Appendix 600A Glossary

This glossary is provided to clarify guidance in the *Federal Information System Controls Audit Manual* (FISCAM). When terminology differs from that used at an entity, auditors use professional judgment to determine if there is an equivalent term.

|  |  |
| --- | --- |
| **access agreement** | A user-based agreement that specifies user responsibilities when exchanging information or accessing information or systems that contain the exchanged information. Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. |
| **access control list** | A register of (1) users (including groups of users, devices, and processes) that have permission to use a particular system resource and (2) the types of access they have been permitted. |
| **access control software** | A type of software external to the operating system that provides a means of specifying the users (including groups of users, devices, and processes) that have access to a system, including specific system resources, and the capabilities authorized users are granted. Access control software can generally be implemented in different modes that provide varying degrees of protection, such as denying access for which the user is not expressly authorized, allowing access that is not expressly authorized but providing a warning, or allowing access to all resources without warning regardless of authority. |
| **access controls** | A control category within the FISCAM Framework that relates to limiting access or detecting inappropriate access to information resources (e.g., data and information technology) and facilities, thereby protecting these resources against unauthorized modification, loss, and disclosure. See also logical access control and physical access control. |
| **access path** | The logical route that an end user request takes through hardware and software components to access computer-processed information. An access path typically includes any information system component capable of enforcing access restrictions or any component that could be used to bypass an access restriction, including the telecommunications software, transaction processing software, and application software. |
| **access privileges** | Precise statements that define the extent to which users, programs, or workstations can access computer systems and use or modify (e.g., read, write, execute, create, and delete) the programs and data on a system, and under what circumstances this access will be allowed. |
| **account management** | Involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions. |
| **accountability** | The security goal that generates the requirement for an entity’s actions to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. |
| **accuracy** | An information processing objective that aims to provide reasonable assurance that data relating to transactions and events are appropriately and timely recorded. |
| **alternate processing site** | A site geographically distinct from primary processing sites that provides processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. |
| **alternate storage site** | A site geographically distinct from primary storage sites that maintains duplicate copies of information and data if the primary storage site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. |
| **alternate worksite** | Entity-authorized work from home (or other designated location) or at geographically convenient satellite offices (e.g., telecommuting, teleworking, or remote working). |
| **application** | A combination of application software, system software, and hardware designed and implemented to serve a particular function. |
| **application controls** | One of the three types of information system controls that are incorporated directly into application software to control the input, processing, and output of data. These controls are designed to achieve information processing objectives—completeness, accuracy, and validity of transactions and data. Application control is also known as business process application controls. |
| **application software** | Software designed to serve a particular function that has specific input, processing, and output requirements. Application software uses database management software to store and retrieve application data. Application software relies on system software to run. |
| **approach** | The nature, timing, and extent of audit procedures applied to the significant business processes and areas of audit interest based on the relevant control objectives and the relevant IS controls. |
| **appropriateness** | The measure of the quality of evidence that encompasses the relevance, validity, and reliability of evidence used for addressing the engagement objectives and supporting findings and conclusions. |
| **areas of audit interest** | A subset of the entity’s information systems that, based on their significance to the engagement objectives, the auditor includes in the scope of the information system (IS) controls assessment. At the business process level, areas of audit interest may include business process applications, process automation software, system interfaces, data management systems, specific data files, and system-generated reports. At the system level, areas of audit interest may include operating systems, access control software, and hardware devices used for information processing, data storage, and network communications. |
| **assessor** | An individual responsible for conducting security and privacy assessment activities under the guidance and direction of a designated authorizing official. For cloud services, the individual is an independent third party. |
| **attack** | Attempt to gain unauthorized access to an information system’s services, resources, or information, or an attempt to compromise an information system’s integrity, availability, or confidentiality. |
| **attribute** | Any distinctive feature, characteristic, or property of an object that can be identified or isolated quantitatively or qualitatively by either human or automated means. |
| **attribute sampling** | Statistical sampling that reaches a conclusion about a population in terms of a rate of occurrence. |
| **audit logging** | Recording a chronological record of system activities, including records of system accesses and operations performed in a period. |
| **audit plan** | Audit documentation that describes (1) the nature and extent of planned audit procedures for the planning phase of the IS controls assessment; (2) the nature, timing, and extent of planned audit procedures for the testing of relevant IS controls for each area of audit interest; and (3) other planned audit procedures that are required to be carried out so that the engagement complies with generally accepted government auditing standards. |
| **audit procedure** | The specific steps and tests auditors perform to address the engagement objectives. Specific tests include inquiry, observation, and inspection. See also walk-through. |
| **audit record** | An individual entry in an audit log related to an audited event. |
| **audit risk** | The possibility that the auditors’ findings, conclusions, recommendations, or assurance may be improper or incomplete. The assessment of audit risk involves both quantitative and qualitative considerations. |
| **audit trail** | A chronological record showing user access and activity or security-related event in an information system during a given period. |
| **authentication** | Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. |
| **authenticator** | The means used to confirm the identity of a user, process, or device (e.g., passwords, tokens, biometrics, key cards, Public Key Infrastructure certificates, or multifactor authenticator). |
| **authenticity** | The property of being genuine, verifiable, and trusted and establishing confidence in the validity of a transmission, a message, or a message originator. |
