering *Scope Notes:* For example, phishing attacks may take the form of an attacker 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 can be used in another form of active attack.
Phreakers	Those who crack security, most frequently telephone and other communication networks
Piggybacking	**1.** The act of following an authorized person into a restricted access area **2.** The act of electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions
PII controller	A privacy stakeholder (or privacy stakeholders) who determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes
PII principal	The natural person to whom personally identifiable information (PII) relates
PII processor	The privacy stakeholder who processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller
PIN	See Personal identification number (PIN)
Pipeline	A set of structured practices, tools and flows that DevOps practitioners adopt throughout the development and operational life cycle
Pivot table	A tool that quickly summarizes long lists of data without requiring a single formula or copying a single cell. However, the most notable feature of pivot tables is that they can be arranged dynamically.
Plain old telephone service (POTS)	A wired telecommunications system
Plaintext	Digital information, such as cleartext, that is intelligible to the reader
Platform	The hardware and software that must be present and functioning for an application program to run (perform) as intended. A platform includes, but is not limited to, the operating system or executive software, communication software, microprocessor, network, input/output hardware, any generic software libraries, database management, user interface software, and the like.
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) (PMBOK)	A project management standard developed by the Project Management Institute (PMI)

TERM	DEFINITION
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 (POS)	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)
Poisson distribution	A distribution of independent events, usually over a period of time or space, used to help predict the probability of an event. Like the binomial distribution, this is a discrete distribution.
Policy	A document that communicates required and prohibited activities and behaviors
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.
Polynomial	Mathematical expression of more than two algebraic terms, especially the sum of several terms that contain different powers of the same variable(s)
Population	The entire set of data from which a sample is selected and about which an IT auditor wishes to draw conclusions
Port	A process or application-specific software element serving as a communication endpoint for the transport layer IP protocols (UDP and TCP)
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
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.
Practical Byzantine fault tolerance (pBFT)	Consensus mechanism in which all nodes are ordered in sequence with one node being primary node or leader, and all others referred to as backup nodes. All nodes in pBFT systems communicate with one another with the goal being that all honest nodes will come to an agreement of the state of the system using a majority rule. Nodes communicate for two reasons: to prove that messages came from a specific peer node and to confirm that messages were not modified during transmission. pBFT can be used for private and public blockchains and allows for instant transaction finality. However, such methodology requires a great number of messages between nodes, hence making a large blockchain network challenging.

TERM	DEFINITION
Practice	A practice consists of two parts: • Required practice information: Information required to understand the full intent and value of the practice, which includes the practice statement (intent), the value statement, and the additional required information • Explanatory practice information: Remaining parts of the practice, including additional explanatory PA/practice information, example activities and work products, which are important and useful to better understand the practice statement (intent), value statement, and additional required information
Practice area (PA)	A collection of similar practices that together achieve the defined intent, value, and required information described in that practice area
Practice area (PA) required information (PA)	The intent, value, and any additional required information for a practice area
Practice group	The organizing structure for practices within a practice area to aid understanding and adoption and provide a path for performance improvement
Predictive analytics	The analysis of data to predict future events, typically to aid in business planning. Predictive analytics incorporates predictive modeling and other techniques. Machine learning may be considered a set of algorithms to help implement predictive analytics.
Predictive modeling	The development of statistical models to predict future events
Preliminary design	**1.** The process of analyzing design alternatives and defining the architecture, components, interfaces and timing and sizing estimates for a system or component See Detailed design. **2.** The result of the process in definition 1
Preliminary findings	Draft strength and weakness statements developed by the appraisal team after evaluating objective evidence. Preliminary findings are validated with appraisal participants prior to the rating and final finding activities. See Appraisal final findings
Preprocessing	Procedures and techniques for cleaning, transforming, and formatting data to enhance its quality and suitability for analysis and modeling
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
Prime number	A natural number greater than 1 that can only be divided by 1 and itself
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.
PRINCE2 (Projects in a Controlled Environment) (PRINCE2)	Developed by the Office of Government Commerce (OGC), PRINCE2 is a project management method that covers the management, control and organization of a project
Principal component analysis	An algorithm that looks at the direction with the most variance and then determines that as the first principal component. This is very similar to how regression works in that it determines the best direction to map data.

TERM	DEFINITION
Principle	A component of a governance system. Principles translate desired behavior into practical guidance for day-to-day management.
Principle of least privilege (PoLP)	A principled approach of controlling what someone can do. This is an extension of need-to-know, whereby individuals are only granted the least amount of system access necessary to perform their jobs.
Principle of least privilege/access	Controls used to allow the least privilege access needed to complete a task
Printed circuit board (PCB)	The foundation of most electronic devices onto which the electrical components, including semiconductors, connectors, resistors, capacitors, memory chips and processors, are mounted and linked via conductive copper circuits
Prior distribution	In Bayesian inference, a distribution that models the many plausible values of the unknown quantity to be estimated. Bayesian inference is then using data (that is considered unchanging) to build a tighter posterior distribution for the unknown quantity.
Privacy	The right 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
Privacy breach	A situation where personally identifiable information (PII) is processed in violation of one or more relevant privacy safeguarding requirements
Privacy by design	The integration of privacy into the entire engineering process
Privacy controls	Measures that treat privacy risk by reducing its likelihood or consequences. Privacy controls include organizational, physical and technical measures, e.g., policies, procedures, guidelines, legal contracts, management practices or organizational structures. Control is also used as a synonym for "safeguard" or "countermeasure."
Privacy engineering	Within systems engineering, a discipline focused on maximizing the freedom of data subjects from adverse consequence associated with illicit or illegal disclosures or abuse during (or as a result of) processing
Privacy impact	Anything that has an effect on the privacy of personally identifiable information (PII) owned by a data subject and/or group of data subjects
Privacy impact assessment	The overall process of identifying, analyzing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information (PII) within the broader risk management framework of an enterprise
Privacy incident management	The process by which an enterprise addresses a privacy breach
Privacy information management system (PIMS)	An information security management system that addresses the protection of privacy potentially affected by the processing of personally identifiable information (PII)
Privacy notice	A notification that provides individuals with information on how their personal data will be processed
Privacy policy	The intention, direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller, related to the processing of PII in a particular setting. It is a set of shared values governing the privacy protection of PII when processed in information and communication technology systems.
Privacy preferences	Specific choices made by an individual about how their personally identifiable information (PII) should be processed for a particular purpose
Privacy principles	A set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems

TERM	DEFINITION
Privacy risk	Any risk of informational harm to data subjects and/or organization(s), including deception, financial injury, health and safety injuries, unwanted intrusion and reputational injuries, where the harm or damage goes beyond economic and tangible losses
Privacy risk assessment	A process used to identify and evaluate privacy-related risk and its potential effects
Private blockchain	A blockchain system in which all physical and digital assets are owned by one entity, group or permissioned participant
Private branch exchange (PBX)	A telephone exchange owned by a private business as opposed to a common carrier or telephone company
Private cloud	An on- or off-premises cloud environment in which a specific enterprise controls all infrastructure resources
Private key	A mathematical key (kept secret by the holder) used to create digital signatures and, depending on the algorithm, decrypt messages or files encrypted for confidentiality with the corresponding public key
Private key cryptosystems	A cryptosystem that involves 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
Privilege	The level of trust with which a system object is imbued
Privileged access management (PAM)	An access control mechanism that uses a combination of people, processes and technology to safeguard identities with special access or capabilities beyond regular users
Privileged access management systems	Solutions that help control, secure, manage and monitor privileged access to critical assets
Privileged user	Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account.
Probability	A mathematical-driven measure of the possibility of a specific outcome as a ratio of all possible outcomes
Probability distribution	For a discrete random variable, a listing of all possible distinct outcomes and their probabilities of occurring. Because all possible outcomes are listed, the sum of the probabilities must add up to 1.0.
Probe	The act of inspecting a network or system to find weak spots
Problem	In IT, the unknown underlying cause of one or more incidents
Problem escalation procedure	The process of escalating a problem 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 parts of processes.

TERM	DEFINITION
Process	**1.** 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 (ISACA) *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. **2.** A set of interrelated activities that transform inputs into outputs to achieve a given purpose (CMMI) See Process element
Process action team	A team with responsibility for developing and implementing process-improvement activities for an organization See Process group
Process architecture	The ordering, interfaces, interdependencies and other relationships among the process elements in a standard process or standard processes
Process capability	A recorded range of expected results that can be achieved by following a process
Process description	A record for a specific process. Process descriptions may be documents, embedded or automated steps or instructions in a robot, component, system, tool, or graphical representations, etc.
Process element	The fundamental unit of a process that cannot be further broken down
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
Process group	The people or team who hold a process role and are responsible for developing, deploying and updating the organization's process assets See Process role
Process improvement	Tasks and activities planned, performed and used to improve an organization's process capability and performance to achieve business objectives more effectively See Organization's business objectives
Process improvement objectives	A set of measurement objectives established to focus process improvement in a specific, measurable way that improves performance to achieve an organization's business objectives and build or improve capability See Measurement and performance objective, Organization's business objectives and Quantitative objective
Process improvement plan	A process improvement plan records the objectives, activities, resources, oversight, schedules, and associated risks to improve processes
Process maturity assessment (PAM)	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

TERM	DEFINITION
Process measurement	Activities performed to collect information and assign numeric values related to the activities, steps and outputs of following a process. This information is analyzed to determine the effectiveness and efficiency of a process. See Measurement and Process performance
Process monitoring	This context focuses on evaluating process adherence and performance improvement. This can be done within a single organization or included in the teaming relationship between an acquiring organization and a supplier organization. An acquiring organization typically conducts appraisals to monitor supplier process implementation, and results can serve as input toward: • Tailoring contract monitoring or process monitoring activities • Deciding incentive/award fees • Developing and keeping updated risk and opportunity management plans
Process owner	The person or team responsible for developing, updating or following a process. An organization or project can have multiple owners at different levels of responsibility for: • An organization's set of standard processes • Project-specific and project-defined processes
Process performance	A measure of results achieved by following a process. Process performance may be characterized by both process measures (e.g., effort, cycle time and defect removal efficiency) and solution measures (e.g., reliability, defect density and response time). See Business performance
Process performance baseline	A record and description of historical process performance resulting from following a defined process, which can include central tendency, e.g., mean, medium, mode, variation, and reflects how the process is being performed. Process performance baselines can be used as benchmarks for comparing actual process performance to expected process performance and can be used in process performance models to predict future process performance. See Process performance and Process performance model
Process performance model	A predictive analytical tool that identifies the controllable factors and describes the relationships between measurable attributes of one or more processes, subprocesses, process elements, or work products See Process performance baseline and Quality and process performance objectives
Process role	A description of the roles of people who develop, use, or follow a process in an organization. This role is typically recorded in a process description or related artifact, e.g., a roles and responsibility table or matrix. People in these roles provide objective evidence OE showing and explaining their roles and responsibilities and how they participate in the processes.
Processing	Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing (by transmission, dissemination or otherwise making available), aligning or combining, restricting, erasing or destructing *Scope Notes:* In the context of privacy (e.g., GDPR)
Processing PII	Operation or set of operations performed on personally identifiable information (PII). Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.
Processor (Data)	A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller
Processor (IT) (IT)	See Central processing unit (CPU).

