INSIDE:
Everything you've always wanted to know about DP . . .





# Glossary of EDP Terminology

Frederick Gallegos

*PAYOFF IDEA. Half the battle in understanding the intricacies of data processing is understanding its terminology and the words and phrases specific to EDP that have evolved over the years. This glossary offers the reader a good working base of these terms.*

**acceptance testing** The formal testing conducted to determine whether a software system satisfies its acceptance criteria, enabling the customer to determine whether to accept the system.

**access** The ability and the means necessary to approach, store, or retrieve data, or communicate with or make use of any resource of a computer information system.

**access category** An authorization classification that defines the resources in a computer-based system to which a user, program, or process is granted access.

**access control** The process of allowing only authorized users, programs, or other computer systems (i.e., networks) to access the resources of a computer system.

**access control mechanisms** Hardware, software, or firmware features and operating and management procedures in various combinations designed to detect and prevent unauthorized access and to permit authorized access to a computer system.

**access list** A catalog of users, programs, or processes and the specifications of the access categories to which each is assigned.

**access period** A segment of time, generally expressed on a daily or weekly basis, during which access rights prevail.

**access type** The nature of access granted to a particular device, program, or file; for example, read, write, execute, append, modify, delete, create.

**accountability** The quality or state that enables attempted and committed violations of computer systems security to be traced to individuals who may then be held responsible.

**accumulator** An area of storage in memory used to develop totals of units or items being computed.

**active wire-tapping** The attachment of an unauthorized device, such as a computer terminal, to a communications circuit to gain access to data by generating false messages or control signals or by altering the communications of legitimate users.

**Ada** A programming language that allows use of structured techniques for program design; concise but powerful language designed to fill government requirements for real-time applications.

**add-on security** The retrofitting of protection mechanisms, implemented by hardware, firmware and/or software, on a computer system that has become operational.

**administrative security** The management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data.

**alphabetic test** The check on whether an element of data contains only alphabetic or blank characters.

**alphanumeric** A character set that includes numeric digits, alphabetic characters, and other special symbols.

**analysis and design phase** The phase of the systems development life cycle in which an existing system is studied in detail and its functional specifications are generated.

**ANSI (American National Standards Institute)** The agency that recommends standards for computer hardware, software, and firmware design and use.

**arithmetic operator** In programming activities, a symbol representing an arithmetic calculation or process.

**arithmetic-logic unit (ALU)** A component of the computer's processing unit, where arithmetic and matching operations are performed.

**array** Consecutive storage areas in memory that are identified by the same name. The elements (groups) within these storage areas are accessed through subscripts.

**artificial intelligence (AI)** A field of study involving techniques and methods under which computers can simulate human intellectual activities, such as learning.

**ASCII (American Standard Code for Information Interchange)** A byte-oriented coding system based on an 8-bit code and used primarily to format information for transfer in a data communications environment.

**assembler language** A computer programming language in which alphanumeric symbols represent computer operations and memory addresses. Each assembler instruction translates into a single machine-language instruction.

**assembler program** A program language translator that converts assembler programs into machine code.

**assertion** A logical expression specifying a program state that must exist or a set of conditions that program variables must satisfy at a particular point during program execution.

**audio output** Voice synthesizers that create audible signals resembling a human voice out of computer-generated output.

**audio response system** The method of delivering output by using audible signals and transmitters that simulate a spoken language.

**audit** An independent review and examination of system records and activities in order to test for the adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, procedures.

**audit trail** A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of each event in a transaction from inception to output of final results.

**authentication** The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. Typically, a measure designed to protect against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

**authorization** The granting of right of access to a user, program, or process.

**automated security monitoring** The use of automated procedures to ensure that the security controls implemented within a computer system or network are not circumvented or violated.

**backup operation** A method of operation used to complete essential tasks (as identified by risk analysis) subsequent to the disruption of the information processing facility and continuing until the facility is sufficiently restored.

**backup procedures** Provisions made for the recovery of data files and program libraries and for the restart or replacement of computer equipment after the occurrence of a system failure or disaster.

**bar code** A series of solid bars of different widths used to encode data. This data can be read by special optical-character-reading devices.

**BASIC (Beginner's All-purpose Symbolic Instruction Code)** This programming language was designed in the 1960s to teach students how to program and to be easy to learn. The powerful language syntax was designed especially for the time-sharing systems.