| **authorization** | The official management decision given by a senior federal official to authorize operation of an information system and to explicitly accept the risk to entity operations (including mission, functions, image, or reputation), entity assets, individuals, other organizations, and the United States based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls that agency information systems inherit. Authorization is also known as authorization to operate and accreditation. |
| **authorization boundary** | Includes all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems to which the information system is connected. Authorization boundary is also known as accreditation boundary. |
| **authorizing official** | A senior federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to entity operations (including mission, functions, image, or reputation), entity assets, individuals, other organizations, and the United States. |
| **availability** | Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system. |
| **backup** | A copy of files and programs made to facilitate recovery if necessary. |
| **baseline configuration** | A documented set of specifications for an information system or a configuration item within a system that has been formally reviewed and agreed on at a given point in time and can be changed only through change control procedures. |
| **biometric** | Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity of, an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. |
| **business process** | The primary means through which the entity accomplishes its mission. Business processes transform inputs into outputs through a series of transactions, activities, and events to achieve the entity’s operations, reporting, and compliance objectives. Business processes support the business functions the entity performs in accomplishing its mission. Financial management is one example of a business function. Financial management business processes include collections, disbursements, and payroll, as well as the related accounting applications. |
| **business process application** | An application that helps the entity perform a specific business process or related business processes within a business function. |
| **business process controls** | A control category within the FISCAM Framework that relates to the structure, policies, and procedures for the input, processing, storage, retrieval, and output of data that operate over individual transactions; activities across business processes; and events between business process applications, their components, and other systems. Business process controls include general controls that directly support information processing objectives. |
| **business process level** | The level at which user, application, and general controls relevant to specific business processes are implemented. These controls are specific to a business process and often correspond to information resources employed by the business process—business process applications, process automation software, system-generated reports, system interfaces, and data management systems. |
| **certificate** | A digital representation of information, which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber’s public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. |
| **certificate store** | Local storage on the computer where certificates are stored. The certificates stored could be issued from several different certification authorities. |
| **certification authority** | A trusted entity that issues and revokes public key certificates. |
| **certification path** | A chain of trusted public key certificates that begins with a certificate whose signature can be verified by a relying party using a trust anchor and ends with the certificate of the entity whose trust needs to be established. |
| **chief information officer** | Agency official responsible for  (1) providing advice and other assistance to the head of the executive entity and other senior management personnel of the executive entity to ensure that information technology is acquired and information resources are managed for entity in a manner consistent with statutes, regulations, executive orders, directives, implementing guidance, policies, and priorities established by the head of the entity;  (2) developing, maintaining, and facilitating the implementation of a sound, secure, and integrated IT architecture for the entity; and  (3) promoting the effective and efficient design and operation of all major information resources management processes for the executive entity, including improvements to the entity’s work processes. |
| **climate controls** | A subset of environmental protection controls that prevents or mitigates damage to facilities and interruptions in service. Thermostats and dehumidifiers are some examples of climate controls. |
| **code** | Computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler, or other translator. See also object code and source code. |
| **code analysis** | The act of analyzing source code with or without executing the code to identify poor coding practices that might introduce security flaws into code during the code development phase. |
| **collaborative computing** | Applications and technology (e.g., white boarding and group conferencing) that allow two or more individuals to share information in real time in an inter- or intra-enterprise environment. |
| **common control** | A security or privacy control that one or more information systems inherit. See also control inheritance. |
| **compensating control** | A control that reduces the risk of an existing or potential control weakness that could result in errors or omissions. |
| **compiler** | A program that translates source code into object code. |
| **complementary user-entity controls** | Controls that management of the service organization assumes, in the design of its service, will be implemented by user entities and are necessary to achieve the control objectives stated in management’s description of the service organization’s system. |
| **completeness** | An information processing objective that aims to provide reasonable assurance that all transactions and events that should have been recorded have been properly recorded. |
| **computer-assisted audit technique** | Any automated audit technique, such as audit software, test data generators, computerized audit programs, and special audit utilities. |
| **computer program** | Complete sets of ordered instructions that a computer executes to perform a specific operation or task. |
| **concept of operations** | Verbal and graphic statement, in broad outline, of an organization’s assumptions or intent regarding an operation or series of operations of new, modified, or existing information systems. |
| **confidence level** | The probability associated with the range of values into which an estimate of a population characteristic is expected to fall. |
| **confidentiality** | Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. |
| **configuration auditing** | Procedures for determining alignment between the implemented configuration settings of an information system and the corresponding baseline configuration settings. |
| **configuration control** | Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation. |
| **configuration control board** | A group of qualified people with responsibility for regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system. |
| **configuration item** | An information system component or an aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process. Configuration items are the information system components, such as the hardware, software, firmware, and documentation, that are placed under configuration management. |
