

Glossary of Terms

Access Control. Manual or automated process designed to control the ability of authorized and unauthorized users to generate, modify, destroy, view, or extract data maintained in information systems.

Access Control Software. Security software used to provide additional security above and beyond that provided by the operating system. Ensures that only authorized persons and/or programs access protected resources, including data, system functions and programs. Examples of common packages used in the mainframe environment are CA-ACF2, RACF, and CA-Top Secret.

Access Method. The technique used for selecting records in a file for processing, retrieval, or storage.

Access Privileges. Precise statements that define the extent to which an individual can access computer systems and use or modify the programs and data on a system, and under what circumstances this access will be allowed.

Accountability. The system does what it is supposed to do – nothing more, nothing less.

Accuracy. Freedom from error in the data.

Affinity Fraud. Refers to investment scams that prey upon members of identifiable groups, such as religious or ethnic communities, the elderly, or professional groups. Many affinity scams involve “Ponzi” or “Pyramid” schemes, where new investor money is used to make payments to earlier investors to give the false illusion that the investment is successful.

Agile Programming. A conceptual framework for software development that promotes development iterations throughout the life-cycle of the project. Each iteration passes through a full software development cycle.

Application. A program designed to perform a specific function for the user or, in some cases, for another application program. Examples would be payroll, labor, inventory, or accounts payable systems.

Application Controls. Application controls, sometimes referred to as business controls, are designed specifically for computer applications to help ensure the validity, completeness, accuracy, and confidentiality of data during application processing and reporting.

Application Control Activities. Controls relating to a specific computer task, such as preparation of payroll.

Application Internal Controls. Controls over computerized systems generally designed for a specific business application. Examples of application controls are automated edit checks, file control reconciliations, and automated segregation of duties. They are generally categorized as to where they occur within the system (Input, Processing or Output). These controls are more data-oriented in nature. (See Application Controls)

Application Level General Controls. Controls consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning.

Application Software. The programmed instructions that control the processing of data within a particular application system (payroll, personnel, etc.). It can either be developed (either internally or by a contractor) or purchased (Commercial Off-the-Shelf [COTS]). Absent a data base management system, this is where the system processing controls are concentrated.

ARCPD. See Assessing the Reliability of Computer-Processed Data

Arithmetic and Logic Unit (ALU). The part of the Central Processing Unit (CPU) in which all arithmetic operations and logical comparisons are performed.

Asportation. A carrying away; specifically: the carrying away of someone else's property that is an element of larceny.

Assessing the Reliability of Computer-Processed Data (ARCPD). GAO Publication, GAO-03-273G, dated October 2002. Provides a flexible, risk-based framework for data reliability assessments that can be geared to the specific circumstances of each engagement.

Audit Logging. Recording of user activity in a system or application initiated by the user (e.g., access to a file, record, or field, use of modem). Further, it may record any attempts to log on (successful or unsuccessful) to a system and record logon ID, date and time of each log on.

Audit Objectives. Broad statements developed by auditors and define intended audit accomplishments.

Audit Procedures. The tasks the auditor undertakes for collecting, analyzing, interpreting, and documenting information during an audit. Also referred to as a means to attain audit objectives.

Audit Risk. Represented by the formula: $\text{Audit Risk} = \text{Inherent Risk} \times \text{Control Risk} \times \text{Detection Risk}$. Also referred to as Residual Risk. It is the risk that material misstatements were undetected by the auditor.

Audit Trail. Consists of the documents created by key personnel that show written proof of approval as each person involved in the process routinely reviews and verifies transactions while they are processed from the initial recording to final posting. In a manual accounting system, this audit trail consists of paper source documents linking individual transactions to journal postings and ledger postings.

Auditing Around the Computer. Testing the reliability of computer-generated information by first calculating expected results from the transactions entered into the system and then comparing to the output results.

Auditing Through the Computer. Process by which the computer is used to test the effectiveness of application internal controls by examining data as it passes through the system.

Auditing With the Computer. Process by which the computer is used as an audit tool in the performance of substantive tests to maximize efficient use of scarce audit resources.

Authentication. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authenticity. The users are who they say they are. It is the property of being genuine and being able to be verified and trusted.

Availability. The information systems on which the organization is heavily dependent is available for the organization at all times when required.

Backdoor. An undocumented way to gain access to a program, data, or an entire computer system, often known only to the programmer who created it. Backdoors can be handy when the standard way of getting information is unavailable, but they usually constitute a security risk.

Backup. Any duplicate of a primary resource function, such as a copy of a computer program or data file. This standby is used in case of loss or failure of the primary resource.

Batch Processing. A system in which like transactions are processed periodically as a group. Executing a series of non-interactive jobs all at one time.

Benchmarking. Establishing a point of reference from which measurements can be made. For example, this is a common technique in measuring and monitoring computer system performance.

Biometric. A physical or behavioral characteristic of a human being.

Black Box Testing. See Generalized Testing.

Botnets. Compromised computers that can be remotely controlled by attackers to automatically launch attacks. Bots (short for robots) have become a key automation tool to speed the infection of vulnerable systems.

Bridge. A device that connects two local-area-networks (LANs) or two segments of the same LAN that use the same protocol, such as Ethernet or token-ring.

Bus. A transmission path on which signals are dropped at every device attached to the line.

BUS Network. An arrangement in a local area network in which each node (work device) is connected to a main cable or link called the bus.

Business Process. The primary function(s) that an entity performs in accomplishing its mission.

Business Process Application. A computer program designed to help perform a business function such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.

Business Process Application Controls. Controls directly related to individual computerized applications. They help ensure that transactions are complete, accurate, valid, confidential, and available. These controls includes programmed control techniques, such as automated edits, and manual techniques such as review of reports identifying rejected or unusual items.

Business Process Application Level. Controls at the business process application level consist of policies, procedures for controlling specific processes. For example, the entity's configuration management should reasonably ensure that all changes to application systems are fully tested and authorized.

Bypass Label Processing (BLP). The technique of reading a computer file while bypassing the internal file/data set label. This process could result in bypassing security access controls.