**batch control** A computer information processing technique in which numeric fields are totaled and records are tabulated to provide a comparison check for subsequent processing results.
**between-the-lines entry** Access obtained through the use of active wiretapping by an unauthorized user to a momentarily inactive terminal of a legitimate user assigned to a communications channel.
**binary digit** A state of function represented by the digit 0 or 1.
**bit** A binary value represented by an electronic component that has a value of 0 or 1.
**block structure** In programming, a segment of code that can be treated as an independent module.
**blocking factor** The number of records appearing between interblock gaps on magnetic storage media.
**bounds checking** The testing of computer program results for access to storage outside of its authorized limits.
**bounds register** A hardware or firmware register that holds an address specifying a storage boundary.
**bpi (bits per inch)** A measurement of the density of data stored on magnetic media.
**branch** An alteration of the normal sequential execution of program statements.
**brevity lists** A coding system that reduces the time required to transmit information by representing long, stereotyped sentences with only a few characters.
**browsing** The searching of computer storage to locate or acquire information, without necessarily knowing whether it exists or in what format.
**bug** A coded program statement containing a logical or syntactical error.
**burst** The separation of multiple-copy printout forms into individual sheets.
**byte** The basic unit of storage for many computers; typically, one configuration consists of 8 bits used to represent data, plus a parity bit for checking the accuracy of representation.
**byte-digit portion** Usually, the four rightmost bits in a byte.

**CAD/CAM (computer-aided design/computer-aided manufacturing)** The interactive use of computers in the design and manufacturing of goods or products.
**CAI (computer-aided instruction)** The interactive use of a computer for instructional purposes. Software provides educational content to students and adjusts its presentation to the responses of the individual.
**callback** A procedure that identifies a terminal dialing into a computer system or network by disconnecting the calling terminal, verifying the authorized terminal against the automated control table, and then, if authorized, reestablishing the connection by having the computer system dial the telephone number of the calling terminal.
**certification** The acceptance of software by an authorized agent, usually after the software has been validated by the agent or its validity has been demonstrated to the agent.
**channel** A magnetic track running along a length of tape that can be magnetized in bit patterns to represent data.
**character** A single numeric digit, special symbol, or letter.
**check digit** A numeric digit that is used to verify the accuracy of a copied or transcribed number. The numeric digit is typically appended to the end of a number.
**chip** A wafer containing miniature electronic imprinted circuits and components.
**cipher system** A system in which cryptography is applied to plain text elements of equal length.
**ciphertext** Encoded text or signals produced through the use of cipher systems.
**COBOL (COmmon Business-Oriented Language)** A high-level programming language for business computer applications.
**CODASYL (COnference on DAta SYstems Languages)** A Department of Defense-sponsored group that studies the requirements and design specifications for a common business programming language.
**COM (computer output microfilm)** The production of computer output on photographic film.
**code system** Any system of communication in which groups of symbols represent plain text elements of varying length.
**coder** The individual who translates program design into executable computer code.

**coding** The activity of translating a set of computer processing specifications into a formal language for execution by a computer.

**communications security** The protection that ensures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons information of value that might be derived from the acquisition of telecommunications.

**compare** A computer-applied function that examines two elements of data to determine their relationship to one another.

**compartmentalization** The isolation of the operating system, user programs, and data files from one another in main storage in order to protect them against unauthorized or concurrent access by other users or programs. Also, the breaking down of sensitive data into small, isolated blocks to reduce risk to the data.

**compiler** A program that translates high-level computer language instruction into machine code.

**completeness** The property that all necessary parts of an entity are included. Completeness of a product often means that all requirements have been met by the product.

**compromise** Unauthorized disclosure or loss of sensitive information.

**compromising emanations** Electromagnetic emanations that convey data and that, if intercepted and analyzed, could compromise sensitive information being processed by a computer system.

**computer program** A series of operations that will perform a task when executed in logical sequence.

**computer security** The practice of protecting a computer system against internal failures, human error, attacks, and natural catastrophes, which might cause improper disclosure, modification, destruction, or denial of service.

**computer system** An interacting assembly of elements including at least computer hardware and usually software, data procedures, and people.

**computer system security** All of the technological safeguards and managerial procedures established and applied to computers and their networks, including related hardware, firmware, software, and data, to protect organizational assets and individual privacy.