TERM	DEFINITION
Product component	A work product that is a building block of the product or solution. Product components can be integrated to produce the final product or solution. There can be multiple levels of components.
Product life cycle	A representation of the set of steps or activities, consisting of phases, that begins at conception of a product or service and ends when the product or service is no longer available for use. For example, a product life cycle could consist of the following phases: • Concept and vision • Feasibility • Design/development • Production • Delivery • Phaseout, retirement or sunset. Organizations can produce multiple products or services for multiple customers, and so may define multiple product life cycles. These life cycles may be adapted from published literature for use in an organization.
Product line	A group of products: • Sharing a common, managed set of features • Satisfying specific needs of a selected market or mission • Developed from a common set of core assets in a prescribed way
Production program	Program used to process live or actual data that were received as input into the production environment
Production software	Software 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 standards and codes of practice.
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 *Scope Notes:* Source: American Institute of Certified Public Accountants (AICPA) AU 230.07
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.
Profiling	The automated processing of personal data to evaluate or make a decision about an individual. Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements

TERM	DEFINITION
Program (IT) (IT)	**1.** A sequence of instructions suitable for processing. Processing may include the use of an assembler, compiler, interpreter or another translator to prepare the program for execution. The instructions may include statements and necessary declarations. **2.** (ISO) To design, write, and test programs **3.** (ANSI) In programming languages, a set of one or more interrelated modules capable of being executed **4.** Loosely, a routine **5.** Loosely, to write a routine
Program (Project Management)	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 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
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
Programmable read-only memory (PROM)	A chip that can be programmed using a PROM programming device. It can be programmed only once. It cannot be erased and reprogrammed. Each of its bit locations is a fusible link. An unprogrammed PROM has all links closed, establishing a known state of each bit. Programming the chip consists of sending an electrical current of a specified size through each link that is to be changed to the alternate state. This causes the fuse to blow, opening that link.
Programming language	A language used to express computer programs Source: IEEE See Computer language, High-level language and Low-level language.
Project	**1.** A structured set of activities concerned with delivering a defined capability (one that is necessary but not sufficient to achieve a required business outcome) to the enterprise based on an agreed-upon schedule and budget (ISACA) **2.** A managed set of interrelated activities and resources, including people, that delivers one or more solutions to a customer or end user. A project typically has an intended beginning (project startup) and end and may be continuous. Projects typically operate according to a plan and set of requirements. The term "project" includes where and how the work gets done —whether developing a product, providing a service, performing an organizational function, acquiring and managing suppliers, etc. Work in support of a project is sometimes performed by workgroups. The operational parameters of workgroups can vary based on objectives and should therefore be clearly defined. Workgroups can operate as a project, if designated accordingly. (CMMI) See Process role and Organizational and in-scope projects.
Project management officer (PMO)	The individual responsible for the implementation of a specified initiative for supporting the project management role and advancing the discipline of project management

TERM	DEFINITION
Project ownership risk	The risk that information and technology (I&T) projects fail to meet objectives through lack of accountability and commitment
Project plan	A management document describing the project approach. The plan typically describes work to be done, resources required, methods to be used, configuration management and quality assurance procedures to be followed, schedules to be met, project organization, etc. Project in this context is a generic term. Some projects may also need integration plans, security plans, test plans, quality assurance plans, etc. (ISACA) Source: NIST See Documentation plan, Software development plan, Test plan and Software engineering. **1.** A plan that provides the basis for performing and controlling project activities and addresses commitments to the customer. A project plan is based on estimating the attributes of work products and tasks, determining the resources needed, negotiating commitments, producing a schedule and identifying and analyzing risks. Iterating through these activities can be necessary to establish the project plan. (CMMI)
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 risk	A failed IT project that poses a significant risk to an enterprise, manifesting as lost market share, failure to seize new opportunities or other adverse impacts on customers, shareholders and staff
Project startup	Initial time period when a project begins See 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
Prompt engineering	In generative artificial intelligence (AI), the process of providing instructions to guide a model toward generating the desired output. Also known as prompting.
Proof of elapsed time (PoET)	A consensus mechanism algorithm often used on permissioned blockchain networks to randomly decide the next block publisher
Proof of importance (PoI)	A variation of proof of stake that takes into consideration the role of validators and shareholders in the blockchain operation
Proof of stake (PoS)	Proof of stake is a type of consensus algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. In PoS consensus, the creator of the next block of data is chosen via several combinations of random selection and wealth or age (i.e., the stake) within the blockchain. With PoS, miners can mine or validate block transactions based on amount of cryptocurrency a miner holds. PoS was created as an alternative to PoW, which requires large amounts of energy. PoS gives mining power based on the percentage of cryptocurrency held by a miner. It is seen as less risky in terms of network attacks and security and used only for public blockchains.

TERM	DEFINITION
Proof of work (PoW)	PoW is conducted through miners (participants who keep the blockchain running by providing computing resources) who are competing to solve a cryptographic problem (i.e., hash puzzle). The PoW algorithm is used to confirm transactions and produce new blocks which are added to the chain. With PoW, miners compete against each other to complete transactions on the network and get rewarded. The computational work required to accomplish this is fairly (and usually increasingly) difficult for miners to perform, but easy for the network to verify. As difficulty increases over time, the amount of computational power, and hence, energy consumption, grows. Bitcoin is the first widespread application use of PoW. PoW is applicable to public blockchains.
Protection domain	The area of the system that the intrusion detection system (IDS) is meant to monitor and protect
Protective measure	A measure intended to achieve adequate risk reduction
Protocol	The rules by which a network operates and controls the flow and priority of transmissions
Protocol code	Cryptographically secure code prescribing strict adherence to the design and functioning of blockchains/distributed networks. This code can only be expanded or modified with approval from the network consensus mechanism.
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 implements 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) to test various aspects of a design, illustrate ideas or features and gather early user feedback. 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.
Provisioning	Allocating resources for cloud computing infrastructure or instance
Proxy (sensitive attributes)	An attribute used as a stand-in for a sensitive attribute
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.
Pseudocode	A combination of programming language and natural language used to express a software design. If used, it is usually the last document produced prior to writing the source code.
Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
Public blockchain	A blockchain system in which physical and digital assets are decentralized, zero-trust based and hosted/maintained on ephemeral networks and nodes
Public cloud	A cloud environment in which resources are shared between enterprises and individuals
Public key	In an asymmetric cryptographic scheme, the key that may be widely published to enable the operation of the scheme

TERM	DEFINITION
Public key cryptosystem	A cryptosystem that combines 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
Public key encryption	A cryptographic system that uses two keys: a public key, which is known to everyone, and 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
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
Purple team	A cooperative engagement where the red team simulates attacks and exploits while the blue team actively defends against them, allowing for real-time feedback, analysis and evaluation of defensive measures, detection capabilities, incident response processes and overall security controls. The purpose of a purple team is to improve the enterprise's security posture by enhancing communication and collaboration between the red and blue teams.
Purpose limitation	A process where data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Python	A scripting programming language created in 1994 that is popular for data science
QA	The acronym for quality assurance
QC	The acronym for quality control
Qualitative risk analysis	An approach based on expert opinion, judgment, intuition and experience
Quality	A term that means being fit for purpose (and achieving intended value) *Scope Notes:* COBIT 5 perspective
Quality and process performance objectives	Quantitative objectives and performance requirements for solution quality and process performance. These objectives include the use of statistical and quantitative analysis on the related data. See Measurement and performance objectives
Quality assurance (QA)	A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements (ISO/IEC 24765)
Quality assurance, software	**1.** A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements **2.** A set of activities designed to evaluate the process by which products are developed or manufactured
Quality attribute	A property of a solution by which affected stakeholders will judge its quality. Quality attributes are nonfunctional, significantly influence architecture and characterized by one or more measures. *Scope Notes*: Examples include availability, maintainability, modifiability, reliability, responsiveness, scalability, security, timeliness, throughput and usability.
Quality control	The operational techniques and procedures used to achieve quality requirements

TERM	DEFINITION
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
Quantile, quartile	When a set of sorted values is divided into groups that each have the same number of values (for example, if the values are divided into two groups at the median), each group is known as a quantile. If values are divided into four groups, they are called quartiles, which is a common way to divide values for discussion and analysis purposes. If there are five groups, they are called quintiles, and so forth.
Quantitative management	A type of project management that uses quantitative techniques to understand actual or predicted process performance relative to quality and process performance objectives, variation and corrective action needed to meet the objectives
Quantitative objective	A desired target value expressed using measures See Measure, Process improvement objectives and Quality and process performance objectives
Quantitative risk analysis	An approach that is based on a calculation of a risk's likelihood and impact using numerical and statistical techniques
Quantitatively managed process	A defined process evaluated and controlled using statistical and other quantitative techniques. A quantitatively managed process is necessary at the Practice Group Level 4 in the CMMI Practice Areas.
Question answering	Systems that retrieve answers to user-posed questions using a variety of natural language processing (NLP), information retrieval and reasoning techniques
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 that 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 hours.
R	An open-source programming language and environment for statistical computing and graph generation available for Linux, Windows and Mac
RACI chart	A matrix that illustrates who is Responsible, Accountable, Consulted and Informed within an organizational framework
RACI model	A method to define and depict roles and responsibilities
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
RAM	Random-access memory
Random forest	An ensemble approach to finding the decision tree that best fits the training data by creating many decision trees and then determining the average one. The random part of the term refers to building each of the decision trees from a random selection of features; the forest refers to the set of decision trees.
Random-access memory (RAM)	A type of primary computer memory. RAM is volatile, and data is lost with power loss.
Randomness	An important concept, also called entropy, in many cryptographic implementations. It is used to create keys, generate initialization vectors (i.e., random values that seed or initialize an algorithm), generate nonces (i.e., single-use, disposable values) and supply padding (i.e., additional data completing a block of fixed length).
Range check	A measurement that ensures that data fall within a predetermined range

TERM	DEFINITION
Rank (ordinality)	The ordinal position of a class in a machine-learning problem that categorizes classes from highest to lowest
Ransomware	Malware that restricts access to the compromised system until a ransom demand is satisfied
Ransomware detectors	Tools used to detect ransomware
Rapid application development (RAD)	A well-defined 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
Rapid elasticity	The ability to quickly increase or reduce the amount of resources utilized by a cloud computing instance or infrastructure
Rapid prototyping	A structured software requirements discovery technique that emphasizes generating prototypes early in the development process to permit early feedback and analysis in support of that process. Contrasts with incremental development, spiral model and waterfall model. See Prototyping.
Rater	A human who provides labels in examples. Sometimes called an annotator.
Read-only memory (ROM)	A type of primary computer memory. ROM is nonvolatile, and data stored there survives power loss.
Real-time analysis	Analysis that is performed on a continuous basis, with results gained in time to alter the run-time system
Real-time database activity monitoring solutions	Solutions that capture database query activity in the present time
Real-time processing	A fast-response (immediate response) online system that obtains data from an activity or a physical process, performs computations and returns a response rapidly enough to affect (i.e., control) the outcome of the activity or process, for example in a process control application. Contrasts with batch processing.
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	A measurement that compares data to predefined reasonability limits or occurrence rates established for that data
Recall	A metric for classification models that answers the following question: Out of all the possible positive labels, how many did the model correctly identify?
Recipient	A natural or legal person, public authority, agency or other body to which personal data are disclosed, whether a third party or not. However, public authorities that may receive personal data in the framework of a particular inquiry in accordance with state law are not regarded as recipients; the processing of those data by those public authorities should be in compliance with the applicable data protection rules, according to the purposes of the processing.
Reciprocal agreement	An emergency processing agreement between two or more enterprises with similar equipment or applications *Scope Notes:* Typically, participants in 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. Separate fields within the record are used for processing of the information.
Record, screen and report layouts	Layouts that provide information regarding the type of record, its size and the type of data contained in the record (record layouts), or that describe what information is provided and necessary for input (screen and report layouts)

TERM	DEFINITION
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)
Recovery action	A response or task executed to recover from a disruption in operations according to a written procedure
Recovery point objective (RPO)	The earliest point in time that is acceptable to recover data, determined based on the acceptable data loss in case of a disruption in operations . 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 a 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
Rectification	A data subject’s ability to have any incorrect personal data be corrected
Recurrent neural network	A neural network that is intentionally run multiple times, where parts of each run feed into the next run
Red team	A group of skilled professionals who simulate real-world cyberattacks, security breaches and physical security compromises to evaluate the effectiveness of an enterprise’s defenses. The red team identifies vulnerabilities, weaknesses and potential exploits in the enterprise’s systems, networks, applications and physical security controls. They often use the same tactics, techniques and procedures as real-world adversaries to provide a realistic testing environment.
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	A test that detects transmission errors by appending calculated bits onto the end of each segment of data
Redundant array of inexpensive disks (RAID)	A storage configuration that uses hardware or software to write information to multiple disks to improve performance and fault-tolerant capabilities and/or save large files simultaneously
Redundant site	A recovery strategy involving the duplication of key IT components, including data or 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.
Reference model	A defined model describing practices and activities that is used for improving performance or as a benchmark for measuring capability or maturity
Refraction	A form of signal degradation due to an RF signal being bent, typically when the signal passes through a medium of different density. This can decrease data rates and cause retransmissions.