CAAT. See Computer-Assisted Audit Technique.

Central Processing Unit (CPU). Consists of an Arithmetic and Logic Unit (ALU), a Control Subsystem, and Primary Storage.

Change Request Log. A log which consists of suggestions for changes in programs. These changes have often been initiated by users who have noted problems or possible enhancements for a program.

Clients. Computers that are configured to allow individual users to access network services. They range from "fat" clients that contain internal processing, programming and data storage (and can function in many cases independently of the network) to "thin" clients that function only when network resources are available and contain no internal secondary storage or programming capacity.

Client/Server Architecture. A model for a relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request.

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. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternative site.

Commercial off-the-Shelf Software (COTS). Ready-made products such as application software marketed by software vendors. The objective of the software vendor is to create a package suitable for a variety of users in the same industry or with the same application.

Competence of Evidence. We can rely on the processing and output being generated by the system.

Compiler. A program that reads the statements in a human-readable programming language and translates them into a machine-readable executable program.

Completeness. The inclusion of all necessary parts or elements. For example, in a data file it means that all of the relevant data elements and records are present in the file.

Completeness Control. Controls that ensure entity management that all transactions that occurred are entered into the system, accepted for processing, and processed once and only once by the system and are properly included in output.

Computer. Generally consists of a central processing unit, storage, input, and output devices.

Computer-Assisted Audit Technique (CAAT). Any automated audit technique, such as generalized audit software, test data generators, computerized audit programs, and special audit utilities.

Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The information in the systems is disclosed only to those who have a need to see and use it.

Confidentiality Control. Controls that are designed to provide reasonable assurance that application data and reports and other output are protected against unauthorized access.

Configuration Control. Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

Configuration Management. The control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of the system.

Consistency. Data that is well defined enough to yield similar results in similar analyses.

Contingency Plan. Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disaster.

Contingency Planning. Encompasses both disaster recovery planning (identifying, quantifying and developing action plans to address risks to the electronic computer capabilities of the entity) and business continuity planning (ensuring that the entity can continue as a going concern, regardless of the state of its' computing capabilities).

Control Activities. Descriptions of individual control requirements for each critical control element (e.g., implement effective authorization controls, adequately protect sensitive system resources).

Control Categories. Groupings of related controls pertaining to similar types of risk. Control categories include security management, access controls, configuration management, segregation of duties, and contingency planning.

Control Environment. The first of five interrelated components of internal control. Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Control Objectives. The intent of the specific control to effectively secure specific general support or business activities.

Control Point Technique. A common audit technique used to gain and document our understanding of the information flow and system of internal controls.

Control Risk. The risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by an entity's internal control.

Control Subsystem. The part of the Central Processing Unit (CPU) that manages the transformation process by overseeing the storage of data and instructions, their transfer to and from the Arithmetic and Logic Unit (ALU), and the ultimate transmittals of the results to the output component of the computer.

Control Techniques. The specific control implemented by the entity to secure a specific general support system or business process activity.

Controlled Programs. Duplicate entity application programs that are maintained under the auditors' control in order to test the programmed control activities.

Corrective Controls. Internal controls designed to remedy problems soon after they arise.

COTS. See Commercial off-the-Shelf Software.

CPU. See Central Processing Unit.

Crasher. An outside intruder, or hacker, that destroys files, software, and other utilities by introducing viruses or worms.

Critical Control Points. Those points at the application level (in addition to critical control points at the system level), which if compromised, could significantly affect the integrity, confidentiality, or availability of key business process applications or related data.

Critical Elements. Tasks that are essential for establishing adequate controls within each control category.

Data. The electronically encoded bits and bytes that represent the information which is entered, stored, manipulated, transmitted and reported as a result of computer processing.

Data Accuracy. All relevant records are completely processed and the computer processing met the intended objectives.

Data Authenticity. The computer-processed data matches factual information contained in source records.

Database. A collection of related data files (for example, questionnaire responses from several different groups of people, with each group's identity maintained) that is organized so that its contents can easily be accessed, managed, and updated. A system that minimizes data redundancy and enforces data integrity by storing data separately from (outside of) programs, and contains data for two or more computer applications.

Database Administrator (DBA). The person who has overall responsibility for developing and maintaining the database and establishing controls.

Database Management System (DBMS). Comprised of computer software designed for the purpose of managing databases based on a variety of data models. DBMS allows related files to be treated as an organized set. It allows the separation of data maintenance from program maintenance, and contains powerful utilities that permit efficient data management and allows the installation of powerful data controls. Examples are: DB2, IMS, IDMS.

Data Completeness. All relevant data elements and records are contained in the universe.

Data Control Language (DCL). A computer language and a subset of SQL (System Query Language) used to control access to data in a data base. It specifies the privileges and security rules governing data base users.

Data Definition Language (DDL). A computer language for defining data structures. It defines the schema and subschema, links between the logical and physical structures of the data base.

Data Dictionary (DD). Describes the use of data from the data base and maps to applications. The DD contains a catalog of all data elements, their names, structures and information about their usage.

Data Element. An individual piece of information that has definable parameters, sometimes referred to as variables or fields (for example, the response to any question in a questionnaire).

Data File. A collection of related data records, also referred to as a data set (for example, the collected questionnaire responses from a group of people).

Data File Survey. Familiarizes the auditor with the types and attributes of data in a specific data file.

Data Manipulation Language (DML). A family of computer languages used by computer programs or data base users to retrieve, insert, delete and update data in a data base. Currently, the most popular is SQL (System Query Language) which is used to retrieve and manipulate data in a relational data base.

Data Mapping Facility (DMF). Used to evaluate and document the data base.

Data Mining. The analysis of data for relationships that have not previously been discovered.

Data Owner. See owner.

Data Processing. The computerized preparation of documents and the flow of data contained in these documents through the major steps of recording, classifying, and summarizing.

Data Record. A collection of logically related data elements that relate to a specific event, transaction, or occurrence (for example, questionnaire responses about one individual – such as age, sex, and marital status).