| **configuration management** | A control category within the FISCAM Framework that relates to identifying and managing security features for all hardware, software, and firmware components of an information system at a given point that systematically controls changes to that configuration during the system’s life cycle. |
| **configuration settings** | The set of parameters (e.g., flags, settings, and paths) that can be changed in hardware, software, or firmware that affect the security posture and functionality of the information system. |
| **contingency plan** | A plan that is maintained for disaster response, backup operations, and post disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency. |
| **contingency planning** | A control category within the FISCAM Framework that provides for the continuation of critical or essential mission and business functions in the event of a system disruption, compromise, or failure and the restoration of the information system following a system disruption. |
| **continuity of operations plan** | A predetermined set of instructions or procedures that describe how an organization’s mission-essential functions will be sustained within 12 hours and for up to 30 days during a disaster event before returning to normal operations. |
| **continuous monitoring strategy** | Maintaining ongoing awareness to support organizational risk decisions. This can include the use of automated procedures to ensure that security controls are not circumvented or the use of tools to track actions taken by those suspected of misusing the information system. |
| **control activities** | One of the five components of internal control. Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity’s information system. |
| **control baseline** | A predefined set of minimum privacy or security controls for low-impact, moderate-impact, or high-impact information or information systems that may be tailored to address specific protection needs based on risk. |
| **control categories** | Control categories are broad groupings of controls based on similar types of risk. Control categories consist of the following: business process controls, security management, access controls, configuration management, segregation of duties, and contingency planning. |
| **control deficiency** | A condition when the design, implementation, or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct errors in information processing on a timely basis. The definition of control deficiency may differ by engagement type. For federal financial audits, control deficiencies exist when misstatements are unlikely to be prevented or detected and corrected on a timely basis. |
| **control dependency** | Exists when the effectiveness of a control depends on the effectiveness of other controls. |
| **control environment** | One of the five components of internal control. The control environment is the foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives. |
| **control inheritance** | A situation in which a system or application receives protection from controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application, entities either internal or external to the organization where the system or application resides. |
| **control objectives** | The aim or purpose of specified controls. Control objectives address the risks to achieving the critical elements. |
| **criteria** | The statutes, regulations, executive orders, implementing guidance, directives, policies, contracts, grant agreements, standards, measures, expected performance, defined business practices, defined benchmarks, or other guidance against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation of internal controls. Suitable criteria are relevant, reliable, objective, and understandable and do not result in the omission of significant information, as applicable, to the engagement objectives. |
| **critical elements** | Components of a control category that are necessary for maintaining adequate controls within the FISCAM control category. |
| **critical infrastructure** | System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. |
| **cryptographic key** | A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. Usually, a sequence of random or pseudorandom bits are used initially to set up and periodically change the operations performed in cryptographic equipment to encrypt or decrypt electronic signals, to determine electronic counter-countermeasures patterns, or to produce another key. |
| **data** | Facts and information that can be communicated and manipulated. |
| **data center** | A purpose-built, physically separate, and dedicated space that contains one or more racks of servers and high-performance computers; has a dedicated uninterruptable power supply, backup generator for prolonged power outages, or combination of both; and has a dedicated cooling system or zone. |
| **data communications** | The transfer of information from one computer to another through a communications medium, such as telephone lines, microwave relay, satellite link, or physical cable. |
| **data definition** | Identification of all fields in the database, how they are formatted, how they are combined into different types of records, and how the record types are interrelated. |
| **data file** | A collection of records stored in computerized form. |
| **data management system** | Includes databases, as well as the middleware, database management software, and data warehouse software, used to define, organize, maintain, and control access to data. |
| **data owner** | Official with statutory or operational authority for specified data and responsibility for establishing the controls for the data’s generation, collection, processing, dissemination, and disposal. |
| **data processing** | The collective set of data actions involved in the data life cycle, including data collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal. |
| **data strategy** | Plan used to identify data needed to support business processes. A clearly defined data strategy minimizes data redundancies, which is fundamental to an efficient, effective transaction processing function. |
| **database** | A repository of information or data, which may or may not be a traditional relational database system. |
| **database administrator** | The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application software and users to the database. Additional responsibilities include operation, performance, integrity, and security of the database. |
| **database management** | Tasks related to creating, maintaining, organizing, and retrieving information from a database. |
| **database management software** | Software designed to define, organize, maintain, and control access to data. Application software uses database management software to store and retrieve application data. Database management software depends on system software to run. Database management software is often referred to as a database management system, or DBMS. |
| **denial-of-service-attack** | Occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyberthreat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. These attacks can cost an organization both time and money while its resources and services are inaccessible. |
| **device lock** | A temporary action taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. |
| **dial-up access** | A means of connecting to another computer, or a network similar to the internet, over a telecommunications line using a modem-equipped computer. |
| **digital media** | A form of electronic media where data are stored in digital (as opposed to analog) form. |
| **digital signature** | Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation. |
| **direct general controls** | Those controls that apply to information systems used within the business process and directly support the effective operation of user and application controls. |
| **disaster recovery plan** | A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. |