TERM	DEFINITION
Registered interpreter	A role that works across the spoken languages of all appraisal stakeholders to simultaneously, clearly and accurately interpret and communicate appraisal information. Interpreters must be registered with ISACA. The interpreter's job is to translate the content of original source information into the spoken language of the Appraisal Team Leader and the appraisal team. Certified CMMI Lead Appraisers may fulfill the role of Registered Interpreter and ATM if approved by ISACA, and consistent with the MDD requirements.
Registered ports	Ports 1024 through 49151, which are listed by the IANA and can be used on most systems by ordinary user processes or programs executed by ordinary users
Registration authority (RA)	An authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it
Regression analysis and testing	A software verification and validation (V&V) task to determine the extent of V&V analysis and testing that must be repeated when changes are made to any previously examined software products Source: IEEE See Testing, regression.
Regression analysis tools	Tools that provide the information to allow for examination of the relationship between two or more variables
Regression model	A type of model that outputs continuous (typically floating-point) values
Regression testing	A testing technique used to retest earlier program abends or logical errors that occurred during the initial testing phase
Regularization	A set of techniques that control a model's complexity during training by penalizing features or weights to prevent overfitting the training data
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 be compliant
Reidentification	The process of discovering the individual to whom deidentified data belong by matching anonymous data with publicly available information or auxiliary data
Reinforcement learning	A class of machine-learning algorithms in which the process is not given specific goals to meet but, as it makes decisions, is instead given indications of whether it is doing well or not
Rekeying	The process of changing cryptographic keys. Periodic rekeying limits the amount of data encrypted by a single key.
Relational database	A database organization method that links files together as required. Relationships between files are created by comparing data, such as account numbers and names. A relational system can take any two or more files and generate a new file from the records that meet the matching criteria. Routine queries often involve more than one data file, e.g., a customer file and an order file can be linked to answer a question that relates to information in both files, such as the names of the customers that purchased a particular product. Contrasts with network database and flat file.
Relational database management system (RDBMS)	A relational database management system (RDBMS) is a collection of programs and capabilities that enable IT teams and others to create, update, administer and interact with a relational database *Scope Notes:* Database management systems have evolved from hierarchical to network to relational models. Today, the most widely accepted database model is the relational model. The relational model has three major aspects or conditions of the populatioin. An Oracle database is a collection of data that is treated as a unit.

TERM	DEFINITION
Release	The formal notification and distribution of an approved version See Version.
Release candidate (RC)	A software version that can possibly be released to end users
Release-candidate push solutions	Solutions that push release-candidate software
Relevance risk	The risk that the correct information may not get to the correct recipients at the correct time to allow the correct action to be taken or the correct decisions to be made
Relevant audit evidence	Audit evidence that pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support
Relevant information	Relating to controls, information that 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. *Scope Notes:* Refer to COBIT 5 information quality goals.
Relevant sampling factor	A sampling factor that describes aspects or conditions that affect the way work is performed in the organizational unit. This effect results in work being performed differently, by either a project team or an organizational function. See Sampling factors.
Reliable audit evidence	Audit evidence that, in the IS auditor's opinion, is valid, factual, objective and supportable
Reliable information	Information that is accurate, verifiable and from an objective source *Scope Notes:* Refer to COBIT 5 information quality goals.
Remediation	Actions taken to mitigate or eliminate a vulnerability after it has been identified and assessed
Remote access	An authorized user’s ability to access a computer or network from anywhere through a network connection
Remote access controllers	Hardware and software solutions for remote systems management
Remote access service (RAS)	Any combination of hardware and software that enables remote access to tools or information that typically reside on a network of IT devices *Scope Notes:* Originally coined by Microsoft when referring to its built-in NT remote access tools, RAS was a service provided by Windows NT that allowed most of the assets that would be available on a network to be accessed over a modem link. Over the years, many vendors have provided hardware and software solutions to create 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

TERM	DEFINITION
Remote Procedure Call (RPC)	The traditional Internet service protocol widely used for many years on UNIX-based operating systems and supported by the Internet Engineering Task Force (IETF) that allows a program on one computer to execute a program on another (e.g., a server) *Scope Notes:* The primary benefit derived from using a remote procedure call 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.
Removable media	Any type of storage device that can be removed from the system while it is running
Repeaters	A physical layer device that regenerates and propagates electrical signals between two network segments *Scope Notes:* Repeaters receive analog or digital signals from a network segment and amplify (regenerate) them to compensate for distortion from transmission loss caused by reduction of signal strength during transmission (i.e., attenuation).
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
Replication	In a broad computing sense, the use of redundant software or hardware elements to provide greater 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 across all systems.
Repository	An enterprise database that stores and organizes data
Representation	A signed or oral statement issued by management to professionals, in which management declares that a current or future fact (e.g., a process, system, procedure or policy) is or will be in a certain state, to the best of management's knowledge
Repudiation	A denial by one of the parties to a transaction of participation in all or part of that transaction, or of the content of a 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 for a different bank and since it cannot discuss any problems in person with the customer.
Request for comments (RFC)	A document approved by the Internet Engineering Task Force (IETF) and 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

TERM	DEFINITION
Requirement	**1.** A condition or capability needed by a user to solve a problem or achieve an objective **2.** A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification or other formally imposed document **3.** A documented representation of a condition or capability as in definition 1 or 2 See Design requirement, Functional requirement, Implementation requirement, Interface requirement, Performance requirement and Physical requirement. (ISACA) **4.** A recorded description of an aspect, performance or capability required by a user or customer (CMMI)
Requirements analysis	**1.** The process of studying user needs to arrive at a definition of a system, hardware or software requirements **2.** The process of studying and refining system, hardware or software requirements (ISACA) Source: IEEE See Prototyping and Software engineering. **3.** Tasks that determine the needs or conditions to meet a new or altered solution, accounting for multiple perspectives, e.g., balancing stakeholder needs and constraints, the allocation of requirements to components, or breaking down complex requirements to lower-level requirements (CMMI)
Requirements definition	A technique in which affected user groups explain what is needed from a system *Scope Notes:* Some of these are business-, regulatory- or security-related requirements as well as development-related requirements.
Requirements elicitation	A technique for gathering knowledge or information to proactively identify and record customer and end-user needs
Requirements management	The process of documenting, analyzing, tracing, prioritizing and agreeing on requirements and then controlling change and communicating to relevant stakeholders. It is a continuous process throughout a project.
Requirements phase	The period in the software life cycle during which requirements, such as functional and performance capabilities for a software product, are defined and documented Source: IEEE
Requirements review	A process or meeting during which the requirements for a system, hardware item or software item are presented to project personnel, managers, users, customers or other interested parties for comment or approval. Types include system requirements review and software requirements review. Contrasts with code review, design review, formal qualification review and test readiness review. Source: IEEE
Requirements traceability	A record of the relationships between requirements and related requirements, implementations and verifications See Bidirectional traceability.
Residual risk	The remaining risk after management has implemented a risk response
Residual security risk	The remaining probability of an event occurring and its consequence that still exists after a risk response has been implemented
Resilience	The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect

TERM	DEFINITION
Resource	Any enterprise asset that can help the organization achieve its objectives *Scope Notes:* COBIT 5 and COBIT 2019 perspective
Resource management	**1.** The coordinated activities taken by an enterprise to plan, schedule, and allocate resources to meet its business objectives *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
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 and COBIT 2019 perspective
Resource pooling	In cloud computing, the ability to combine computing resources and services to serve multiple customers at once
Responsible (RACI)	In a Responsible, Accountable, Consulted, Informed (RACI) chart, refers to the person who must ensure that activities are completed successfully
Restricted access window (RAW)	A set access window in which a device can receive communications from other devices
Restriction of processing	The marking of stored personal data with the aim of limiting their processing in the future
Return on investment (ROI)	**1.** 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 (ISACA) **2.** The ratio of benefit of a process or solution improvement to implementation costs to determine the value (CMMI)
Return-oriented programming 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
Reverse engineering	A software engineering technique whereby existing application system code can be redesigned and coded using computer-aided software engineering (CASE) technology
Review	A process or meeting during which a work product or set of work products is presented to project personnel, managers, users, customers or other interested parties for comment or approval. Types include code review, design review, formal qualification review, requirements review and test readiness review. Contrasts with audit and inspection. Source: IEEE See Static analysis.
Ring configuration	A type of network architecture in which all stations (nodes) are connected to a multi-station access unit (MSAU) that physically resembles a star-type topology. This configuration is used in either token ring or fiber distributed data interface (FDDI) networks. *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 to 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 each receiving node reading those messages addressed to it.

TERM	DEFINITION
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. After receiving a message, each station also acts as a repeater, retransmitting the message at its original signal strength.
Risk	**1.** The combination of the likelihood of an event and its impact (ISACA) **2.** A potential uncertain event that may be harmful or may negatively impact objective achievement (CMMI)
Risk acceptance	A decision to accept a risk, made according to the risk appetite and risk tolerance set by senior management, where the enterprise can assume the risk and absorb any losses
Risk aggregation	The process of integrating risk assessments at a corporate level to obtain a complete view of the overall risk for the enterprise
Risk analysis	**1.** A process by which the 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:* Risk analysis 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 *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 project delivery risk and project benefit risk.
Risk avoidance	The process for systematically avoiding risk, constituting one approach to managing risk
Risk awareness program	A program that creates an understanding of risk, risk factors and the various types of risk that an enterprise faces
Risk capacity	The objective magnitude or amount of loss that an enterprise can tolerate without risking its continued existence
Risk culture	An organization's shared values and beliefs that govern attitudes toward risk-taking, care and integrity, and determine how openly risk and losses are reported and discussed
Risk evaluation	The process of comparing 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, the magnitude and ultimately the business impact of IT-related risk scenarios
Risk gap	A gap that exists when the acceptable level of risk and the current state of risk are different
Risk identification	The process for determining and documenting the risk an enterprise faces
Risk indicator	A metric capable of showing that the enterprise may realize a risk.