Data Reliability. Refers to the accuracy and completeness of computer-processed data.

Data Structures. Describe the ways that data is stored and accessed (e.g., fixed versus variable length records; sequential, indexed sequential and direct access; flat versus data base files).

Data Test Plan. Clearly states the condition or objective the auditor hopes to accomplish by the test and how that objective is to be accomplished.

Data Warehouse. A generic term for a system used to store, retrieve, and manage large amounts of data. A central repository for all or significant parts of the data than an enterprise's various business systems collect.

DBA. See Database Administrator.

DBMS. See Database Management System.

Debug. With software, to detect, locate, and correct logical or syntactical errors in a computer program.

Decryption. The process of changing cipher text using a cryptographic algorithm and key.

Denial of Service (DOS) Attack. An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate of speed.

Detailed Testing. A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as White Box Testing.

Detection Risk. The risk that the auditor will not detect a material misstatement that exists in an assertion.

Detective Controls. Actions taken to detect and correct undesirable events which have occurred, i.e., internal controls designed to identify problems soon after they arise.

Developing Test Tools. Specifying the data to be used, the processing to be performed on it, and the types of output reports to be produced.

Dial-Up Access. A means of connecting to another computer, or a network similar to the Internet, over a telecommunication line using a modem-equipped computer.

Dichotomy. Division into two mutually exclusive, opposed, or contradictory groups.

Digital Signature. Cryptographic process used to assure message originator authenticity, integrity, and nonrepudiation.

Direct (Random) Access. A storage technique in which each piece of data is assigned an address and may be retrieved without searching through other stored data. A magnetic disk drive is a direct access device.

Directive Controls. Actions taken to cause or encourage a desirable event to occur.

Directory System (DS). A collection of definitions, rules and advisories of data, designed to be used as a guide or reference with the data warehouse. The directory includes definitions, examples, relations, functions and equivalents in other environments.

Disaster Recovery Plan. A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

Distributed Processing. A variety of computer systems that use more than one computer, or processor, to run an application. A computer system that uses communication links to share data and programs among various users in remote locations throughout the organization. The users may process the data in their own departments.

Domain Name System (DNS) Server. A server dedicated to housing the domain name system which serves as the “phone book” for the Internet by translating human-readable computer host names, e.g., www.example.com, into IP addresses, e.g., 208.77.188.166, which networking equipment needs to deliver information.

E-commerce Software. Software that is used to accommodate the buying or selling of goods and/or services electronically over systems such as the Internet and other computer networks.

Electronic Data Interchange (EDI). A system in which data are exchanged electronically between the computers of different organizations. A standard format for exchanging business data. EDI is one form of e-commerce.

Electronic Funds Transfer (EFT). A system of transferring money from one bank account directly to another without any paper money changing hands. One of the most widely-used EFT programs is Direct Deposit.

Electronic Mail (E-Mail). A store-and-forward method of composing, sending, receiving and storing messages over electronic communication systems. The term “e-mail” applies to both the Internet e-mail system based on the Simple Mail Transfer Protocol (SMTP) and to X.400 systems, and to intranet systems allowing users within one organization to e-mail to each other.

Electronic Mail (E-Mail) Spoofing. Forging an e-mail header to make it appear as if it came from somewhere or someone other than the actual source. The mail protocol that is used when sending e-mail – SMTP- does not include a way to authenticate. In some jurisdictions, e-mail spoofing anyone other than yourself is illegal.

Electronic Signature. A symbol generated through electronic means that can be used to (1) identify the sender of information and (2) ensure the integrity of the critical information received from the sender.

Embedded Audit Module Technique. Inserting a programmed module or routine into an application program. Classified as a continuous audit approach.

Encryption. Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people.

End User Computing. An environment where a user department is responsible for developing or purchasing, and running, a computer system (application) with minimal or no support from the central information systems department.

Enterprise. An organization that uses computers. A word that encompasses corporations, small businesses, non-profit institutions, government bodies, and possibly other kinds of organizations.

Enterprise Resource Planning (ERP). An industry term for the broad set of activities supported by multi-module application software that help a manufacturer or other business manage the important parts of its business.

Entry Points. Access points to the entity's information systems. This may include remote access through dial-up, wireless devices, or the Internet.

Ethernet. The most widely-installed local area network technology. An Ethernet LAN typically uses coaxial cable; however, it is also used in wireless LANs.

FAM. See Financial Audit Manual

Federal Information Processing Standards (FIPS). With the passage of FISMA in 2002, NIST (National Institute of Standards and Technology) was tasked with responsibilities for standards and guidelines. NIST developed the FIPS publications which are standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. Key publications are FIPS Pub 199 and 200.

Federal Information Security Management Act (FISMA). Enacted into law as Title III of the E-Government Act of 2002 (PL 107-347; December 17, 2002), FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.

Federal Information System Controls Audit Manual (FISCAM). GAO Publication, GAO-09-232G, dated February 2009. Provides a methodology for performing information system (IS) control audits in accordance with GAGAS, where IS controls are significant to the audit objectives.

Federal Managers' Financial Integrity Act of 1982 (FMFIA). PL 97-255, September 8, 1982. An Act to amend the Accounting and Auditing Act of 1950 to require ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control of each executive agency, and for other purposes.

Fiber Optic Transmission. Transmission using a glass or plastic filament cable used to communicate signals in the form of light waves.

Field. A location in a record in which a particular type of data are stored, such as a name, date of birth or salary.

File. An organized collection of related records, such as a customer or vendor file.

File Transfer Protocol (FTP). A standard Internet protocol which is viewed as the simplest way to exchange files between computers. This is the usual way you send files to your server.

Financial Audit Manual (FAM). GAO Publication, GAO-08-586G, dated July 2008. An outgrowth of cooperation between GAO and PCIE (President's Council on Integrity and Efficiency) in complying with the Government Management and Reform Act of 1994. This act provided executive branch IGs and GAO statutory responsibility for auditing agency and government-wide consolidated financial statements.