| **encryption** | Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called decryption, which is a transformation that restores encrypted data to their original state. |
| **engagement objective** | What the engagement is intended to accomplish. Engagement objectives identify the audit subject matter and performance aspects to be included. Engagement objectives can be thought of as questions about the program that the auditors seek to answer based on evidence obtained and assessed against criteria. Engagement objectives may also pertain to the current status or condition of a program. |
| **entity level** | The level at which general controls relevant to the entire entity or component are implemented. These controls are broader than those applied at the system level and often correspond to the entity’s information security management program or most of its information systems. |
| **entity risk assessment** | One of the five components of internal control. Entity risk assessment is the assessment of the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. |
| **entry points** | Access points to the entity’s information systems. These may include remote access through dial-up, wireless devices, or the internet. |
| **environmental controls** | A subset of contingency planning general controls that prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies are some examples of environmental controls. |
| **event** | Any observable occurrence in a network or system. |
| **Federal Information Security Modernization Act of 2014** | A federal law enacted to, among other things, provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets (Pub. L. No. 113-283, 129 Stat. 3073 (Dec. 18, 2014)). This 2014 statute largely superseded the similar Federal Information Security Management Act of 2002, Pub. L. No. 107-347, title III,116 Stat. 2899, 2946 (Dec. 17, 2002). In particular, the 2014 statute amended the U.S. Code to establish a new subchapter on information security (44 U.S.C. §§ 3551-3558). In FISCAM, “FISMA” sometimes refers to both the 2014 statute and its 2002 predecessor collectively. |
| **field** | A location in a record in which a particular type of data are stored. In a database, this is smallest unit of data that can be named. |
| **file** | A collection of information logically grouped into a single entity and referenced by a unique name, such as a file name. |
| **Financial management systems** | Systems that include the financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. This is a statutory definition included in the Federal Financial Management Improvement Act of 1996 (FFMIA). |
| **firecall** | Any method established to provide emergency access to a secure information system. |
| **firewall** | Hardware and software components that protect one set of system resources (e.g., computers and networks) from attack by outside network users (e.g., internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users. |
| **firmware** | Software that is embedded in the read-only memory of hardware that enables the hardware to function and communicate with other software. |
| **flowchart** | A diagram of the movement of transactions, computer functions, media, and operations within a system. The processing flow is represented by arrows between symbolic shapes for operation, device, data file, and other categories to depict the system or program. |
| **fraud** | A type of illegal act involving the obtaining of something of value through willful misrepresentation. Whether an act is fraudulent is determined through the judicial or other adjudicative system and is beyond management’s professional responsibility for assessing risk. |
| **generally accepted government auditing standards** | Also referred to as the Yellow Book or GAGAS), standards that provide a framework for performing high-quality audits of government organizations, programs, activities, and functions, and of government assistance received by contractors, nonprofit organizations, and other nongovernment organizations, with competence, integrity, objectivity, and independence.  These standards are to be followed by auditors and audit organizations when required by law, regulation, agreement, contract, or policy. They pertain to auditors’ professional qualifications, the quality of audit effort, and the characteristics of professional and meaningful audit reports. |
| **general controls** | One of the three types of information system controls that apply to all or a large segment of an entity’s information systems. When designed, implemented, and operating effectively, these controls create a suitable environment to support the effective operation of user and application controls. See also direct general controls and indirect general controls. |
| **general support system** | An interconnected set of information system resources under the same direct management control that share common functionality. Normally, the purpose of a general support system is to provide processing or communications support. |
| **hardware** | Physical equipment used to process, store, or transmit computer programs or data. It includes computing devices (e.g., servers, workstations, and mobile devices), peripheral equipment (e.g., keyboards, monitors, webcams, and printers), networking devices (e.g., firewalls, routers, and switches), cables, and other telecommunications equipment. |
| **hashing** | The process of using a mathematical algorithm against data to produce a numeric value that is representative of those data. |
| **identification** | The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an information system. |
| **impact level** | The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate, or high. |
| **incident** | An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. |
| **incident response program** | A process that involves detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference. |
| **incompatible duties** | When work responsibilities are not segregated such that one individual controls multiple critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs. Similarly, one computer programmer should not be allowed to independently write, test, and approve program changes. |
| **indirect general controls** | Those controls, which apply to the information system security program and information systems, that are intended to create a suitable environment to support the effective operation of user, application, and direct general controls within the business process. |
| **information** | Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. |
| **information and communication** | One of the five components of internal control. Information and communication consists of the quality information management and personnel communicate and use to support the internal control system. |
| **information owner** | Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. |
| **information processing objectives** | Requirements for effective information processing, including completeness, accuracy, and validity. |
| **information resources** | The people, processes, data, and information technology used to collect, process, store, maintain, use, share, disseminate, or dispose of information. |
| **information security** | The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. |
| **information security management program** | A program designed, implemented, and operated to reasonably assure that adequate information security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information systems. |
| **information security management program plan** | Formal document that provides an overview of the security requirements for an entity-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. |
| **information spill** | Security incident that results when information that is thought to be at certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. |
| **information system** | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. |