TERM	DEFINITION
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	**1.** The management of risk through the use of countermeasures and controls (ISACA) **2.** A set of planned activities that, if performed, may minimize the probability or impact of the risk (CMMI)
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.
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 or scenarios, or risk concentration or correlation across silos) and the potential effect of risk response across multiple types of risk
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 register	A list of risk scenarios that have been identified, analyzed and prioritized
Risk response	Any combination of risk avoidance, risk acceptance, risk sharing or transfer, or risk mitigation that leads to a situation in which as much future residual risk (i.e., current risk with the risk response defined and implemented) as possible (usually depending on budgets available) falls within risk appetite limits
Risk scenario	A tangible and assessable representation of risk *Scope Notes:* One of the key information items needed to identify, analyze and respond to risk (COBIT 2019 objective APO12)
Risk scope	The selection of items included in the risk activities, based on understanding the full risk universe and then down-selecting to the specific part of the enterprise to which the risk activities will be applied
Risk sharing	*Scope Notes:* See Risk transfer
Risk source	An element that, alone or in combination, has the potential to give rise to risk
Risk statement	A description of the current conditions that may lead to a loss, along with a description of the potential 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.
Risk taxonomy	A scheme for classifying sources and categories of risk that provides a common language for discussing and communicating risk to stakeholders

TERM	DEFINITION
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)
Risk universe	An enterprise's overall conception of risk, which encompasses the overall risk environment, defines the areas that risk management activities will address and provides a structure for information and technology (I&T)-related risk management
Robotics	The design, development, and operation of autonomous or semiautonomous machines capable of performing tasks in the physical world
Robustness	The degree to which a software system or component can function correctly in the presence of invalid inputs or stressful environmental conditions See Software reliability.
ROI	See Return on Investment.
ROM	See Read-only memory.
Root cause	The underlying source of a defect or problem
Root cause analysis	A process of diagnosis to establish the origins of events that can be used for learning from consequences, typically from errors and problems
Root mean squared error	The root mean square error (RMSE) measures the average difference between a statistical model's predicted values and the actual values. RMSE is one of two main performance indicators for regression models.
Rootkit	A software suite designed to aid an intruder in gaining unauthorized administrative access to a computer system
Rotating standby	A failover 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 fraud involving a computer code that instructs the computer to remove small amounts of money from authorized transactions 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, protocols and network applications (ports).
Routine	A subprogram that is called by other programs and subprograms *Scope Notes:* This term is defined differently in various programming languages. Source: IEEE See Module.
RS-232 interface	An interface between data terminal equipment and data communications equipment employing serial binary data interchange

TERM	DEFINITION
RSA (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.
Ruby	A scripting language that first appeared in 1996. Ruby is popular in the data science community, but not as popular as Python, which has more specialized libraries available for data science tasks.
Rulebase	The list of rules and/or guidance used to analyze event data
Run instructions	Computer operating instructions that detail the step-by-step processes that are to occur so an application system can be properly executed. These instructions also identify how to address problems that occur during processing.
Run-to-run totals	Aggregate numbers that provide evidence that a program processed all input data and that it processed the data correctly
S curve	A type of curve that shows the growth of a variable in terms of another variable, often expressed as units of time. The S curve is often mentioned when someone predicts that a rising value will eventually level off.
Safeguard	A practice, procedure or mechanism that reduces risk
Safety	A condition of protection from harm. The two key domains of safety are workplace environment and functional safety.
Salami technique	A method of computer fraud involving a computer code that instructs the computer to slice off small amounts of money from authorized transactions and reroute these amounts to the perpetrator's account
Sample eligible (SE)	A project or organizational support function in an OU that is suitable to be considered for the randomly generated sample (RGS) because the project is performing process activities that are believed to align to model practices
Sampling factors	Context that reflects potential differences in processes and the way work is performed See Relevant sampling factor.
Sampling risk	The probability that an IT 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.
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
Sandboxing	Using an isolated environment for testing purposes
SAS	A commercial statistical software suite that includes a programming language also known as SAS
Scalar	A quantity that has magnitude but no direction in space, such as volume or temperature
Scaling	A commonly used practice in feature engineering to tame the range of values of a feature to match the scale of other features in the data set
Scattering	Signal degradation that occurs when RF signal increases in size due to reflection or passing through objects
Schedule risk	The risk that information and technology (I&T) projects will take longer than expected

TERM	DEFINITION
Scheduling	A method used in the information processing facility (IPF) to determine and establish the sequence of computer job processing
Scope creep	Uncontrolled changes in a project's scope. Also called requirement creep. *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 the 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 which products and features are required to bring about the achievement of project objectives or a weak project manager or executive sponsor.
Scoping process	A process for identifying the boundary or extent to which a process, procedure, certification, contract, etc., applies
Scoring	The part of a recommendation system that provides a value or ranking for each item produced by the candidate generation phase
Screening router	A router configured to permit or deny traffic based on a set of permission rules installed by the administrator
Scripting	Generally, the use of a computer language to write a program or script that can be run directly, with no need to compile it to binary code, as with languages such as Python, Java and C
Secure development life cycle	The inclusion of security in the software development life cycle
Secure Electronic Transaction (SET)	A standard that ensures credit card and associated payment order information travel safely and securely between the various involved parties on the Internet
Secure multiparty computation (SMP or MPC)	Data operation in which multiple parties transact jointly while maintaining privacy of their individual and/or several input(s) during processing
Secure Multipurpose Internet Mail Extensions (S/MIME)	Cryptographic security services for electronic messaging applications: authentication, message integrity and nonrepudiation 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
Secure Sockets Layer (SSL)	A protocol used to transmit private documents through the Internet *Scope Notes:* The SSL protocol uses a private key to encrypt the data 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 as a Service (SecaaS)	The next generation of managed security services dedicated to the delivery over the Internet of specialized information-security services

TERM	DEFINITION
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), United Kingdom, 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 several security awareness campaigns.
Security awareness coordinator	The individuals responsible for creating and maintaining the security awareness program and coordinating the different campaigns and efforts of the various groups involved in the program. They are also responsible for ensuring 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 the goal is to realize and maintain a security-aware culture, i.e., 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 • Creating 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 typically 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 incident response team (SIRT)	Cross-functional team responsible for addressing security incidents
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 comprise 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 model	An engineering model informed by policies that specify how a system will enforce security

TERM	DEFINITION
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 established in the security policy and standards are to be achieved
Security resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from security disruptions, including cybersecurity. Resilience includes the capability to withstand and recover from deliberate attack, accidents or naturally occurring threats, vulnerabilities or other security events
Security reviews and evaluations	The coverage or inclusion of security needs, constraints, efforts and activities in a continuous manner over time throughout the life cycle of a solution or when triggered by a security event. These reviews and evaluations focus on identifying and addressing, and when possible, preventing the most critical and urgent security issues first. Security events, trends, potential threats and disruptions can also trigger reviews or evaluations.
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 the required work and focus areas of current relevance and concern and are a translation of issues already mentioned in the security policy
Security steps or actions	The terms used interchangeably to indicate the same intent or meaning as "security measures" in the CMMI Product Suite®. Most security standards and frameworks refer to "security measures," where measures are not measurements (a noun) but rather steps or actions (a verb).
Security testing	Assurance 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 threats	Any circumstance or event with the potential to adversely impact organizational operations including mission, functions, assets, personnel, processes, systems or brand reputation through unauthorized access, destruction, disclosure, modification of information or denial of service. *Source: CMMC without redundancies*
Security token	Digital assets or tokens created to represent a quantity of a specified investment, including rights to ownership, payment of a specific sum under a contract, entitlement to future profits, etc.
Security vulnerabilities	Weakness in a solution, information system, system security procedure, internal control or implementation that could be exploited by a threat source *Source: CMMC/NIST SP 800-30 Rev 1*
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.
Segmentation	See Network segmentation
Segregation of duty (SoD)	See Segregation/separation of duties (SoD).

TERM	DEFINITION
Segregation/ separation of duties (SoD)	A basic internal control that prevents or detects errors and irregularities by assigning the responsibility for initiating and recording transactions and the custody of assets to separate individuals *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.
Semiconductor	Substrate for integrated circuit that regulates electric current and often made primarily of silicon
Senior management	The person or persons who provide the policy and overall guidance for the process but do not typically provide the direct day-to-day monitoring and controlling of the process. A senior manager has authority to direct the allocation or reallocation of resources in support of organizational process improvement effectiveness. A senior manager can be any manager who satisfies this description, including the CEO of the organization.
Sensitive attribute	A human attribute that may be given special consideration for legal, ethical, social or personal reasons
Sensitive PII	Category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal. It can consist of PII that reveals the racial origin; political opinions or religious or other beliefs; personal data on health, sex life or criminal convictions; and other PII that may be defined as sensitive.
Sensitivity	A measure of the impact that improper disclosure of information may have on an enterprise
Sensor	A device or component that gathers information critical to an IoT application and converts it to data
Sentiment analysis	The process of automatically determining the emotional tone, such as positive, negative, or neutral, expressed in a piece of text (e.g., opinions, reviews, social media posts) using natural language processing (NLP) and machine learning (ML) models trained on labeled data
Separation of duty (SoD)	See Segregation/separation of duties (SoD).
Sequence check	Verification that the control number follows sequentially and any control numbers out of sequence are rejected or noted in an exception report for further research *Scope Notes:* Can be alpha or numeric and usually utilizes a key field
Sequence-to-sequence model	A model that processes an input sequence to generate a new output sequence (e.g., transforming the text of an input in one language to generate an output in a different language)
Sequential file	A computer file storage format in which one record follows another *Scope Notes:* Records can be accessed sequentially only.
Serial correlation	The relationship between a variable and a lagged version of itself over various time intervals. Repeating patterns often show serial correlation when the level of a variable affects its future level.
Server	A high-speed computer in a network shared by multiple users that holds the programs and data shared by all users
Service	An activity that provides a promised exchange of value between a service provider and customer, product or work product. Services do not always produce tangible or storable products; in such instances, the service itself is the deliverable. See Solution.
Service bureau	A computer facility that provides data processing services to clients on a continual basis

TERM	DEFINITION
Service catalogue	Structured information on all IT services available to customers *Scope Notes:* COBIT® 5 perspective
Service delivery objective (SDO)	The level of services directly related to the business needs that must 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)	**1.** 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 (ISACA) **2.** A contract between a service provider, either internal or external, and the customer or end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive. SLAs do not define how the service itself is provided or delivered. (CMMI®)
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 system	An integrated and interdependent combination of components that satisfy stakeholder requirements
Service system component	A process, work product, person, consumable, customer or other resource required for a service system to deliver value that can include components owned by the customer or a third party
Service system consumable	An item used by the service system that ceases to be available or becomes permanently changed by its use during the delivery of a service
Service user	The organization using the outsourced service
Service-oriented architecture (SOA)	A cloud-based library of proven, functional software applets that can 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)	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.
Shadow IT	The use of systems, services, hardware or software on an enterprise network or within an enterprise's infrastructure without proper vetting and approval from the IT or cybersecurity department
Shall	An indication of a method requirement and hence not a tailoring option when used in any statement in the Appraisal Method Definition Document (MDD). In the MDD, "shall" may be used interchangeably with the word "must." See Must

TERM	DEFINITION
Shared responsibility model (SRM)	A cloud security framework that dictates the security obligations of a cloud service provider and its users to ensure accountability
Shared vision	A common understanding of guiding principles, including mission, objectives, expected behavior, values and final outcomes developed and used by a project or work group
Shell	Command line scripting languages, such as Perl and Python. Popular for data wrangling, Linux-based shell tools (which are either included with or easily available for Mac and Windows machines), include grep, diff, split, comm, head and tail.
Shell programming	A script written for the shell or command line interpreter of an operating system and 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 also act 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).
Sidechain	A separate blockchain that links data entries or transactions to a primary blockchain, allowing operations both from and to the sidechain
Sign-on procedure	The procedure performed by a user to gain access to an application or operating system *Scope Notes:* If the users are properly identified and authenticated by the system's security, they will be able to access the software.
Signal-to-noise ratio (SNR)	A measurement of the level of a desired signal to background noise documented in decibels. Ratios greater than 1 dB indicates the signal exceeds noise by that level. Signal power less than 1 dB represents an unusable signal.
Signature verification solutions	Secure solutions used to validate the identity of an individual
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 *Scope Notes:* A material weakness is a significant deficiency or a combination of significant deficiencies that result in more than a remote likelihood of an undesirable event(s) not being prevented or detected.
Simple fail-over	A fail-over process in which the primary node owns the resource group *Scope Notes:* The backup node runs a noncritical 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 (email) protocol on the Internet