**concealment systems** A method of keeping sensitive information confidential by embedding it in irrelevant data.

**concurrent processing** The capability of a computer to share memory with several programs and simultaneously execute the instructions provided by each.

**condition test** In a program, a comparison of two data items to determine whether one value is equal to, less than, or greater than the second value.

**conditional branch** The alteration of the normal sequence of program execution following the test of the contents of a memory area.

**confidentiality** A concept that applies to data that must be held in confidence and describes the status or degree of protection that must be provided for such data about individuals as well as organizations.

**configuration management** The use of procedures appropriate for controlling changes to a system's hardware, software, or firmware structure to ensure that such changes will not lead to a weakness or fault in the system.

**consistency** Logical coherency among all integrated parts; also, adherence to a given set of instructions or rules.

**console operator** Someone who works at a computer console to monitor operations and initiate instructions for efficient use of computer resources.

**constant** A value in a computer program that does not change during program execution.

**contingency plans** Plans for emergency response, backup operations, and post-disaster recovery maintained by a computer information processing facility as a part of its security program.

**control** Any protective action, device, procedure, technique, or other measure that reduces exposures.

**control break** A point during program processing at which some special processing event takes place. A change in the value of a control field within a data record is characteristic of a control break.

**control field** A field of data within a record used to identify and classify a record.
**control logic** The specific order in which processing functions will be carried out by a computer.
**control signals** Computer-generated signals for the automatic control of machines and processes.
**control statement** A command in a computer program that establishes the logical sequence of processing operations.
**control structure** A program that contains a logical construct of sequences, repetitions, and selections.
**control totals** Accumulations of numeric data fields that are used to check the accuracy of the input, processed, or output data.
**control unit** A component of the central processing unit that evaluates and carries out program processing and execution.
**control zone** The space surrounding equipment that is used to process sensitive information and that is under sufficient physical and technical control to preclude an unauthorized entry or compromise.
**controllable isolation** Controlled sharing in which the scope or domain of authorization can be reduced to an arbitrarily small set or sphere of activity.
**controlled sharing** The condition that exists when access control is applied to all users and components of a resource-sharing computer system.
**conversational program** A program that permits interaction between a computer and a user.
**conversion** The process of replacing an existing computer system with a new one.
**correctness** The extent to which software is free from design and coding defects (i.e., fault free). Also, the extent to which software meets its specified requirements and user objectives.
**cost-risk analysis** The assessment of the cost of potential risk of loss or compromise of data in a computer system without data protection versus the cost of providing data protection.
**cost/benefit analysis** Determination of the economic feasibility of developing a system on the basis of a comparison of the projected costs of a proposed system and the expected benefits from its operation.
**courseware** Computer programs used to deliver educational materials within computer-assisted instruction systems.
**CPU (central processing unit)** The part of the computer system containing the control and arithmetic-logic units.
**crosstalk** An unwanted transfer of energy from one communications channel to another.
**CRT (cathode-ray tube)** The display device for computer terminals, typically a television-like electronic vacuum tube.
**cryptanalysis** The deciphering of encrypted messages into plain text without initial knowledge of the key employed in the encryption algorithm.
**cryptographic system** The documents, devices, equipment, and associated techniques that are used as a unit to provide a single means of encryption.
**cryptography** The art or science that applies the principles, means, and methods for producing unintelligible plaintext and converting encrypted messages into intelligible form.
**cryptology** The field of study that encompasses both cryptography and cryptanalysis.

**data** Raw facts and figures that are meaningless by themselves. Data can be expressed in characters, digits, and symbols, which can represent people, things, and events.
**data capture** The process of collecting and encoding data for entry into a computer system.
**data communications** The transmission of data between more than one site through the use of public and private communication channels or lines.
**data contamination** A deliberate or accidental process or act that compromises the integrity of the original data.
**data dictionary** A document or listing defining all items or processes represented in a data flow diagram or used in a system.

**data element** The smallest unit of data accessible to a data base management system or a field of data within a file processing system.

**data flow analysis** A graphical analysis technique to trace the behavior of program variables as they are initialized, modified, or referenced during program execution.

**data integrity** The state that exists when computerized information or data is the same as that in the source documents and has not been exposed to accidental or malicious modification, alteration, or destruction.