FIPS. See Federal Information Processing Standards

Firewall. A set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. It is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources. A firewall's basis task is to regulate some of the flow of traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust.

Firmware. Program recorded in permanent or semi-permanent computer memory.

FISCAM. See Federal Information System Controls Audit Manual

FISMA. See Federal Information Security Management Act

Flowchart. A diagram of the movement of transactions, computer functions, media, and/or operations within a system. The processing flow is represented by arrows between symbolic shapes for operation, device, data file, etc. to depict the system or program.

FMFIA. See Federal Managers' Financial Integrity Act of 1982

Focused Testing. A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as Gray Box Testing.

Fraud. Fraud is a type of illegal act involving the obtaining of something of value through willful misrepresentation.

Freeware. Software available to the public free of charge. Many viruses have been transmitted in freeware.

FTP. See File Transfer Protocol.

GAGAS. See Generally Accepted Government Auditing Standards

Gateway. A network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. In enterprises, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the gateway is the ISP (Internet Service Provider) that connects the user to the Internet.

General Controls. General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They include an entity-wide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls. These controls are more procedural-oriented in nature.

Generalized Audit Software. Computer programs used by auditors to locate and process data contained in an entity's computer-based records. The programs perform such functions as rearranging the data in a format more useful to the auditors, comparing records, selecting samples, making computations, and documenting the audit procedures performed. This software is compatible with a wide variety of different computer systems.

Generalized Testing. A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as Black Box Testing.

Generally Accepted Government Auditing Standards (GAGAS). GAO Publication, GAO-07-731G, dated July 2007, a.k.a. Yellow Book. It provides standards and guidance for use by government auditors to ensure that they maintain competence, integrity, objectivity, and independence in planning, conducting, and reporting their work, and are to be followed by auditors and audit organizations when required by law, regulation, contract, agreement, or policy.

Gray Box Testing. See Focused Testing.

Hacker. A person who attempts to enter a system without authorization from a remote location. The term often refers to any programmer, but its true meaning is someone with a strong technical background who is "hacking away" at the bits and bytes.

Hard Copy. Computer output in printed form, such as printed listings, reports, and summaries.

Header Label. A machine-readable record at the beginning of a file that identifies the file.

Hierarchical Data Base. A model for organizing data into a tree-like structure. The structure allows repeating information using parent/child relationships: each parent can have many children but each child only has one parent. The most recognized example of hierarchical model data base is IMS designed by IBM.

Host. Generally means a device (mainframe computer, large server, etc.) or program that provides services to some smaller or less capable device or program.

Hot Site. A fully operational off-site 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 commonly used to connect segments of a local area network (LAN). 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.

Hypertext Transfer Protocol (HTTP). The set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

IDS. See Intrusion Detection System.

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.

Information and Communication. The fourth of five interrelated components of internal control. Includes the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for the generation, collection, processing, dissemination, and disposal of information.

Information System (IS). A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System (IS) Control. As defined in GAGAS, information system (IS) controls consist of those internal controls that are dependent on information systems processing and include general controls and application controls.

Information System (IS) Risk. The likelihood that a loss of confidentiality, integrity, or availability could occur that would materially/significantly affect the audit objectives.

Information Technology (IT). Encompasses automated means of originating, processing, storing, and communicating information, and includes recording devices, communications systems, computer systems (including hardware and software components and data), and other electronic devices. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Inherent Risk. The likelihood that a loss of confidentiality, integrity, or availability could occur that would materially/significantly affect the audit objectives assuming that there are no related internal controls.

In-House. Refers to application software developed by the Application Programming staff within an organization.

Input. Any information entered into a computer, or the process of entering data into the computer.

Input Devices. Used to introduce various pieces of electronic information into the computer. Examples include keyboards, mice, scanners, electronic transfer from external sources and touch screens.

Instructive. Serving to instruct or inform, conveying instruction, knowledge, or information enlightening.

Integrated Test Facility (ITF) Technique. Using a set of dummy records and files, this technique enables test data to be continually evaluated when transactions are processed simultaneously with live input by online systems. Classified as a continuous audit approach.

Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The information provided by the systems is always accurate, reliable and timely.

Internal Control. Process, effected by management and other personnel of an entity, to provide reasonable assurance regarding achievement of objectives in the following categories: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations.

Internet. An international network of independently owned computers that operates as a giant computing network. Data on the Internet are stored on “Web Servers”, computers scattered throughout the world.

Internet Message Access Protocol (IMAP). A protocol for retrieving e-mail messages from the mail server. IMAP was developed at Stanford University in 1986.

Internet Protocol (IP). The method or protocol by which data is sent from one computer to another on the Internet. Used in conjunction with Transmission Control Protocol (TCP), IP handles the address part of each packet to ensure that it gets to the correct destination.

Intranets. Private organization computer networks that use Internet software to link employees and business partners.

Intrusion. Any intentional violation of the security policy of a system.

Intrusion Detection System (IDS). Generally detects unwanted manipulations of computer systems, mainly through the Internet. The manipulations may take the form of attacks by crackers. An IDS cannot detect attacks with encrypted traffic. Used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, Trojan horses, and worms).

Intrusion Prevention System (IPS). A computer security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass. IPS technology is considered by some to be an extension of IDS technology.

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.

Job Control Language (JCL). A scripting language used on IBM mainframe operating systems to instruct the system on how to run a batch job or start a subsystem. The term “job control language” can also be used generically to refer to all languages which perform these functions, such as Burroughs’ WFL and ICL’s OCL.

Job Scheduling System Software. Used by most installations that process a large number of batch jobs. It can automate the process of setting up daily work schedules, and can automatically determine which jobs are to be submitted and admitted to the system for processing.

Key. A long stream of seemingly random bits used with cryptographic algorithms. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message.

Legacy System. Comprised of applications and data that have been inherited from languages, platforms, and techniques earlier than current technology.

Library Management Software. Used to facilitate effective and efficient management of the data center software inventory. Of particular importance is maintaining access to the production library.