TERM	DEFINITION
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.
Simple Text-Oriented Message Protocol (STOMP)	A plaintext protocol with semantics similar to HTTP designed for messaging applications
Single factor authentication (SFA)	Authentication process that requires only the user ID and password to grant access
Single point of failure	A resource whose loss will result in the loss of service or production
Single sign-on (SSO)	A single point authentication system used by multiple systems and applications
Size	Number of items or volume of work effort or work products being produced, such as activities, pages, requirements, number of components, solutions. Use size as a basis for scoping when producing estimates and plans.
Skill	The learned capacity to achieve predetermined results *Scope Notes:* COBIT® 5 and COBIT® 2019 perspective
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 of the transaction.
Small form factor	An engineering design that allows device components to use as little physical space as possible while still remaining functional
SMART (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.
Smart contract	Software (computer code) that automatically executes transactions and/or enforces agreements based on the fulfillment of the terms of the agreement by leveraging decentralized ledger technology that uses public validation to ensure correct and reliable performance according to agreed rules
Sniff	The act of capturing network packets, including those not necessarily destined for the computer running the sniffing software
Sniffers	Programs or hardware that monitor Internet traffic in real time

TERM	DEFINITION
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
Social IoT (SIoT)	A network of IoT-enabled devices that work together to provide a service or feature
Soft fork	A software upgrade that is backward compatible with previous versions of the blockchain software. Thus, a soft fork does not require all blockchain nodes to upgrade to maintain functionality.
Software	Programs, procedures, rules and any associated documentation pertaining to the operation of a system. It contrasts with hardware. See Application software, Operating system, System software and Utility software.
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 email).
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
Software development kit (SDK)	A group of utilities and libraries provided by a manufacturer or open source community to develop software for a particular framework or device
Software development plan	The project plan for the development of a software product. It contrasts with software development process and software life cycle.
Software development process	The process by which user needs are translated into a software product. The process involves translating user needs into software requirements, transforming the software requirements into design, implementing the design in code, testing the code and sometimes installing and reviewing the software for operational activities. Note that these activities may overlap or be performed iteratively. See Incremental development, Rapid prototyping, Spiral model and Waterfall model.
Software distribution solutions	Applications that build software installation packages and distribute them to end users
Software documentation	Technical data or information, including computer listings and printouts in human-readable form, that describe or specify the design or details, explain the capabilities or provide operating instructions for using the software to obtain desired results from a software system. Types of software documentation include: • Project planning documents, i.e., software development plans and software verification and validation (V&V) plans • Software requirements and design specifications • Test documentation • Customer-deliverable documentation • Program source code • Representation of software solutions implemented in firmware • Reports, e.g., review, audit and project status • Data, i.e., defect detection and test • It contrasts with software item. See: Specification; Specification, requirements; Specification, design; Software design description; Test plan, Test report, User's guide.

TERM	DEFINITION
Software element analysis	See Software review.
Software engineering	The application of a systematic, disciplined, quantifiable approach to the development, operation and maintenance of software, i.e., the application of engineering to software See Project plan, Requirements analysis, Architectural design, Structured design, System safety, Testing and Configuration management.
Software engineering environment	The hardware, software and firmware used to perform a software engineering effort. Typical elements include computer equipment, compilers, assemblers, operating systems, debuggers, simulators, emulators, test tools, documentation tools and database management systems.
Software life cycle	Period of time, beginning when a software product is conceived and ending when the product is no longer available for use. The software life cycle is typically broken into phases, denoting activities, such as requirements, design, programming, testing, installation, operation and maintenance. It contrasts with software development process. See waterfall model.
Software reliability	**1.** The probability that software will not cause the failure of a system for a specified time under specified conditions. The probability is a function of the inputs to and use of the system in the software. The inputs to the system determine whether existing faults, if any, are encountered. **2.** The ability of a program to perform its required functions accurately and reproducibly under stated conditions for a specified period of time
Software review	An evaluation of software elements to ascertain discrepancies from planned results and to recommend improvement. This evaluation follows a formal process. It is synonymous with software audit. See Code audit, Code inspection, Code review, Code walk-through, Design review, Specification analysis and Static analysis.
Software-defined access (SD-Access)	An intent-based networking technology that enables reduction of manual work, faster resolution of performance issues and better security. It is an evolution of SDN.
Software-defined networking (SDN)	Microsegmentation network infrastructure technology that separates the management and data planes. Typically used on core distribution networks, SDN aids performance management, policy administration and bandwidth on demand.
Software-defined wide area network (SD-WAN)	An extension of SDN across a WAN. It focuses on routing and traffic prioritization.
Solution	A product, product component, service, service system, service system component or delivered or acquired product or service including relevant safety or security components
Solution component	A work product that is a building block of the solution. Solution components are integrated to produce the solution. There can be multiple levels of solution components. See Product component
Solution stack	A collection of hardware, software and services that work simultaneously to provide an enterprise or user with a final product
SOPs	Standard operating procedures
Source code	Computer instructions and data definitions documented in a form suitable for input to an assembler, compiler or other translator
Source code compare program	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

TERM	DEFINITION
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 a deriver of single-point software-size estimations
Source program	A computer program that must be compiled, assembled or otherwise translated to be executed by a computer. It contrasts with object program. See Source code.
Source routing specification	A transmission technique where the sender of a packet can specify the route that packet should follow through the network
Spaghetti code	Program source code written without a coherent structure. It implies the excessive use of GOTO instructions and contrasts with structured programming.
Spam	Computer-generated messages sent as unsolicited advertising
Spanning port	A port configured on a network switch to receive copies of traffic from one or more other ports on the switch
Spatiotemporal data	Time series data that also include geographic identifiers, such as latitude-longitude pairs
Spear phishing	An attack designed to entice specific individuals or groups to reveal important information. Social engineering techniques are used to masquerade as a trusted party to obtain important information, such as passwords from the victim.
Special cause of variation	A cause of process variation that is a result of a known factor that results in a nonrandom distribution of output. It is also referred to as “exceptional” or “assignable” cause variation and is temporary in nature and not an inherent part of the process. See Common cause of variation
Specification tree	A diagram that depicts all the specifications for a given system and shows their relationship to one another Source: IEEE
Specification, requirements	A specification that documents the requirements of a system or system component. It typically includes functional requirements, performance requirements, interface requirements, design requirements (attributes and constraints), development (coding) standards, etc. This contrasts with "requirement." Source: NIST
Spiral model	A model of the software development process in which the constituent activities (typically requirements analysis, preliminary and detailed design, coding, integration and testing) are performed iteratively until the software is complete. It is synonymous with "evolutionary model." Spiral model contrasts with "incremental development," "rapid prototyping" and "waterfall model."
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 enterprise-wide, 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

TERM	DEFINITION
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. This is a condition under which two or more entities separately have key components that individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.
Spoofing	The act of faking the sending address of a transmission in order to gain illegal entry into a secure system
SPOOL (simultaneous peripheral operations online) (SPOOL)	An automated function that can be based on an operating system or application in which electronic data 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 with other operations instead of waiting on the slower speed receiving device, such as a printer.
SPSS	A commercial statistical software package used for predictive analysis
Spyware	Software whose purpose is to monitor a computer user's actions (e.g., websites visited) and report these actions to a third party without the informed consent of that machine's owner or legitimate user
SQL (SQL)	The ISO standard query language used by application programmers and end users to access relational databases. Variations of this popular language are often available for data storage systems that are not strictly relational.
SQL injection	An attack that results from the failure of an 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. Source: MITRE
Stable process	The state in which special causes of process variation have been removed from the process and prevented from recurring. In a stable process, only common cause variation of the process remains. See Capable process, Common cause of variation and Special cause of variation
Stablecoins	A type of cryptocurrency that is tied to an outside currency, such as the US dollar, to stabilize its value
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
Stakeholder	Anyone who has a responsibility for, an expectation of or some other interest in an enterprise *Scope Notes:* Examples include shareholders, users, government, suppliers, customers and the public.
Standard	A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as the International Organization for Standardization (ISO)
Standard deviation	The square root of a variance and a common way to indicate how different a particular measurement is from the mean
Standard normal distribution	A normal distribution with a mean of 0 and a standard deviation of 1. When graphed, it is a bell-shaped curve centered around the y axis, where x=0.
Standard operating procedures (SOP)	Written procedures that prescribe and describe the steps to be taken in normal and defined conditions and that are necessary to ensure control of production and processes

TERM	DEFINITION
Standardized score	A score that transforms a raw score into units of standard deviation above or below the mean. This translates the scores so they can be evaluated in reference to the standard normal distribution.
Standing data	Permanent reference data used in transaction processing *Scope Notes:* These data are changed infrequently, e.g., 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.
Stata	A commercial statistical software package; not to be confused with "strata"
State	A condition or mode of existence in which a system, component or simulation may be, e.g., the preflight state of an aircraft navigation program or input state of a given channel
State diagram	A diagram that depicts the states that a system or component can assume and shows the events or circumstances that cause or result from a change from one state to another. It is synonymous with "state graph." See State-transition table
Stateful inspection	A firewall architecture that tracks each connection traversing all interfaces of the firewall and makes sure they are valid
Statement of objectives (SOO)	The recorded top-level objectives of an acquisition or procurement used to guide discussions and negotiations between the acquirer and supplier
Statement of work (SOW)	A description of work to be performed and their respective groupings of tasks or activities See Memorandum of agreement
Static analysis	An analysis of information that occurs on a noncontinuous basis; also known as interval-based analysis
Statistical and other quantitative techniques	A term used to acknowledge that while statistical techniques are required, other quantitative techniques can also be used effectively. Analytic techniques allow parameters describing a task or work product to be quantified. Use statistical and other quantitative techniques to: • Analyze variation in process performance • Monitor the selected processes that help achieve quality and process performance objectives This term is used at levels 4 and 5, where practices describe how statistical and other quantitative techniques are used to improve understanding of work groups and organizational processes and performance. See Statistical techniques and Quantitative management
Statistical process control	Statistical analysis that identifies common and special causes of process variation and seeks to maintain process performance within limits See Common cause of variation, Special cause of variation and Statistical techniques
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

TERM	DEFINITION
Statistical stratification	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
Statistical techniques	Mathematical techniques used with the collection, analysis, interpretation and presentation of masses of numerical data to understand process variation and predict process performance. Examples include sampling techniques, analysis of variance, chi-squared tests, regression analysis and process control charts.
Statutory requirements	Laws created by government institutions
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.
Storage device	A unit into which data or programs can be placed, retained and retrieved See Memory.
Storage limitation	The principle that personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Strata, stratified sampling	Sampling technique used to divide the units into homogeneous groups (strata) and draw a simple random sample from each group
Strategic planning	The process of deciding on the enterprise's objectives, changes in these objectives, and the policies to govern their acquisition and use
Strategic risk	The risk associated with the future business plans and strategies of an enterprise
Strength	A type of preliminary or final finding that is an exemplary or noteworthy implementation of a process that meets the intent and value of a CMMI model practice
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
String	**1.** A sequence of characters **2.** A linear sequence of entities, such as characters or physical elements
Structured design	Any disciplined approach to software design that adheres to specified rules based on principles such as modularity, top-down design and stepwise refinement of data; system structure and processing steps See Data structure centered design, Input-processing-output, Modular decomposition, Object-oriented design, Rapid prototyping, Stepwise refinement, Structured programming, Transaction analysis, Transform analysis, Graphical software specification/design documents, Modular software and Software engineering.
Structured programming	Any software development technique that includes structured design and results in the development of structured programs See Structured design.
Structured Query Language (SQL)	A language used to interrogate and process data in a relational database. Originally developed for IBM mainframes, many implementations have been created for mini- and microcomputer database applications. SQL commands can be used to interactively work with a database or embedded with a programming language to interface with a database.
Subject access	This is the data subject's right to obtain from the data controller, on request, certain information relating to the processing of his/her personal data