| **information system boundaries** | Logical or physical boundaries around information resources and implementing measures to prevent unauthorized information exchange across the boundary in either direction. Firewall devices represent the most common boundary protection technology at the network level. |
| **information system component** | A discrete identifiable IT asset that represents a building block of a system and may include hardware, software, and firmware. |
| **information system controls** | Internal controls that depend on information system processing. They include user controls, application controls, and general controls. |
| **information system owner** | Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. |
| **information system processing** | Processing performed by information systems using information technology. |
| **information system control risk** | The likelihood that conditions or events, related to the areas of audit interest, that could significantly affect the entity’s ability to achieve its information processing objectives will not be prevented, or detected and corrected, on a timely basis by the entity’s IS controls. |
| **information system risk factors** | Conditions or events that affect the susceptibility of the area of audit interest to information system processing errors before consideration of any mitigating IS controls. |
| **information technology** | The hardware, software, firmware, equipment, media, and services used for information system processing. |
| **infrastructure** | The physical information system resources necessary to run software that includes the hardware devices used for information processing, data storage, and network communication. Infrastructure also includes the logical information system resources necessary to run multiple virtual machines on shared physical information system resources. |
| **input** | Any information entered into a computer, or the process of entering data into the computer. |
| **integration testing** | Testing to determine if related information system components perform to specifications. |
| **integrity** | Guarding against improper information modification or destruction, which includes ensuring information’s nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information. |
| **interconnection security agreement** | A document that regulates security-relevant aspects of an intended connection between an entity and an external system. It regulates the security interface between any two systems operating under two distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal memorandum of understanding that defines high-level roles and responsibilities in management of a cross-domain connection. |
| **interface** | A common boundary between information systems and information system components where interactions take place. Interfaces include system interconnections and system information exchanges. Interface also refers to the portion of a program that interacts with the user. The terms system interface and user interface may also be used in FISCAM. |
| **interface design** | Uses guidelines set by the system interface strategy and provides specific information for each of the characteristics defined in the system interface strategy. |
| **interface strategy** | Describes at the highest level how the system interfaces are implemented between two applications. The interface strategy includes an explanation of each interface, the interface method chosen (manual or batch, etc.), the data fields being interfaced, the controls to reasonably assure that the data are interfaced completely and accurately, timing requirements, assignment of responsibilities, ongoing system balancing requirements, and security requirements. |
| **internal control** | A process effected by an entity’s oversight body, management, and other personnel designed to provide reasonable assurance that the entity’s objectives will be achieved. |
| **intrusion** | A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, unauthorized access to an information system or information system resource. |
| **intrusion detection system** | Software that inspects network activity to identify suspicious patterns that may indicate a network or system attack. |
| **intrusion prevention system** | Software that inspects network activity to identify suspicious patterns that may indicate a network or system attack and can also attempt to stop the activity, ideally before it reaches its targets. |
| **inventory** | A listing of items, including identification and location information. |
| **job** | A set of data that completely defines a unit of work for a computer. A job usually includes programs, linkages, files, and instructions to the operating system. |
| **key resources protection plan** | A plan that identifies key resources across all asset types and the corresponding consequences of loss. |
| **labeling** | The association of attributes with the subjects and objects represented by the internal data structures within information systems. This facilitates system-based enforcement of information security and privacy policies. |
| **least privilege** | The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations it needs to perform its function. |
| **library** | A collection of similar files, such as datasets contained on tape or disks and stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. Libraries are also called program libraries and partitioned datasets.  Library can also refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape libraries. |
| **log** | A record of the events occurring within an organization’s systems and networks. |
| **logical access** | Ability to interact with information system resources granted using identification, authentication, and authorization. |
| **logical access control** | Involves requiring users to authenticate themselves, limiting their access to files and other resources, and limiting the actions that they can execute. Such controls are also referred to as logical security. |
| **log-on** | The process of establishing a connection with, or gaining access to, a computer system or peripheral device. |
| **maintenance** | Altering programs after they have been in use for a while. Maintenance programming may be performed to add features, correct errors that were not discovered during testing, or update key variables (such as the inflation rate) that change over time. |
| **major application** | An application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in that application. |
| **major information system** | An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. |
| **malicious code** | Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Examples include a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. |
| **marking** | The association of attributes with objects in a human-readable form displayed on system output. Marking enables manual, procedural, or process-based enforcement of information security and privacy policies. |
| **master data** | Referential data that provides the basis for ongoing business activities, for example, data about customers, vendors, and employees. |
| **media controls** | Controls implemented to prevent unauthorized physical access to digital (e.g., diskettes, flash drives, thumb drives, and compact disks) and printed (e.g., paper and microfilm) media removed from an information system and during pickup, transport, and delivery to authorized users. |
| **methodology** | The nature and extent of audit procedures for gathering and analyzing evidence to address the engagement objectives. |
| **middleware** | Software designed for data transport and communications. |
| **mobile code** | Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. |
| **monitoring** | One of the five components of internal control. Monitoring consists of activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews. |