**data management system** System software that supervises the handling of data required by programs during execution.

**data protection engineering** The methodology and tools used to design and implement data protection mechanisms.

**data representation** The manner in which data is characterized in a computer system and its peripheral devices.

**data security** The protection of data from accidental or malicious modification, destruction, or disclosure.

**data segment** A collection of data elements accessible to a data base management system; a record in a file processing system.

**data-dependent protection** The protection of data at a level that is commensurate with the sensitivity of the individual data elements rather than with the sensitivity of the entire file.

**data base** An integrated aggregation of data usually organized to reflect logical or functional relationships among data elements.

**DBA (data base administrator)** A person who is in charge of defining and managing the contents of a data base.

**DBMS (data base management system)** The software that directs and controls data resources.

**debugging** The process of correcting static and logical errors detected during coding. With the primary goal of obtaining an executable piece of code, debugging shares certain techniques and strategies with testing but differs in its usual ad hoc application and scope.

**decipher** The ability to convert, by use of the appropriate key, enciphered text into its equivalent plaintext.

**decrypt** Synonymous with **decipher**

**dedicated mode** The operation of a computer system such that the central computer facility, connected peripheral devices, communications facilities, and all remote terminals are used and controlled exclusively by the users or groups of users for the processing of particular types and categories of information.

**degauss** To erase, or demagnetize magnetic recording media (usually tapes) by applying a variable, alternating current (ac) field.

**design and implementation** A phase of the systems development life cycle in which a set of functional specifications produced during systems analysis is transformed into an operational system for hardware, software and firmware.

**digit** A single numeral representing an arithmetic value.

**direct access** The method of reading and writing specific records without having to process all preceding records in a file.

**direct organization** A method of file organization under which records are located on the basis of their keys and associated addresses on the storage media.

**disk address** The positional location of a data record on magnetic disk storage.

**diskette** A flexible disk storage medium most often used with microcomputers; also called a floppy disk.

**documentation** The written narrative of the development, workings, and operation of a program or system.

**downtime** A period of time in which the computer is not available for operation.

**DSS (decision support system)** A computer information system that helps executives and managers formulate policies and plans. This support system enables the user to access information and assess the likely consequences of their decisions through scenario projections.

**dump** The contents of a file or memory that is output as listings. These listings may be formatted.

**dynamic analysis** The execution of program code to detect errors by analyzing the code's response to input.



**dynamic processing** The technique of swapping jobs in and out of computer memory. This technique can be controlled by the assignment priority and the number of time slices allocated to each job.

**eavesdropping** The unauthorized interception of information-bearing emanations through methods other than wiretapping.
**EBCDIC (extended binary-coded decimal interchange code)** A data representation and code system based on the use of an 8 bit-byte.
**echo** The display of characters on a terminal output device as they are entered into the system.
**edit** The process of inspecting a data field or element to verify the correctness of its content.
**electromagnetic emanations** Signals transmitted as radiation through the air or conductors.
**electronic document file** A magnetic storage area that contains electronic images of papers and other communications documents.
**electronic journal** A computerized log file summarizing, in chronological sequence, the processing activities and events performed by a system. The log file is usually maintained on magnetic storage media.
**electronic mail** Formal or informal communications electronically transmitted or delivered.
**electronic office** An office that relies on word processing, computer systems, and communications technologies to support its operations.
**emanation security** The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from interception and analysis of compromising emanations.
**encipher** The process of converting plaintext into unintelligible form by means of a cipher system.
**encryption algorithm** A set of mathematically expressed rules for encoding information, thereby rendering it unintelligible to those who do not have the algorithm decoding key.
**end-to-end encryption** The encryption of information at the point of origin within the communications network and postponing of decryption to the final destination point.
**entrapment** The deliberate planting of apparent flaws in a system to detect attempted penetrations or confuse intruders about which flaws to exploit.
**EPROM (eraseable programmable read-only memory)** A memory chip that can have its circuit logic erased and reprogrammed.
**evolution checking** Testing to ensure the completeness and consistency of a software product at different levels of specification when that product is a refinement or elaboration of another.
**exception report** A management report that highlights abnormal business conditions. Usually, such reports prompt management action or inquiry.
**expert system** The application of computer-based artificial intelligence in areas of specialized knowledge.
**exposure** A form of possible loss or harm, such as erroneous recordkeeping, unmaintainable applications, or business interruptions that affect the profitability of the going concern.