Local Area Network (LAN). A group of computers and associated devices that share a common communications line or wireless link and the resources of a single processor or server within a limited area, typically a building or a small cluster of buildings.

Log. With respect to computer systems, to record an event or transaction.

Log On. The process of establishing a connection with, or gaining access to, a computer system or peripheral device.

Logical Access Control. The use of computer hardware and software to prevent or detect unauthorized access. For example, users may be required to input user identification numbers (ID), passwords, or other identifiers that are linked to predetermined access privileges.

Logical Security. Security over access to the electronic environment. This type of security may involve mechanisms such as perimeter protections, access control programs to enforce defined delegations of authority and more proactive mechanisms, such as challenge-response systems.

Mainframe. Industry term for a large computer, typically manufactured for commercial applications and other large-scale computing purposes. Historically, a mainframe is associated with centralized rather than distributed computing.

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. 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.

Malware. See Malicious Code.

Master File. A file of relatively permanent data or information that is updated periodically.

Material Weakness. A deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Materiality. An auditing concept regarding the relative importance of an amount or item. An item is considered not to be material when it is not significant enough to influence decisions or have an effect on the financial statements.

Media. Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Media Access Control (MAC). Data communication protocol sub-layer, also known as Medium Access Control, is a sub-layer of the data link layer specified in the seven-layer OSI model (layer 2). It provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multipoint network, typically a local area network (LAN) or metropolitan area network (MAN).

Metadata. Describes how and when and by whom a particular set of data was collected, and how the data is formatted. Metadata is essential for understanding information stored in data warehouses and has become increasingly important in XML-based Web applications.

Microcomputer. Generally synonymous with personal computer (PC), or a computer that depends on a microprocessor. Designed to be used by individuals, whether in the form of PCs, workstations or notebook computers.

Microwave Transmission. Transmission using electromagnetic waves of certain radio frequencies.

Middleware. Another term for an application programmer interface (API). It refers to the interfaces that allow programmers to access lower- or higher-level services by providing an intermediary layer that includes function calls to the services.

Minicomputer. A mid-sized computer. In size and power, minicomputers lie between workstations and mainframes. It is a multiprocessing system capable of supporting from 4 to about 200 users simultaneously.

Modem. A device or program that enables a computer to transmit data over telephone lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modulator/demodulator converts between these two forms.

Monitoring. The fifth of five interrelated components of internal control. A process that assesses the quality of internal control performance over time.

Multifarious. Numerous and various; greatly diverse or manifold.

Network. Represents a series of points or nodes interconnected by communications paths. Networks can interconnect with other networks and contain sub-networks.

Network Administration. The function responsible for maintaining secure and reliable network operations. This function serves as a liaison with user departments to resolve network needs and problems.

Network Interface Cards (NICs). Links the computers and possibly printers and other devices to the network. They contain unique addresses that permit identification of each “node” in the network and permit the routing of data across the network.

Network Management Software. Provides a set of functions to control and maintain the network, and provides detailed information about the status of all network components (line status, active terminal, length of message queues, line error rate, and volume of traffic over the line).

Network Sniffing. A hacker attack that can occur from any station on a network, and can be difficult or impossible to detect. Ethernet-based Internet traffic, as used by most corporate networks, is generally implemented locally as a broadcast technology, and includes plain text and encrypted passwords, as well as other content such as Web addresses, e-mail messages, and instant messages. Network switches are often put into place to remove the risk of network sniffing, but it is possible to spoof the switches or attack the switches and gain access to internal traffic.

Network Switch. See Switch.

Network Weaving. A computer hacking technique whereby the intruder uses several telecommunication networks in a series to avoid detection.

Node. A connection point, either a redistribution point or an end point for data transmissions.

Nonrepudiation. The ability to prevent senders from denying that they have sent messages and receivers from denying that they have received messages.

Not Sufficiently Reliable. Significant errors or incompleteness exist in some or all of the key data elements and using the data would probably lead to an incorrect or unintentional message.

Object Code. The machine code generated by a source code language processor such as an assembler or compiler. 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.

Offline. Pertaining to peripheral devices or equipment not in direct communication with the central processing unit of the computer.

Off-the-Shelf Software. Software that is marketed as a commercial product, unlike custom programs that are privately developed for a specific client. See COTS.

Online. Pertaining to peripheral devices or equipment in direct communication with the central processing unit of the computer.

Online Programming Facilities. Allows application programmers to interactively enter, modify, and delete programming codes, and also allows programmers to interactively compile and store programs (source and object) on the computer, and list programs.

Operating System Software. The programs and routines used to control the operations of the computer. Some of the functions performed by the operating system are controlling the execution of application programs, allocating use of systems devices such as disks and printers, maintaining a log of system use, and coordinating communication between the computer and users. UNIX, Windows 98, 2000, and NT, DEC's VMS, IBM's OS/2, AIX, and OS/390 are all examples of operating systems.

Operational Controls. The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

Output. Data/information produced by computer processing, such as graphic display on a terminal, hard copy, or an electronic print file.

Output Devices. Used to provide evidence of what has been stored and/or processed within the computer. Examples include video display screens, speakers, electronic transfer to external sources (through devices such as modems), printers and disk drives.

Override. Decision made by entity management or operation staff to bypass established control(s) to allow a transaction or transactions that would otherwise be rejected by the system controls to be processed.

Owner. Manager or director who has responsibility for a computer resource, such as a data file or application program.

Packet. The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, etc.) is sent from one place to another, it is divided into individual packets that may travel different routes through the Internet or network and then are reassembled into the original file at the receiving end.

Parallel Simulation Technique. An attempt to simulate or duplicate the entity's actual processing results by writing a routine using an audit software package or packaged accounting software. Classified as a non-continuous audit approach.

Password. A confidential character string used to authenticate an identity or prevent unauthorized access.

Patch. A new section of coding added in a rough or expedient way to modify a program. Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software.

Peer-to-Peer File Sharing. Refers to providing and receiving files over a network, where files are stored on and served by workstations and involves both downloading and uploading of files.