| **multifactor authenticator** | An authenticator that provides more than one distinct authentication factor, such as a cryptographic authentication device with an integrated biometric sensor. |
| **naming conventions** | Standards for naming information system resources, such as data files, program libraries, individual programs, and applications. |
| **network** | A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area. |
| **network administration** | The function responsible for maintaining secure and reliable network operations. This function serves as a liaison for user departments to resolve network needs and problems. |
| **network component** | Any device that supports a network, including workstations, servers, switches, and routers. |
| **network session** | A connection between two network component peers. |
| **nonrepudiation** | Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action, such as creating information, sending a message, approving information, and receiving a message. |
| **nonstatistical selection** | A method of selecting items from a population to reach a conclusion only on the items selected. This selection method is not representative of the population and not projectable to the portion of the population that was not selected. To determine whether sufficient evidence has been obtained to conclude on the effectiveness of the controls tested, the auditor considers the results of the nonstatistical selection in conjunction with other sources of evidence. |
| **object code** | Machine-readable instructions translated from source code by a compiler or assembler program. A file of object code may be immediately executable, or it may require linking with other object code files (e.g., libraries) to produce a complete executable program. See also code and source code. |
| **operating system** | The software that controls the execution of other computer programs, schedules tasks, allocates storage, manages the interface to peripheral hardware, and presents a default interface to the user when no application program is running. |
| **operational environment** | Context determining the setting and circumstance of all influences on an information system. |
| **output** | Data and information produced by information system processing, such as graphic display or hard copy. |
| **output device** | Peripheral equipment, such as a printer or tape drive, that provides the results of processing in a form that can be used outside the system. |
| **override** | Decision made by management or operation staff to bypass established controls to allow a transaction (or transactions) that would otherwise be rejected to be processed. |
| **owner** | Manager or director who has responsibility for an information system resource, such as a data file or application software. |
| **parameter** | A value that is given to a variable. Parameters provide a means of customizing programs. |
| **partitioning** | Process of physically or logically separating different functions, such as applications, security, and communication activities. Separation may be accomplished by using different computers, central processing units, operating systems, network addresses, or combinations of these methods. |
| **password** | A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. |
| **patch** | An additional piece of code that has been developed to address specific problems or flaws in existing software. |
| **penetration testing** | A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system. |
| **personally identifiable information** | Any information about an individual maintained by an entity, including (1) any information that can be used to distinguish or trace an individual’s identity, such as that person’s name, Social Security number, date of birth, or biometric records, and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. |
| **physical access control** | Involves restricting physical access to information system resources and protecting these resources from intentional or unintentional loss or impairment. |
| **plan of action and milestones** | A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. |
| **platform** | The logical information system resources necessary to run application software, including the operating system and related computer programs, tools, and utilities. |
| **privacy impact assessment** | An analysis of how information is handled to  (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;  (2) determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and  (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy concerns.  A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis. |
| **privacy management program plan** | A formal document that provides an overview of an agency’s privacy program, including a description of the structure of the privacy program, the resources dedicated to the program, the role of the privacy officer and other privacy officials and staff, the strategic goals and objectives of the program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. |
| **privacy requirements** | Requirements levied on an information system that are derived from statutes, regulations, executive orders, implementing entity guidance, directives, policies, standards, procedures, organizational mission, or business case needs with respect to privacy. |
| **privileged account** | An authorized information system account with approved authorizations of a privileged user. |
| **privileged user** | A user who is authorized (and therefore trusted) to perform functions, including those relevant to security, that ordinary users are not authorized to perform. |
| **process** | Systematic sequences of operations to produce a specified result. This includes all functions performed using a computer, such as editing, calculating, summarizing, categorizing, and updating. |
| **processing** | The execution of program instructions by the computer’s central processing unit. |
| **production control and scheduling** | The function responsible for monitoring the information into, through, and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is used in this task. |
| **production environment** | An environment where functionality and availability must be ensured for the completion of day-to-day activities. |
| **programmer** | A person who designs, codes, tests, debugs, and documents computer programs. |
| **proprietary** | Technology that is privately owned, based on trade secrets, or privately developed, or specifications that the owner refuses to divulge, which prevents others from duplicating a product or program unless an explicit license is purchased. |
| **protocol** | A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. |
| **public key infrastructure** | A set of policies, processes, server platforms, software, and workstations used for administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. |
| **public key infrastructure certificate** | A digital representation of information that at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber’s public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. |
| **quality assurance testing** | The function that reviews software project activities and tests software products throughout the software life cycle to determine if (1) the software project is adhering to its established plans, standards, and procedures and (2) the software meets the user-defined functional specifications. |
| **query** | The process of extracting data from a database and presenting it for use. |
| **record** | A unit of related data fields, or the group of data fields that can be accessed by a program and contains the complete set of information on a particular item. |
| **relevant information system controls** | Those user, application, and general controls that are suitably designed and are necessary to achieve relevant control objectives and that the auditor plans to test for implementation and operating effectiveness. |