**fail safe** The automatic termination and protection of programs or other processing operations when a hardware, software, or firmware failure is detected in a computer system.
**fail soft** The selective termination of nonessential processing affected by a hardware, software, or firmware failure in a computer system.
**failure access** An unauthorized and usually inadvertent access to data resulting from a hardware, software, or firmware failure in the computer system.
**failure control** The methodology used to detect and provide fail-safe or fail-soft recovery from hardware, software, or firmware failures in a computer system.

**Fair Credit Reporting Act** A federal law that gives individuals the right of access to credit information pertaining to them and the right to challenge such information.
**fault** A weakness of the system that allows someone to circumvent protective controls.
**feasibility study** An investigation of the legal, political, social, operational, technical, economic, and psychological effects of developing and implementing a system.
**federal computer fraud act** The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 outlaws unauthorized access to the federal government's computers and certain financial data bases as protected under the Right to Financial Privacy Act of 1978 and the Fair Credit Reporting Act of 1971.
**fetch protection** A system-provided restriction to prevent a program from accessing data in another user's segment of storage.
**fiche** A sheet of photographic film containing multiple microimages; a form of computer output microfilm.
**field** A basic unit of data, usually part of a record that is located on an input, storage, or output medium.
**file** An aggregation of data records organized on a storage medium for convenient location, access, and updating.
**file creation** The building of master or transaction files.
**file inquiry** The selection of records from files and immediate display of their contents on a terminal output device.
**file maintenance** The changing of a master file by changing the contents of existing records, adding new records, or deleting old records.
**file protection** The aggregate of all processes and procedures established in a computer system and designed to inhibit unauthorized access, contamination, or elimination of a file.
**file updating** The posting of transaction data to master files or maintenance of master files through record additions, changes, or deletions.
**firmware** Software or computer instructions that have been permanently encoded into the circuits of semiconductor chips.
**Foreign Corrupt Practices Act** The act covers an organization's system of internal accounting control and requires public companies to make and keep books, records, and accounts that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of company assets and to devise and maintain a system of sufficient internal accounting controls.
**formal analysis** The use of rigorous mathematical techniques to analyze the solution. The algorithms may be analyzed for numerical properties, efficiency, and correctness.
**format** The physical arrangement of data characters, fields, records, and files.
**FORTRAN (FORmula TRANslation)** A high-level programming language developed primarily to translate mathematical formulas into computer code.
**formulary** A technique for permitting the decision to grant or deny access to be determined dynamically at access time rather than at the time the access list is created.
**front-end computer** Sometimes called a front-end processor; a computer that offloads input and output activities from the central computer so it can operate primarily in a processing mode.
**function** In computer programming, a processing activity that performs a single, identifiable task.
**functional specification** The main product of systems analysis, which presents a detailed logical description of the new system. It contains sets of input, processing, storage, and output requirements specifying what the new system can do.
**functional testing** The application of test data derived from the specified functional requirements without regard to the final program structure.

**general-purpose computer** A computer that can be programmed to perform a wide variety of processing tasks.
**graphic output** Computer-generated output in the form of pictures, charts, and line drawings.
**graphics terminal** An output device that displays pictures, charts, and line drawings, typically a high-resolution CRT.

**handshaking procedure** A dialogue between a user and a computer, two computers, or two programs to identify a user and authenticate his or her identity. This is done through a sequence of questions and answers that are based on information either previously stored in the computer or supplied to the computer by the initiator of the dialogue.

**hardware** The physical equipment or devices included in computer systems.

**humanware** Computer programs that interface or communicate with users via voice-integrated technology, interpret user-specified commands, and execute or translate commands into machine-executable code.

**IBG (interblock gap)** A blank space appearing between records or groups of records on magnetic storage media.

**identification** The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to the computer system.

**impact printer** A hard-copy device on which a print mechanism strikes against a ribbon to create imprints on paper. Some impact printers operate one character at a time, while others strike an entire line at a time.

**impersonation** An attempt to gain access to a system by posing as an authorized user.

**implementation** The specific activities within the systems development life cycle through which the software portion of the system is developed, coded, debugged, tested, and integrated with existing or new acquired hardware.

**incomplete parameter checking** A system fault that exists when all parameters have not been fully checked for correctness and consistency by the operating system, thus leaving the system vulnerable to penetration.