Penetration Testing. Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.

Perfidy. A deliberate breach of faith or trust or an act or instance of faithlessness or treachery.

Peripheral. A hardware unit that is connected to and controlled by a computer, but that is external to the CPU. These devices provide input, output, or storage capabilities when used in conjunction with a computer.

Personnel Controls. This type of control involves screening individuals prior to their authorization to access computer resources. Such screening should be commensurate with the risk and magnitude of the harm the individual could cause.

Phishing. Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Physical Access Control. This type of control involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment.

Physical Security. Mechanisms to provide physical security over data, hardware, software, and programs. They may involve passive perimeter protections, such as fences and locks, as well as more proactive mechanisms, such as human guards and electronic personal recognition systems.

Plain Text. Data input to the Cipher (Encryption) or output from the Inverse Cipher (Decryption).

Platform. An underlying computer system on which application programs can run. Windows 2000, XP, and NT, and IBM's OS/2, AIX, and OS/390 are all examples of operating system platforms.

Post Office Protocol (POP). A protocol used to retrieve e-mail from a mail server. There are actually two versions of POP. The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

Preventive Controls. Actions taken to deter undesirable events from occurring, i.e., internal controls designed to deter problems before they arise.

Primary Key. Contains a unique value for each record in the data base file.

Primary Storage. Also known as main storage or memory, it is the main area in a computer in which data is stored for quick access by the computer's processor. Referred to as RAM (random access memory) on today's smaller computers.

Private Key Encryption. Also known as symmetric encryption, is a form of cryptography in which the key used to encrypt a message is also used to decrypt the message.

Privileged Account. Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts.

Process. Systematic sequences of operations to produce a specified result. This includes all functions performed within a computer such as editing, calculating, summarizing, categorizing, and updating.

Processing. The execution of program instructions by the computer's CPU.

Production Environment. The system environment where the entity performs its operational information processing activities.

Production Programs. Programs that are being used and executed to support authorized organizational operations. Such programs are distinguished from "test" programs that are being developed or modified, but have not yet been authorized for use by management.

Profile. A set of rules that describe the nature and extent of access to available resources for a user or group of users with similar duties, such as accounts payable clerks.

Program. A set of related instructions that, when followed and executed by a computer, perform operations or tasks. Application programs, user programs, system programs, source programs, and object programs are all software programs.

Program Analysis Techniques. Techniques for testing programmed control activities that involve the examination of computer-generated flowcharts of application programs.

Program Flowchart. A graphic representation of the major steps and logic of a computer program.

Programmer. A person who designs, codes, tests, debugs, and documents computer programs.

Proscription. The act of proscribing: prohibition or the condition of having been proscribed: outlawry.

Protocol. The special set of rules that end points in a telecommunication connection use when they communicate. Examples of common protocols are TCP, IP, HTTP, and FTP.

Proxy Server. A server (a computer system or an application program) which services the requests of its clients by forwarding requests to other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource by connecting to the specified server and requesting the service on behalf of the client.

Public Access Controls. A subset of access controls that apply when an entity application promotes or permits public access. These controls protect the integrity of the application and public confidence in the application and include segregating the information made directly available to the public from official entity records.

Public Key Encryption. Also known as asymmetric encryption, is a form of cryptography in which the key pairs are used. A user has a pair of cryptographic keys – a public key and a private key. The private key is kept secret, while the public key may be widely distributed. One key is used to encrypt a message and the other key is used to decrypt it.

Public Key Infrastructure (PKI). A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Query. The process of extracting data from a database and presenting it for use.

Read Access. This level of access provides the ability to look at and copy data or a software program.

Real-Time System. A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed.

Record. A group of related items or fields of data handled as a unit.

Redundant Array of Independent Drives (RAID). A technology that employs the simultaneous use of two or more hard disk drives to achieve greater levels of performance, reliability, and /or larger data volume sizes.

Relational Data Base. A collection of data items organized as a set of formally-described tables from which data can be accessed or reassembled in many different ways without having to reorganize the database tables. Examples of relational data bases are Oracle's ORACLE and Microsoft's ACCESS.

Relevance of Evidence. Audit evidence is relevant when the evidence is relevant to the assertion about which the evidence is being gathered. It is one aspect of the quality of audit evidence, the other being the reliability of evidence.

Reliability. The capability of hardware or software to perform as the user expects and to do so consistently, without failures or erratic behavior.

Reliability of Evidence. We can rely on the processing and output being generated by the system.

Remote Access. The process of communicating with a computer located in another place over a communications link.

Remote Job Entry (RJE). With respect to computer systems with locations geographically separate from the main computer center, submitting batch processing jobs via a data communications link.

Report of the Service Auditor. A report issued by the auditor of a service center to attest to the internal control of a computer service center. User auditors make use of these reports in considering the internal control over data processing performed for the entity by the service center. Often referred to as a "SAS 70" report.

Repudiation. The denial by one of the parties to a transaction or participation in all or part of that transaction or of the content of communications related to that transaction.

Risk. The level of impact on entity operations (including mission, functions, image, reputation), entity 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 Analysis. The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.

Risk Assessment. The second of five interrelated components of internal control. The entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.

Router. A device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. A device that connects any number of local area networks (LANs). Routers use headers and a forwarding table to determine where packets go, and they use ICMP (Internet Control Message Protocol) to communicate with each other and configure the best route between any two hosts.

Scanning. A computer hacking technique whereby the intruder performs a methodical search for valid access codes or trap doors.

Schema. The overall logical structure of the data base.

SDLC. See System Development Life Cycle.

Secondary Key. Used for file linkage, may occur in more than one record in the data base file.

Secondary Storage. Sometimes called auxiliary storage, it is all data storage that is not currently in a computer's primary storage or memory. An additional synonym is external storage. In a personal computer, secondary storage typically consists of storage on the hard disk and on any removable media, if present, such as a floppy disk, CD, DVD, flash drive or external hard drive.

Secure Socket Layer (SSL). A protocol developed by Netscape for transmitting private documents via the Internet. SSL used a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with the “https:” instead of “http:” protocol identifier.