| **relevant control objectives** | Those control objectives pertaining to areas of audit interest that are necessary to achieve the engagement objectives. |
| **relevant information systems** | A subset of the entity’s information systems that, based on their significance to the engagement objectives, the auditor includes in the scope of the IS controls assessment. See also areas of audit interest. |
| **remote access** | Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the internet). |
| **remote maintenance** | Maintenance activities conducted by individuals communicating through an external network (e.g., the internet). |
| **residual risk** | Portion of risk remaining after security measures have been applied. |
| **risk** | The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. |
| **risk factor** | A characteristic used in a risk model as an input to determine the level of risk in a risk assessment. |
| **risk management** | The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system. The process includes conducting a risk assessment, implementing a risk mitigation strategy, and employing techniques and procedures for the continuous monitoring of the security state of the information system. |
| **risk management strategy** | A strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. |
| **router** | An intermediary device on a communications network that expedites message delivery. As part of a local area network, a router receives transmitted messages and forwards them to their destination over the most efficient available route. |
| **run** | A popular, idiomatic expression for program execution. |
| **safeguards** | Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features; management constraints; personnel security; and security of physical structures, areas, and devices. Safeguards is synonymous with security controls and countermeasures. |
| **sanitization** | Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. |
| **scope** | The boundary of the IS controls assessment that is directly tied to the engagement objectives. |
| **security administrator** | Person who is responsible for managing the security program for computer facilities, computer systems, data that are stored on computer systems or transmitted via computer networks, or a combination of these. |
| **security architecture** | A set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected. |
| **security categorization** | The process of determining the security category for information or an information system. Security categorization methodologies are described in Committee on National Security Systems Instruction 1253 for national security systems and in Federal Information Processing Standard 199 for other than national security systems. |
| **security controls** | The controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. |
| **security domain** | An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. |
| **security management** | A control category within the FISCAM Framework that provides the foundation of a security-control structure and reflects senior management’s commitment to addressing security risks. |
| **security objectives** | Requirements for effective information security, including confidentiality, integrity, and availability. |
| **security requirements** | Requirements levied on an information system that are derived from laws, executive orders, implementing entity guidance, directives, policies, instructions, regulations, organizational mission, or business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. |
| **segregation of duties** | A control category within the FISCAM Framework that relates to the policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations and thereby prevent unauthorized actions or unauthorized access to assets or records. Segregation of duties involves segregating work responsibilities so that one individual does not control all critical stages of a process. |
| **sensitive** | The nature of information system resources where the loss, misuse, or unauthorized access or modification could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled. |
| **server** | A computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries). |
| **service** | See system service. |
| **service auditor** | An independent auditor hired by the service organization to provide a report on internal controls at the service provider. |
| **service-level agreement** | Represents a commitment between a service provider and one or more customers and addresses specific aspects of the service, such as responsibilities; details on the type of service; expected performance level (e.g., reliability, acceptable quality, and response times); and requirements for reporting, resolution, and termination. |
| **service organization** | External organizations used to support business processes. Service organizations provide services ranging from performing a specific task (e.g., payroll processing) to replacing entire business units or functions of an entity. |
| **significant** | The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Such factors include the magnitude of the matter in relation to the subject matter of the engagement, the nature and effect of the matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the matter’s effect on the audited program or activity. The term significant is comparable to the term material as used in the context of financial audits. |
| **significant business process** | Business processes that are significant to the engagement objectives. |
| **simple random selection** | A method of selecting a sample of items from a population in which each item of the population has an equal probability of selection. |
| **smart card** | A plastic card with embedded, integrated circuits that can store, process, and communicate information for authenticating a user. |
| **software** | An integrated set of computer programs that facilitates the use of a computer to perform operations or tasks. |
| **source code** | A set of computer instructions and data definitions expressed in a form suitable for input to an assembler, compiler, or other translator. A programmer writes source code in a programming language that humans can read and understand. Source code is ultimately translated into object code, which a computer can read. See also code and object code. |
| **spyware** | Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. |
| **standard** | In computing, a set of detailed technical guidelines to establish uniformity in an area of hardware or software development. |
| **sufficiency** | The measure of the quantity of evidence used to support the findings and conclusions related to the engagement objectives. |
| **switch** | A network component that filters and forwards packets between local area network segments. |
| **system** | See information system. |
| **systematic random selection** | A method of selecting a sample of items from a population in which a uniform interval is determined, a starting point is randomly selected in the first interval, and then every kth unit is selected. |
| **system administrator** | An individual, group, or organization responsible for setting up and maintaining a system or specific system elements, implementing approved secure baseline configurations, incorporating secure configuration settings for information system components, and conducting or assisting with configuration monitoring activities as needed. |
| **system boundary** | All components of an information system to be authorized for operation by an authorizing official. The system boundary excludes separately authorized systems, to which the information system is connected. |
| **system developer** | An individual group or organization that develops hardware and software for distribution or sale. |
| **system development life cycle** | The scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, operation, maintenance, and ultimately its disposal. |