TERM	DEFINITION
Subject access request	Request by data subject to receive a copy of personal data that an enterprise processes, to understand the purpose of said processing, or to understand and/or delimit how the data may be shared by the enterprise
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)
Subprocess	A process that is part of a larger process. Subprocesses can be further decomposed into subprocesses and/or process elements. See Process, Process description and Process element
Subprogram	A separately compilable, executable component of a computer program. Note that this term is defined differently in various programming languages. See Coroutine, Main program, Routine and Subroutine.
Subroutine	A routine that returns control to the program or subprogram that called it. Note that this term is defined differently in various programming languages. See Module.
Subroutine trace	A record of all or selected subroutines or function calls performed during the execution of a computer program and, optionally, the values of parameters passed to and returned by each subroutine or function
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
Sufficient evidence	The measure of the quantity of audit evidence, supports all material questions to the audit objective and scope *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. *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 *Scope Notes:* Refer to COBIT 5 information quality goals
Supervised learning	A type of machine learning algorithm in which a system is taught to classify input into specific, known classes
Supervisory authority	An independent public authority
Supervisory control and data acquisition (SCADA)	Systems used to control and monitor industrial and manufacturing processes and utility facilities
Supplier	An entity having an agreement with an acquirer to design, develop, manufacture, maintain, modify, deliver or supply solutions under terms of an agreement. Examples include individuals, partnerships, companies, corporations, and associations. See Acquirer
Supplier deliverable	An item to be provided to an acquirer or other recipient as specified in an agreement. The item can be a document, hardware or software item, service, solution, or any type of work product.

TERM	DEFINITION
Supply chain management (SBx)	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
Support software	Software that aids in the development and maintenance of other software, e.g., compilers, loaders and other utilities
Support vector machine	A supervised learning algorithm used for classification and regressions tasks
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.
Sustainment appraisal	A consistent and reliable assessment method that is a type of benchmark appraisal with reduced sampling. A sustainment appraisal can only be performed if eligibility requirements are met. This includes clear and repeatable process steps that when followed are capable of achieving high accuracy and reliable appraisal results through the collection of objective evidence (OE) from multiple sources. A maturity level (ML) profile or capability level (CL) profile must be produced as part of this appraisal process and allows Appraisal Sponsors to compare an organization's or project's process implementation with others. Like other appraisal methods, sustainment appraisals identify opportunities for improving both process implementation and business performance.
Switches	A data link layer device that enables local area network (LAN) segments to be created and interconnected, giving the added benefit of reducing collision domains in Ethernet-based networks
Symmetric cipher	An algorithm that encrypts data using a single key. In symmetric cryptographic algorithms, a single key is used for encipherment (encrypting) and decipherment (decrypting).
Symmetric key encryption	A 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 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	A term that means occurring at regular, timed intervals, i.e., timing dependent
Synchronous transmission	Block-at-a-time data transmission
Syntax	The structural or grammatical rules that define how symbols in a language are to be combined to form words, phrases, expressions and other allowable constructs
System	**1.** People, machines and methods organized to accomplish a set of specific functions **2.** A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support or mission requirement. (DOD)

TERM	DEFINITION
System analysis	A systematic investigation of a real or planned system to determine its functions and how they relate to each other and any other system See Requirements phase
System design	A process of defining the hardware and software architecture, components, modules, interfaces and data for a system to satisfy specified requirements See Design phase, Architectural design and Functional design
System design review	A review conducted to evaluate the manner in which the requirements for a system have been allocated to configuration items, the system engineering process that produced the allocation, the engineering planning for the next phase of the effort, manufacturing considerations and the planning for production engineering Source: IEEE See Design review
System development life cycle (SDLC)	The phases deployed in the development or acquisition of a software system *Scope Notes:* SDLC is an approach used to plan, design, develop, test and implement an application system or major modification to an application system. Typical phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and postimplementation review but not the service delivery or benefits realization activities.
System documentation	The collection of documents that describe the requirements, capabilities, limitations, design, operation and maintenance of an information processing system Source: ISO See Specification, Test documentation and User's guide
System exit	Special system software features and utilities that allow the user to perform complex system maintenance *Scope Notes:* The 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 hardening	A process to eliminate as much security risk as possible by removing all nonessential software programs, protocols, services and utilities from the system
System integration	The progressive linking and testing of system components into a complete system Source: ISO See Incremental integration
System life cycle	The course of developmental changes through which a system passes from its conception to the termination of its use, e.g., the phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance and modification of a system See Software life cycle
System narrative	An overview explanation of system flowcharts, including key control points and system interfaces

TERM	DEFINITION
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
System software	**1.** Application-independent software that supports the running of application software **2.** Software designed to facilitate the operation and maintenance of a computer system and its associated programs, e.g., operating systems, assemblers and utilities. This contrasts with application software. See Support software
System testing	Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements *Scope Notes:* System test procedures are typically 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
Systems engineering	An interdisciplinary approach governing the technical and managerial effort required to transform a set of customer needs, expectations and constraints into solutions and to support solutions throughout their life cycle
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.
T-distribution	A variation on normal distribution that accounts for the fact that only a sampling of all the possible values is being used instead of all of them
Table look-up	Used to ensure that input data agree with predetermined criteria stored in a table
Tableau	A commercial data visualization package often used in data science projects
Tailoring	Developing or adapting a process description or work product according to organizational defined standard guidelines to achieve a result. For example, a project develops its tailored process from the organization’s set of standard processes to meet objectives and constraints within the project environment. See Organization’s set of standard processes and Process description
Tailoring guidelines	Organizational guidelines that enable individuals, projects, and organizational functions to appropriately adapt standard processes for their use. Tailoring guidelines may allow additional flexibility when dealing with less critical processes or those that only indirectly affect business objectives. See Organization’s set of standard processes and Tailoring
Tangible asset	Any assets that have physical form
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
Target	Person or asset selected as the aim of an attack

TERM	DEFINITION
Target wake time (TWT)	A set time interval in which a device can receive communications from other devices
TB	Terabyte
Tcpdump	A network monitoring and data acquisition tool that performs filter translation, packet acquisition and packet display
Technical data package	A set of work products and information used to implement the design, e.g., coding standards, version control information, and engineering drawings
Technical infrastructure security	Refers to the security of the infrastructure that supports the enterprise resource planning (ERP) networking and telecommunications, operating systems, and databases
Technical performance	Characteristic of a process or solution generally defined by a functional or technical requirement that is often recorded in a contract or statement of work
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
Technology stack	The underlying elements used to build and run an application
Telecommunications	Electronic communication by special devices over distances or around devices that preclude direct interpersonal exchange
Teleprocessing	Using telecommunications facilities for the 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.
TensorFlow	A large-scale, distributed, machine-learning platform
Terabyte	Approximately one-trillion bytes; precisely 2^{40} or 1,099,511,627,776 bytes See Kilobyte, Megabyte and Gigabyte.
Terminal	A device, usually equipped with a CRT display and keyboard, used to send and receive information to and from a computer via a communication channel
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	An activity in which a system or component is executed under specified conditions, the results are observed or recorded and an evaluation is made of some aspect of the system or component
Test case	Documentation specifying inputs, predicted results and a set of execution conditions for a test item
Test case generator	A software tool that accepts as input source code, test criteria and specifications or data structure definitions, then uses these inputs to generate test input data and, sometimes determines expected results Synonymous with test data generator and test generator

TERM	DEFINITION
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 design	Documentation specifying the details of the test approach for a software feature or combination of software features and identifying the associated tests See Testing functional; Cause effect graphing; Boundary value analysis; Equivalence class partitioning; Error guessing; Testing, structural; Branch analysis; Path analysis; Statement coverage; Condition coverage; Decision coverage and Multiple-condition coverage.
Test documentation	Documentation describing plans for, or results of, the testing of a system or component. Types include test case specification, test incident report, test log, test plan, test procedure and test report.
Test driver	A software module used to invoke a module under test and, often, provide test inputs, control and monitor execution, and report test results Synonymous with test harness
Test generators	Software used to create data for use in the testing of computer programs
Test item	A software item that is the object of testing
Test log	A chronological record of all relevant details about the execution of a test
Test phase	The period of time in the software life cycle in which the components of a software product are evaluated and integrated, and the software product is evaluated to determine whether or not requirements have been satisfied
Test plan	Documentation specifying the scope, approach, resources and schedule of intended testing activities. It identifies test items, the features to be tested, the testing tasks, responsibilities, required resources and any risk requiring contingency planning. See Test design and Validation protocol.
Test procedure	A formal document developed from a test plan that presents detailed instructions for the setup, operation and evaluation of the results for each defined test See Test case.
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 readiness review	**1.** A review conducted to evaluate preliminary test results for one or more configuration items; to verify that the test procedures for each configuration item are complete, comply with test plans and descriptions, and satisfy test requirements; and to verify that a project is prepared to proceed to formal testing of the configuration items **2.** A review, as in definition 1, for any hardware or software component Contrasts with code review, design review, formal qualification review and requirements review
Test report	A document describing the conduct and results of the testing carried out for a system or system component
Test scripts	A set of instructions to be performed on a system or program to test functionality and anticipated output

TERM	DEFINITION
Test set	The subset of the data set used to test a model after the model has gone through initial vetting by the validation set
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 realtime recovery process
Testability	**1.** The degree to which a system or component facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met **2.** The degree to which a requirement is stated in terms that permit establishment of test criteria and performance of tests to determine whether those criteria have been met See Measurable.
Testing	**1.** The examination of a sample from a population to estimate characteristics of the population **2.** In machine learning (ML), evaluating the performance and robustness of models with the aim of assessing the model's generalization ability and identifying potential issues such as overfitting or underfitting
Testing, acceptance	Testing conducted to determine whether a system satisfies its acceptance criteria and to enable the customer to determine whether to accept the system. Contrasts with testing, development and testing, operational.
Testing, alpha	Acceptance testing performed by the customer in a controlled environment at the developer's site. The software is used by the customer in a setting approximating the target environment, with the developer observing and recording errors and usage problems. Source: Pressman.
Testing, beta	**1.** Acceptance testing performed by the customer in a live application of the software, at one or more end-user sites, in an environment not controlled by the developer. Source: Pressman **2.** For medical device software, such use may require an Investigational device exemption [IDE] or Institutional Review Board [IRB] approval.
Testing, boundary value	A testing technique using input values just below and just above the defined limits of an input domain, and with input values causing outputs to be just below and just above the defined limits of an output domain See Boundary value analysis and Testing, stress.
Testing, branch	Testing technique to satisfy coverage criteria that require each possible branch (outcome) to be executed at least once for each decision point. Contrasts with testing, path and testing, statement. See Branch coverage.
Testing, compatibility	The process of determining the ability of two or more systems to exchange information. In a situation where the developed software replaces an already working program, an investigation should be conducted to assess possible comparability problems between the new software and other programs or systems. See Different software system analysis, testing, integration and testing, interface.