Security Controls. The management, operational, and technical 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 Software. See Access Control Software.

Segregation/Separation of Duties. A basic control that prevents or detects errors and irregularities by assigning responsibility for initiating transactions, recording transactions and custody of assets to separate individuals. Commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

Sequential Access. A storage technique in which data are read and written in linear (e.g., account number) sequence. A magnetic tape drive is a sequential storage device.

Server. A computer program that provides services to other computer programs (and their users) in the same or other computers. The computer that a server program runs in is also frequently referred to as a server. For example, these computers can function as application, chat, fax, FTP (file transfer protocol), telnet, web, database, proxy, mail, file or print servers.

Service Auditor. An independent auditor hired by the service organization to provide a report on internal controls at the service provider. See Service Organization.

Service Bureau. A computer facility that provides data processing services to clients on a continual basis.

Service Organization. Outside 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.

Service Set Identifier (SSID). A name used to identify particular wireless local-area-networks (LANs) to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one.

Simple Mail Transport Protocol (SMTP). The standard e-mail protocol on the Internet. A protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another. The messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

Shareware. Software available to anyone paying the cost of reproducing it. It is also a source of viral infections.

Smart Card. A credit card-sized token that contains a microprocessor and memory circuits for authenticating a user of computer, banking, or transportation services.

SMF. See System Management Facility.

Sniffer. Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

Social Engineering. A method used by hackers to obtain passwords for unauthorized access. For example, a hacker may call an authorized user of a computer system and pose as a network administrator to gain access.

Software. Consists of programs (sets of instructions to the computer), procedures and rules that regulate the operation of a computer system.

Software Virus. A program that can attach itself to a legitimate program and modify other programs and systems. A virus may cause the loss of data or programs on a system.

Source Code. Human-readable program statements written in a high-level or assembly language, as opposed to object code, which is derived from source code and designed to be machine-readable.

Source Document. Information that is the basis for entry of data into a computer.

Special Publications (SPs). The 800-series guidance documents published by NIST (National Institute of Standards and Technology) to assist federal agencies in implementing the FISMA of 2002 and in managing cost-effective programs to protect their information and information systems.

Spoofing. A computer hacking technique whereby the intruder attempts to gain information about a system by deception. One form of spoofing is faking the sending address of a transmission in order to gain illegal entry into a secure system.

Spyware. Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.

Standards for Internal Controls in the Federal Government. GAO Publication, GAO/AIMD-00-21.3.1, dated November 1999. Issued to comply with FMFIA of 1982. Adopted the definition, objectives, and five interrelated components as published in the Internal Control – Integrated Framework (COSO Report).

Steganography. A technique that hides the existence of a message (for example, by embedding it within another message) and may be used where encryption is not permitted or to hide information in a encrypted file in case the encrypted file is deciphered.

Subschema. A particular user’s logical view of a part of the data base.

Subsystem. A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

Sufficiency of Evidence. The quantity and appropriate quality of evidence (i.e., appropriate relevance and reliability) that an auditor gathers to form their opinion on the financial statements.

Sufficiently Reliable. The likelihood of significant errors or incompleteness is minimal and the use of the data would not lead to an incorrect or unintentional message.

Supervisor Call (SVC). A supervisor call instruction interrupts a program being executed and passes control to the supervisor so that it can perform a specific service indicated by the instruction.

Switch. In networks, a small hardware device that filters and forwards packets between local area network (LAN) segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI (Open Systems Interconnection) Reference Model and therefore support any packet protocol. The switch provides the actual path for the packet in and out of a gateway. Synonymous with the term “Network Switch.”

Switcheroo. A computer hacking technique whereby the intruder switches back and forth between benign activity and hacking to avoid discovery.

System. See Information System.

System Administrator. The person responsible for administering use of a multi-user computer system, communications system, or both.

System Development Life Cycle (SDLC). The policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle.

System Management Facility (SMF). An IBM control program that provides the means for gathering and recording information that can be used to evaluate the extent of computer system usage.

System Privilege. Ability of the user within the database to interact with the database itself. They include: CREATE, ALTER, DROP, CONNECT, and AUDIT, among many others.

System Programmer. A person who develops and maintains system software.

System Software. The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. 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 program code.

Tagging and Tracing. A technique for testing programmed control activities in which selected transactions are tagged when they are entered for processing. A computer program provides a printout of the steps in processing the tagged transactions that may be reviewed by the auditors.

Tape and Disk Management Software. Tracks and lists tape/disk resources needed for data center processing (e.g., DSNs [data set names], specific device location, creation date, tape security BLP [bypass label processing])

TCP. See Transmission Control Protocol.

TCP/IP. See Transmission Control Protocol/Internet Protocol.

Technical Controls. See Logical Access Control.

Telecommunications. The electronic transmission of information by radio, wire, fiber optics, microwave, laser, and other electromagnetic systems.

Terminal. A device consisting of a video adapter, a monitor, and a keyboard.

Test Data Technique. Using a set of hypothetical (dummy) transactions to audit the edit checks, programmed checks and program logic in the actual production computer programs. Classified as a non-continuous audit approach.

Test Facility. A processing environment that is isolated from the production environment and dedicated to testing and validating systems and/or their components.

Testing of Controls. Tests include inquiries, inspection of documents or electronic files, observation of the application of the control and reprocessing transactions.

Threat. Any circumstance or event with the potential to adversely impact entity operations (including mission, functions, image, or reputation), entity assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Token. In authentication systems, some type of physical device (such as a card with a magnetic strip or a smart card) that must be in the individual's possession in order to gain access. The token itself is not sufficient, the user must also be able to supply something memorized, such as a personal identification number (PIN).

Token Ring. A local area network in which all computer are connected in a ring or star topology and a bit-or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time. Most widely-used protocol on local area networks after Ethernet.

Topologies. Arrangement of mapping of network elements.

Transaction. A discrete activity 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 money and entered in accounting records.