| **system information exchange** | Access to or the transfer of data outside of system authorization boundaries to accomplish a mission or business function. This includes connections via leased lines or virtual private networks; connections to internet service providers; database sharing or exchanges of database transaction information; connections and exchanges with hosted services by external parties; exchanges via web-based services; or exchanges of files via file transfer protocols, network protocols (e.g., IPv4 and IPv6), email, or other organization-to-organization communications. |
| **system interconnection** | A direct connection between two or more systems in different authorization boundaries to exchange information; allow access to information, information services, and resources; or both. |
| **system level** | The level at which general controls relevant to an information system are implemented. These controls are specific to certain information systems and often correspond to one of three sublevels inherent in all information systems—infrastructure, platform, and software. |
| **system privacy plan** | A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks. The plan details how the controls have been implemented and describes the methodologies and metrics that will be used to assess the controls. |
| **system security plan** | A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. |
| **system service** | A function performed by system software that facilitates information processing, storage, or transmission. Such functions include loading and executing computer programs, resource allocation, and error detection. |
| **system software** | Software designed to operate and control the processing activities of hardware. It includes the operating system and utility programs and is distinguished from application software. |
| **system utilities** | Software used to perform system maintenance routines that are frequently required during normal processing operations. Some of the utilities have powerful features that will allow a user to access and view or modify data or code. |
| **telecommunications** | The preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. |
| **those charged with governance** | Those who have the responsibility for overseeing the strategic direction of the entity and obligations related to the accountability of the entity. This includes overseeing the financial reporting process, subject matter, or program under audit, including related internal controls. For a federal entity, those charged with governance may be members of a board or commission, an audit committee, the secretary of a cabinet-level department, or senior executives and financial managers responsible for the entity. |
| **threat** | Any circumstance or event with the potential to adversely affect entity operations (including mission, functions, image, or reputation), entity assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service. |
| **token** | A device used to store cryptographic information and possibly also perform cryptographic functions for use in authentication systems. |
| **tolerable rate of deviation** | A rate of deviation set by the auditor in respect of which the auditor seeks to obtain an appropriate level of assurance that the rate of deviation is not exceeded by the actual error rate of the population. This is also referred to as tolerable error, tolerable rate, or tolerable deviation. |
| **topology** | The physical layout of how computers are linked together. |
| **transaction** | A discrete event captured by a computer system, such as the entry of a customer order or an update of an inventory item. In financial systems, a transaction generally represents a business event that can be measured in dollars and cents and entered in accounting records. |
| **transaction data** | The finite data pertaining to a given event occurring in a business process. This process produces documents or postings, such as purchase orders and obligations. |
| **trust anchor** | A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g., in a public key certificate). A trust anchor may have name or policy constraints limiting its scope. |
| **trust store** | A repository that contains cryptographic artifacts like certificates that are used for cryptographic protocols. |
| **trusted communications path** | A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. Only the user or the security functions of the information system can activate this mechanism, and it cannot be imitated by untrusted software. |
| **uninterruptible power supply** | Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level. |
| **unit testing** | Testing individual program modules to determine if they perform to specifications. |
| **user** | Individual or system process authorized to access an information system. |
| **user controls** | One of the three types of information system controls that apply to portions of controls that are performed by people interacting with information systems. These controls are designed to achieve information processing objectives—completeness, accuracy, and validity of transactions and data. A user control is an information system control if its effectiveness depends on information system processing or the reliability (completeness, accuracy, and validity) of information processed by information systems. |
| **user identification (user ID)** | Unique symbol or character string used by an information system to identify a specific user. |
| **user-defined processing** | When a user is allowed to establish or modify processing steps. This frequently occurs in application-based spreadsheets and report writer tools and data extraction tools. |
| **utility program** | Specialized system software used to perform particular computerized functions and routines that are frequently required during normal processing. |
| **validation** | The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. |
| **validity** | An information processing objective that aims to provide reasonable assurance that all recorded transactions and events actually occurred, are related to the entity, and were executed according to prescribed procedures. |
| **virus** | A program that “infects” computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the “infected” file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. |
| **vulnerability** | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. |
| **vulnerability scan** | Type of network security testing that enumerates the network structure and determines the set of active hosts and associated software and verifies that software (e.g., operating system and major applications) is up to date with security patches and software version. |
| **walk-through** | A combination of observation, inspection, and inquiry audit procedures that helps the auditor understand (1) the steps and information resources involved in a significant business process from beginning to end and (2) the design and implementation of the controls involved. When performing walk-throughs to obtain an understanding of a significant business process, the auditor generally traces one or more transactions, activities, or events from initiation through all processing, observing the processing in operation, inspecting relevant documentation, and making inquiries of entity staff. |
| **web application** | An [application](http://en.wikipedia.org/wiki/Application_software) that is accessed over a network, such as the [internet](http://en.wikipedia.org/wiki/Internet) or an [intranet](http://en.wikipedia.org/wiki/Intranet). |
| **workstation** | A microcomputer connected to a network. Workstation can also refer to a powerful, stand-alone computer that has considerable calculating or graphics capability. |
| **worm** | An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. |