TERM	DEFINITION
Testing, design based functional	The application of test data derived through functional analysis that is extended to include design functions and requirement functions Source: NBS See Testing, functional.
Testing, development	Testing conducted during the development of a system or component, usually in the development environment, by the developer. Contrasts with testing, acceptance and testing, operational.
Testing, functional	**1.** Testing that ignores the internal mechanism or structure of a system or component and focuses on the outputs generated in response to selected inputs and execution conditions **2.** Testing conducted to evaluate the compliance of a system or component with specified functional requirements and corresponding predicted results Synonymous with black-box testing and input/output driven testing. Contrasts with testing, structural.
Testing, integration	An orderly progression of testing in which software elements, hardware elements or both are combined and tested to evaluate their interactions, until the entire system has been integrated
Testing, interface	Testing to evaluate whether systems or components pass data and control correctly to one another. Contrasts with testing, unit and testing, system. See Testing, integration.
Testing, invalid case	A testing technique using erroneous (invalid, abnormal or unexpected) input values or conditions See Equivalence class partitioning.
Testing, operational	Testing to evaluate a system or component in its operational environment. Contrasts with testing, development and testing, acceptance. See Testing, system.
Testing, parallel	Testing a new or an altered data processing system with the same source data used in another system. The other system is considered as the standard of comparison. Synonymous with parallel run
Testing, path	Testing to satisfy coverage criterion that each logical path through the program be tested. Often, paths through the program are grouped into a finite set of classes. One path from each class is then tested. Synonymous with path coverage. Contrasts with testing, branch; testing, statement; branch coverage; condition coverage; decision coverage; multiple condition coverage and statement coverage.
Testing, performance	Functional testing to evaluate the compliance of a system or component with specified performance requirements
Testing, regression	Rerunning test cases that a program has previously executed correctly to detect errors spawned by changes or corrections made during software development and maintenance
Testing, special case	A testing technique using input values that seem likely to cause program errors, e.g., 0, 1, NULL and empty string See Error guessing.
Testing, statement	Testing to satisfy the criterion that each statement in a program be executed at least once during program testing. Synonymous with statement coverage. Contrasts with testing, branch; testing, path; branch coverage; condition coverage; decision coverage; multiple condition coverage and path coverage.
Testing, storage	A determination of whether certain processing conditions use more storage (i.e., memory) than estimated

TERM	DEFINITION
Testing, stress	Testing to evaluate a system or component at or beyond the limits of its specified requirements. Synonymous with testing, boundary value.
Testing, system	The process of testing an integrated hardware and software system to verify that the system meets its specified requirements. Such testing may be conducted in the development environment and the target environment.
Testing, unit	**1.** Testing of a module for typographic, syntactic and logical errors; for correct implementation of its design; and for satisfaction of its requirements **2.** Testing to verify the implementation of the design for one software element, e.g., a unit or module, or a collection of software elements Source: IEEE Synonymous with component testing.
Testing, usability	Tests designed to evaluate the machine/user interface. Determines if the communication devices are designed in a manner so that the information displayed is understandable, enabling the operator to correctly interact with the system
Testing, valid case	A testing technique using valid (normal or expected) input values or conditions See Equivalence class partitioning.
Testing, volume	Testing designed to challenge the ability of a system to manage the maximum amount of data over a period of time. This type of testing also evaluates the ability of a system to handle overload situations in an orderly fashion.
Testing, worst case	Testing that encompasses upper and lower limits and circumstances that pose the greatest chance of finding errors. Synonymous with most appropriate challenge conditions. See Testing, boundary value; Testing, invalid case; Testing, special case; Testing, stress and Testing, volume.
Text generation	The process of creating new text sequences using generative models capable of generating coherent and contextually relevant text
Text summarization	The process of automatically generating a concise version of a given text, capturing the key points and main ideas, using techniques like sentence extraction, keyword identification, and information compression
Third party	A natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data
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
Thread Protocol	An IEEE 802.15.4-based protocol for IPv6 over low-power wireless personal area networks (6LoWPAN)
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.

TERM	DEFINITION
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
Threat intelligence	Threat intelligence, or cyber threat intelligence, is information an organization uses to understand the threats that have, will, or are currently targeting the organization. This information is used to prepare, identify, and prevent security and cybersecurity threats looking to take advantage of valuable resources.
Threat intelligence analysis	The application of individual and collective methods to analyze data and test hypotheses within various organizational or solution contexts. Threat intelligence data is extracted from multiple data sources, some of which will be deliberately deceptive. The threat intelligence analyst must analyze, isolate, separate, and sort the data to determine truth from deception. Although this discipline is found in its purest form inside national intelligence agencies, its methods are also applied and used for business or competitive intelligence. *Source: CMMC/NIST 800 171B and CSF*
Threat intelligence systems	Systems that perform threat intelligence
Threat vector	The path or route used by the adversary to gain access to the target
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.
Thundering herd	Loss of service resulting from a lapse in connectivity that causes devices to simultaneously attempt reconnection
Time series data	Time series data have measurements of observations accompanied by datetime stamps
Timelines	Chronological graphs where events related to an incident can be mapped to look for relationships in complex cases *Scope Notes:* Timelines can provide simplified visualization for presentation to management and other nontechnical audiences.
Timely information	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 *Scope Notes:* Refer to COBIT 5 information quality goals
Token	**1.** In security systems, a physical device that is used to authenticate a user, typically in addition to a username and password; in programming languages, a single element of the language **2.** In natural language processing (NLP), a unit of data representing individual words, subwords, or characters typically used as input for models
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.
Tokenization	The process of breaking down text or data into smaller units

TERM	DEFINITION
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' judgment about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the professionals are willing to accept.
Tolerable risk	Risk that is within a tolerable or acceptable range, based on management's appetite
Toolchain	The portfolio of tools and technologies used by DevOps practitioners to automate and enable the DevOps practices.
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
Touch screen	A touch-sensitive display screen that uses a clear panel over or on the screen surface. The panel is an input device, a matrix of cells that transmits pressure information to the software.
Traceability	**1.** The degree to which a relationship can be established between two or more products of the development process, especially products having a predecessor-successor or master-subordinate relationship to one another, e.g., the degree to which the requirements and design of a given software component match See Consistency. **2.** The degree to which each element in a software development product establishes its reason for existing, e.g., the degree to which each element in a bubble chart references the requirement that it satisfies See Traceability analysis and Traceability matrix.
Traceability analysis	The tracing of: **1.** Software requirements specifications to system requirements in concept documentation **2.** Software design descriptions to software requirements specifications and software requirements specifications to software design descriptions **3.** Source code to corresponding design specifications and design specifications to source code Analyze identified relationships for correctness, consistency, completeness and accuracy See: Traceability and Traceability matrix.
Traceability matrix	A matrix that records the relationship between two or more products, e.g., a matrix that records the relationship between the requirements and the design of a given software component See Traceability and Traceability analysis.
Trade study	An evaluation of alternatives based on criteria and systematic analysis, to select the best alternative for attaining determined objectives
Trademark	A sound, color, logo, saying or other distinctive symbol closely associated with a certain product or company
Training	The process of determining the ideal parameters comprising a model
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.

TERM	DEFINITION
Transaction (IT) (IT)	**1.** A command, message or input record that explicitly or implicitly calls for a processing action, such as updating a file **2.** An exchange between an end user and an interactive system **3.** In a database management system, a unit of processing activity that accomplishes a specific purpose, such as a retrieval, an update, a modification or a deletion of one or more data elements of a storage structure
Transaction analysis	A structured software design technique, deriving the structure of a system from analyzing the transactions that the system is required to process
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 similar to electronic vaulting except that instead of transmitting several transaction batches daily, the archive logs are shipped as they are created
Transfer learning	A process that uses knowledge gained from solving one task to improve performance on another related task, typically by transferring learned representations or parameters from a pretrained model to a new model trained for a different but related task
Transformer	An artificial intelligence (AI) model architecture that uses “attention” to collect relationships in data, particularly language. It processes information all at once, leading to faster learning and tasks like translation and text generation.
Translation	Converting from one language form to another Source: NIST See Assembling, Compilation and Interpret.
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 (email), 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.
Transport Layer Security (TLS)	A cryptographic protocol that provides secure communications, endpoint security and privacy on the Internet
Trap door	Unauthorized electronic exit, or doorway, out of an authorized computer program into a set of malicious instructions or programs
Triple DES (3DES)	A block cipher created from the Data Encryption Standard (DES) cipher by using it three times. 3DES was broken in 2016.
Trojan horse	Purposefully hidden malicious or damaging code within an authorized computer program
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

TERM	DEFINITION
Tunnel	The paths that the encapsulated packets follow in an Internet virtual private network (VPN)
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 an AH or ESP header and an additional IP header.
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
Turing-complete	A computational term meant to describe a system that can successfully be used as a Turing Machine, i.e., a system whose programming language can simulate what another programming language can accomplish
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 both a smart card and a password), typically the combination of something you know, are or have
UIMA	A framework used to analyze unstructured information, especially natural language. OASIS Unstructured Information Management Architecture (UIMA) is a specification that standardizes this framework, and Apache UIMA is an open-source implementation of it.
Unambiguous	**1.** A term that means not having two or more possible meanings **2.** A term that means not susceptible to different interpretations **3.** A term that means not obscure or vague **4.** A term that means clear, definite and certain
Uncertainty	The difficulty of predicting an outcome due to limited knowledge of all components
Underfitting	When a machine learning (ML) model is too simple to capture the complexities and underlying structure of the data, resulting in poor performance for both the training and text data
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.
Uniform resource locator (URL)	The string of characters that form a web address
Uninterruptible power supply (UPS)	A type of power supply that provides short-term backup power from batteries to a computer system when the electrical power fails or drops to an unacceptable voltage level
Unit	**1.** A separately testable element specified in the design of a computer software element **2.** A logically separable part of a computer program. It is synonymous with "component" and "module." Synonymous with component and module

TERM	DEFINITION
Unit testing	**1.** A testing technique used to test program logic within a particular program or module (ISACA) *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. **2.** Testing of individual hardware or software units
Universal description, discovery and integration (UDDI)	A web-based version of the traditional telephone book's yellow and white pages that enables businesses to be publicly listed and promotes 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 to up to 127 peripheral devices.
UNIX	A multitasking, multiple-user (time-sharing) operating system developed at Bell Labs to create a favorable environment for programming research and development
Unlinkability	A condition of privacy-relevant data that cannot be linked (i.e., related) across domains
Unsupervised learning	A class of machine-learning algorithms designed to identify groupings of data without knowing what the groups will be in advance
Untrustworthy host	A host that cannot be protected by the firewall. As a result, 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.
Upfade	A byproduct of multipath whereby the RF signal takes multiple paths and results in stronger signal strength
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.
Usability	The ease with which a user can learn to operate, prepare inputs for and interpret outputs of a system or component
User	Any person, organization or functional unit that uses the services of an information processing system See End user
User acceptance testing (UAT)	A type of functional testing that validates the results of the development phase where software is tested by the intended audience or business representative (from Stanford University)
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
User entity and behavioral analytics (UEBA)	The process of monitoring an account for abnormal activity and atypical usage to identify patterns (heuristics) that highlight user activity trends. UEBA can act as a proactive access control mechanism by identifying threat indicators, alerting on malicious behavior earlier and improving threat intelligence.
User interface impersonation	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

TERM	DEFINITION
User mode	A 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
User's guide	Documentation that describes how to use a functional unit and may include a description of the rights and responsibilities of the user, the owner and the supplier of the unit. It is synonymous with "user manual" and "operator manual."
Utility program	A computer program that generally supports the processes of a computer, e.g., a diagnostic program, a trace program and a sort program
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 or routines designed to perform some general support function required by other application software, the operating system or the system users. They perform general functions, such as formatting electronic media, making copies of files or deleting files.
Utility token	Digital assets or tokens created and utilized to finance the creation of a network by providing its buyers with the ability to use some of the network ecosystem or products. They do not give any legal or economic right of ownership over the developer or any part of the ecosystem.
V&V	The acronym for verification and validation
Vaccine	A program designed to detect computer viruses
Val IT	The standard framework for enterprises to select and manage IT-related business investments and IT assets by means of investment programs such that they deliver optimal value to the enterprise. It is based on COBIT.
Valid input	Test data that lies within the domain of the function that the program represents
Validate	A term that means to prove to be valid
Validation	The process of establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product meeting its predetermined specifications and quality attributes
Validation, process	The process of establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product meeting its predetermined specifications and quality characteristics Source: FDA
Validation, software	The process of determining the correctness of the final program or software produced from a development project with respect to the user's needs and requirements. Validation is usually accomplished by verifying each stage of the software development life cycle. See Verification, software
Validation, verification and testing	Techniques used as an entity to define a procedure of review, analysis and testing throughout the software life cycle to discover errors, determine functionality and ensure the production of quality software Source: NIST
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