Transaction Data. The finite data pertaining to a given event occurring in a business process. The result of this process is in the form of documents or postings, such as purchase orders and obligations.

Transaction Data Input. Relates to controls over data that enter the application (e.g., data validation and edit checks).

Transaction Data Output. Relates to controls over data output and distribution (e.g., output reconciliation and review).

Transaction Data Processing. Relates to controls over data integrity within the application (e.g., review of transaction processing logs).

Transaction Processing. A type of computer processing in which the computer responds immediately to user requests. Each request is considered to be a transaction. Automatic teller machines for banks are an example of transaction processing.

Transmission Control Protocol (TCP). A connection-based Internet protocol that supports reliable data transfer connections. A set of rules used with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. TCP takes care of keeping track of all of the individual units (packets) of data that the message is divided into for efficient routing through the Internet.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that encompasses media access, packet transport, session communications, file transfer, electronic mail, terminal emulation, remote file access and network management. TCP/IP provides the basis for the Internet.

Transmission Media. Used to connect individual devices to the network and to each other, as well as connecting multiple networks together. Includes wireless media, cables, gateways, routers, hubs and switches.

Trojan Horse. A type of virus whereby program routines are secretly hidden inside legitimate programs. Often viruses and worms attach themselves to legitimate programs, becoming Trojan Horses and spreading to other systems.

Tunneling. The term tunneling protocol is used to describe when one network protocol called the payload protocol is encapsulated within a different delivery protocol (e.g., VPN functionality). Reasons to use tunneling include carrying a payload over an incompatible delivery network, or to provide a secure path through an untrusted network. Tunneling can also be used to “sneak through” a firewall. A protocol that is blocked by the firewall is “wrapped” inside a protocol that is NOT blocked by the firewall, such as HTTP. If the firewall policy has not been written to exclude this kind of “wrapping”, this trick can be used to get around the intended firewall policy.

Undetermined Reliability. The review of some of the related information or testing raises questions about the data’s reliability or there is too little information to judge reliability.

Uninterruptible Power Supply (UPS). Provides short-term backup power from batteries for a computer system when the electrical power fails or drops to an unacceptable voltage level.

UNIX. A multitasking operating system originally designed for scientific purposes that have subsequently become a standard for midrange computer systems with the traditional terminal/host architecture. UNIX is also a major server operating system in the client/server environment.

Upload. The process of transferring a copy of a file from a local computer to a remote computer by means of a modem or network.

User. The person who uses a computer system and its application programs to perform tasks. Commonly referred to as the “end-user.”

User Auditor. The auditor of the user organization.

User Control Activities. Controls performed by users of computer information to test its accuracy and completeness.

User Identification (ID). A unique identifier assigned to each authorized computer user.

User Privilege. Right to execute a particular type of Microsoft SQL server statement, or a right to access another user’s object.

User Profile. A set of rules that describes the nature and extent of access to each resource that is available to each user.

Utility Program. System software used to perform system maintenance and routines that are frequently required by the system during normal processing operations. Types of utility software programs include: Flow Charters, Data Manipulation Utilities, Test Data Generators, etc.

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. See Validity Control.

Validity Control. Controls designed to provide reasonable assurance (1) that all recorded transactions actually occurred (are real), relate to the entity, and were properly approved in accordance with management's authorization, and (2) that output contains only valid data.

Validity of Data. The accuracy of data which is used to determine the extent of reliance that can be placed on the data.

Verifying File Integrity. Proving that the totality of data in the file is correct.

Virtual Private network (VPN). A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with quasi-secure access to their organization's network. A VPN is viewed as a protected IS link utilizing tunneling, security controls, and end-point address translation giving the impression of a dedicated line.

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 Assessment. Formal description and evaluation of the vulnerabilities in an information system.

War Biking. Essentially the same as war driving but it involves searching for wireless networks while on a moving bicycle or motorcycle. This activity is sometimes facilitated by the mounting of a wifi-capable device on the vehicle itself.

War Dialer. Software packages that sequentially dial telephone numbers, recording any numbers that answer.

War Driving. Involves simply driving around in a car with a laptop computer looking for accessible wireless computer networks. Once an unsecured network is found, the intruders would hack into the system and install "sniffer programs" to capture specific information.

Web Application. An application that is accessed via the web over a network such as the Internet or an intranet. The ability to update and maintain Web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity.

Web Service. A software system designed to support interoperable machine to machine interaction over a network. It encompasses many different systems, but in common use the term refers to clients and servers that communicate using XML messages.

White Box Testing. See Detailed Testing.

Wide Area Network (WAN). A communication network that interconnects computers within a large geographical area.

Wired Equivalent Privacy (WEP). A deprecated algorithm to secure wireless networks. Wireless networks broadcast messages using radio and are thus more susceptible to eavesdropping than wired networks. WEP is sometimes inaccurately referred to as a *Wireless Encryption Protocol*.

Wireless Access Point (WAP). A device that connects wireless communication devices together to form a wireless network. The WAP usually connects to a wired network, and can relay data between wireless devices and wired devices. Wi-Fi (wireless fidelity) is a commonly used wireless network in computer systems which enable connection to the Internet or other machines that have Wi-Fi functionalities. Wi-Fi networks broadcast radio waves that can be picked up by Wi-Fi receivers that are attached to different computers or mobile phones.

Wi-Fi Protected Access (WPA). The Wi-Fi (Wireless Fidelity) Protected Access (WPA) security protocol was designed to improve upon the security features of WEP for wireless communications. It is defined in IEEE's 802.11i standard.

Workstation. A microcomputer or terminal connected to a network. Workstation can also refer to a powerful, stand-alone computer that has considerable calculating or graphics capability.

World Wide Web (WWW). A sub-network of the Internet through which information is exchanged by text, graphics, audio and video.

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.

XML (Extensible Markup Language). A general-purpose specification for creating custom markup languages. It is classified as an extensible language because it allows its users to define their own elements. Its primary purpose is to facilitate the sharing of structured data across different information systems, particularly via the Internet, and it is used both to encode documents and to serialize data.