TERM	DEFINITION
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 and COBIT 2019 perspective
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	A name, label, quantity or data item whose value may be changed many times during processing. This contrasts with constant.
Variable sampling	A sampling technique used to estimate the average or total value of a population based on a sample. It is a statistical model used to project a quantitative characteristic, such as a monetary amount.
Variable trace	A record of the name and values of variables accessed or changed during the execution of a computer program. It is synonymous with data-flow trace, data trace and value trace. Source: IEEE See Execution trace, Retrospective trace, Subroutine trace and Symbolic trace
Variance	**1.** The measure of how much a list of numbers varies from the mean (average) value. It is frequently used in statistics to measure how large the differences are in a set of numbers. It is calculated by averaging the squared difference of every number from the mean. **2.** In artificial intelligence (AI), the measure of how much the model varies when it is trained on different subsets of the training data. A model with high variance is very sensitive to the training data and might tend to overfit.
Vaults	A secure environment to store critical data that is isolated from production and backup storage environments to limit exposure to cyberthreats
Vector	An ordered set of real numbers, each denoting a distance on a coordinate axis. These numbers may represent a series of details about a single person, movie, product or the entity being modeled.
Vector space	A collection of vectors, e.g., a matrix
Vectorization	The process of representing input data as an array of vectors that can be processed by a machine learning (ML) algorithm or model
Vendor	A person or an organization that provides software, hardware, firmware and/or documentation to the user for a fee or in exchange for services, e.g., a medical device manufacturer
Verifiable	A term that means can be proved or confirmed by examination or investigation See Measurable
Verification	Checks that data is entered correctly
Verification, software	In general, the demonstration of consistency, completeness and correctness of the software at each stage and between each stage of the development life cycle Source: NBS See Validation, software
Verification-based appraisal	An appraisal in which the appraisal team focuses on verifying the set of objective evidence provided by the appraised organization in advance in order to reduce the amount of discovery during the appraisal onsite period See Discovery-based appraisal

TERM	DEFINITION
Verify	**1.** A term that means to determine whether a transcription of data or other operation has been accomplished accurately Source: ANSI **2.** A term that means to check the results of data entry, e.g., keypunching **3.** A term that means to prove to be true by demonstration
Version	An initial release or a complete rerelease of a software item or software element See Release
Version control	A practice that identifies the correct versions of work products and ensures they are available for use or for restoring to a previous version. It also includes the establishment and maintenance of baselines and the identification of changes to baselines to obtain previous baselines.
Version number	A unique identifier used to identify software items and related software documentation that are subject to configuration control
Vertical defense in depth	A strategy where controls are placed at different system layers, including hardware, operating system, application, database or user levels
View	A selection of model components relevant to the organization or user. Two primary types of views currently exist: • Predefined view: A logical grouping of predefined CMMI model components used to define the appraisal model view scope. Examples include CMMI-DEV Maturity Level 2 and CMMI-SVC Maturity Level 5. • Customized view: Any combination of capability areas, practice areas, practice groups or practices that are defined by the end user. Customized views are defined to be relevant to business objectives. See Benchmark model view
Virtual appraisal	Any appraisal (benchmark, evaluation, sustainment or APR) where ***any*** appraisal activity is performed virtually or remotely by the Appraisal Team Leader or appraisal team
Virtual currency	Digital representations of value, not created or issued by a central bank or sovereign state, which can be used as a method of exchange
Virtual face-to-face (F2F)	A meeting over a remote or virtual platform such as Teams, Zoom, FaceTime, etc., where the participants can actively, clearly and continually see and hear each other on camera with audio
Virtual local area network (VLAN)	Logical segmentation of a LAN into different broadcast domains *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 even though the devices are located on different LAN segments. A VLAN is based on logical rather than physical connections.
Virtual machine (VM)	An emulation of a computing environment or operating system separate from the host computing system
Virtual machine (VM) jumping (VM)	Exploitation of a hypervisor that allows an attacker to gain access to one virtual machine from another
Virtual organizations	An organization that has no official physical site presence and is made up of diverse, geographically dispersed or remote 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 enterprise, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that passes between two Internet points, maintaining privacy and security.

TERM	DEFINITION
Virtual private network (VPN) concentrator (VPN)	A system used to establish VPN tunnels and handle large numbers of simultaneous connections. This system provides authentication, authorization and accounting services.
Virtual reality	Computer-generated simulations that present the user with an altered reality. VR users typically wear a headset and hold a hand controller while experiencing an immersive recreation of a real or imaginary environment that masks their actual environment.
Virtual solution delivery	A solution that includes the use of virtual, remote or hybrid methods to deliver a given service, process, activity, task or solution to customers and affected stakeholders. For context, the terms virtual delivery and remote delivery are used interchangeably.
Virtualization	The process of adding a guest application and data onto a virtual server, recognizing that the guest application will ultimately be removed from the physical server
Virus	A piece of code that can replicate itself and spread from one computer to another. It requires intervention or execution to replicate and/or cause damage. See Bomb, Trojan horse and Worm
Virus signature	The file of virus patterns that are compared to existing files to determine whether they are infected with a virus or worm
Virus signature file	The file of virus patterns that are compared to existing files to determine whether they are infected with a virus or worm
VMS	The acronym for virtual memory system
Voice mail	A system of storing messages in a private recording medium to allow the called party to retrieve the messages later
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 any dedicated Internet Protocol (IP) network instead of over dedicated voice transmission lines
Volatile data	Data that changes frequently and can be lost when the system power is shut down
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 occurs. Note that this increase in vulnerability can result from changes in control conditions or threat capability/force. *Scope Notes:* From Jones, J.; "FAIR Taxonomy," Risk Management Insight, USA, 2008
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
Wallet	An application or other service that gives holders of cryptocurrency the ability to store and retrieve their digital assets. Such wallets come in many forms, including hot wallets (any wallet application or service connected to the Internet) and cold wallets (or cold storage, often hardware devices that can be disconnected from the Internet or other electronic services).
War dialer	Software packages that sequentially dial telephone numbers, recording any numbers that answer
Warm site	A site that is 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

TERM	DEFINITION
Waterfall model	A model of the software development process in which the constituent activities, typically a concept phase, requirements phase, design phase, implementation phase, test phase, installation and checkout phase, and operation and maintenance, are performed in that order, possibly with overlap but with little or no iteration. It contrasts with incremental development, rapid prototyping and spiral model.
Weakness	A type of preliminary or final finding, which involves an ineffective, or nonexistent, implementation of one or more processes that meet the intent and value of a practice based on verified objective evidence. It is applicable across the project(s) and organizational support functions or organizational unit as a whole. This is realized if a) the process itself does not address a CMMI practice requirement or b) the project(s) or organizational support functions are not following their process that is compliant with the intent and value of the applicable CMMI practice.
Web application firewalls	A buffer used between a web application and the Internet to mitigate cyberattacks
Web hosting	The business of providing the equipment and services required to host and maintain files for one or more web sites and providing fast Internet connections to those sites *Scope Notes:* Most hosting is "shared," which means that web sites for 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 contracted with the enterprise.
Web server	End-point hardware or software that serves web pages to users
Web Services Description Language (WSDL)	A language formatted with extensible markup language (XML). It is 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	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.
Webapp security tools	Open-source tools used to identify threats to applications and data
Weight	A coefficient for a feature in a linear model or an edge in a deep network
Weka	An open-source set of command line and graphical user interface data analysis tools developed at the University of Waikato in New Zealand
Well-known ports	Ports controlled and assigned by the Internet Assigned Numbers Authority (IANA). On most systems, they can be used only by system (or root) processes or 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 0-1023.
White box testing	A testing approach that uses knowledge of a program/module’s underlying implementation and code intervals to verify its expected behavior
Wi-Fi HaLow	An IEEE 802.11 modification that uses license-exempt 900 MHz bands to extend the WiFi connectivity range up to 1 kilometer

TERM	DEFINITION
Wi-Fi Protected Access (WPA)	A class of security protocols used to secure wireless (Wi-Fi) computer networks
Wi-Fi Protected Access II (WPA2)	A 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.
Wide area network (WAN)	A computer network connecting multiple offices or buildings over a larger area
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.
Width	The number of neurons in a particular layer of a neural network
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 network users from each other), hence the name. Cryptoanalysts identified several serious weaknesses, 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). This involves those technologies converging around IEEE 802.11 and 802.11b and radio band services used by mobile devices.
Wireless local area network (WLAN)	A wireless communication network that serves several users within a specified limited geographic area
Wiretapping	The practice of eavesdropping on information being transmitted over telecommunications links
Work Breakdown Structure (WBS)	A list of tasks and activities, related work elements and their relationship to each other and the end product or service
Work product	An output from a process, activity or task that may be stand-alone or part of a solution
Work product and task attributes	Characteristics of solutions and tasks used to estimate work. These characteristics often include size, complexity, weight, form, fit and function. Characteristics are typically used as one input to deriving other resource estimates, e.g., effort, cost, schedule. See Work product
Workaround	A sequence of actions the user should take to avoid a problem or system limitation until the computer program is changed. They may include manual procedures used in conjunction with the computer system.
Workgroup	A collection of people who work together closely on highly interdependent tasks to achieve shared objectives. A workgroup typically reports to a responsible individual who may be involved in managing its daily activities. The operational parameters of workgroups can vary based on objectives and should, therefore, be clearly defined. Workgroups can operate as a project if designated accordingly.
World Wide Web (WWW)	A sub network of the Internet through which information is exchanged by text, graphics, audio and video

TERM	DEFINITION
World Wide Web Consortium (W3C)	Founded in 1994, an international consortium of affiliates from public and private organizations involved with the Internet and 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
WPA2	A 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.
WPA3	A wireless security protocol released in mid-2018 that improves on WPA2 by eliminating the preshared key (PSK), which is susceptible to dictionary attacks
Write blocker	A device 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 from being 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 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.
Z-Wave	A protocol that operates in the Part 15 unlicensed industrial, scientific and medical (ISM) band (approximately 900 MHz, depending on the location), giving it excellent barrier penetration and low power utilization. Z-Wave is similar to LoRa. It was originally developed by Zensys in 1999 for system on a chip (SoC) applications.
Zero trust	A security model anchored in the assumption of breach, which means that anything outside or inside the network cannot be trusted and anyone who tries to access the network needs to be verified in advance
Zero-day exploit	A vulnerability that is exploited before the software creator/vendor is aware of its existence. It may also refer to known flaws that do not have an available patch.
Zero-knowledge proof	A critical aspect of cryptography, a method by which one party (Party A) is able to prove to another party (Party B) that Party A is aware of the value of a specific variable without conveying any additional information about that variable other than that they know its value
Zero-trust architecture (ZTA)	A security model based on microsegmentation and the continuous validation of digital interactions to address the threat of lateral movement within a network. See also Zero trust.
Zigbee	An IEEE 802.15.4 personal area network (PAN) protocol developed in 1998 that aims to provide moderate throughput and reliable connectivity via a mesh topology (similar to Z-Wave)