**indexed sequential filing** A file organization method in which records are maintained in logical sequence and indexes, or tables, are used to reference their storage addresses. The method allows direct and serial access to records.

**information** Meaningful data; the result of processing data by computer or other means.

**input controls** Techniques and methods for verifying, validating, and editing data to ensure that only correct data enters a system.

**inquiry processing** The process of selecting a record from a file and immediately displaying its contents.

**inspection** A manual analysis technique that examines the program requirements, design or code in a formal and disciplined manner to discover errors.

**instrumental input** The capture of data and its placement directly into a computer by machines.

**integrated circuit** A miniature microchip incorporating circuitry and semiconductor components. The circuit elements and components are created as a part of the same manufacturing process.

**integration testing** The orderly progression of testing in which software, hardware, or both are combined and tested until all intermodule communication links have been integrated.

**integrity checking** The testing of programs to verify the soundness of a software product at each phase of development.

**interdiction** Impeding, or denying someone, the use of system resources.

**interface analysis** The checking and verification process that ensures that intermodule communication links are performed correctly.

**interleaving** The alternating execution of programs residing in the memory of a multiprogramming environment.

**internal accounting control** The process of safeguarding the accounting functions and processes of a business. This process includes validating that the accounting system complies with the appropriate, generally accepted accounting principles and that audit trails exist for verification of all processes.

**internal control** The method of safeguarding business assets, including verifying the accuracy and reliability of accounting data, promoting operational efficiency, and encouraging adherence to prescribed organizational policies and procedures.

**investigation** The phase of the systems development life cycle in which the problem or need is identified and a decision is made on whether to proceed with a full-scale study.
**isolation** The separation of users and processes in a computer system from one another as well as from the protection controls of the operating system.

**job** A complete set of programs to be executed in sequence on a computer.
**job accounting system** A set of systems software that can track the services and resources used by computer system account holders.
**job queue** A set of programs held in temporary storage and awaiting execution.

**K** The symbol representing the value 1,024; thus, 2K bytes is equivalent to 2,048 bytes.
**key** A control field in a record that uniquely identifies the record or classifies it as a member of a segment of records within a file. In cryptography, a sequence of symbols that controls encryption and decryption.
**key generation** The origination of a key or set of distinct keys.
**key-to-disk device** A keyboard unit that records data as patterns of magnetic spots onto magnetic disks.
**key-to-tape device** A keyboard unit that records data as patterns of magnetic spots onto magnetic tape.
**kilobyte (KB)** The equivalent of 1,024 bytes.

**language translator** Systems software that converts programs written in assembler or a higher-level language into machine code.
**laser printer** An output unit that uses intensified light beams to form an image on an electrically charged drum, then transfers the image to paper.
**limit check** An input control test that assesses the value of a data field to determine whether values fall within set limits.
**line printer** An output unit that prints alphanumeric characters a line at a time.
**link encryption** The application of online crypto-operations to a link of a communications system, so that all information passing over the link is encrypted in its entirety.
**linkage** The purposeful combination of data or information from one information system with that from another system in the hope of deriving additional information.
**lock/key protection system** A protection system that involves matching a key or password with a specified access requirement.
**logical error** A programming error that causes the wrong processing to take place in a syntactically valid program.
**logical file organization** The sequencing of data records in a file according to their key.
**logical operation** A comparison of data values within the arithmetic-logic unit. These comparisons show when one value is greater than, equal to, or less than a second value.
**logical operator** A symbol used in programming that initiates a comparison operation of two or more data values.
**logical organization** Data elements organized in a manner that meets the human and organizational processing needs.
**loophole** An error of omission or oversight in software, hardware, or firmware that permits circumventing the access control process.

**machine language** Computer instructions or code representing computer operations and memory addresses in a numeric form that is executable by the computer without translation.
**magnetic disk** A storage device consisting of metallic platters coated with an oxide substance that allows data to be recorded as patterns of magnetic spots.
**magnetic tape** A storage medium consisting of a continuous strip of coated plastic film wound onto a reel and upon which data can be recorded as defined patterns of magnetic spots.

**master file** A computerized file that contains semipermanent or permanent information and is maintained over a period time required by organizational policy.
**matrix display** The alphanumeric representation of characters as patterns of tiny dots within specific positions on a display terminal.
**matrix printer** A hard-copy printing device that forms alphanumeric characters with small pins arranged in a matrix of rows and columns.
**mature system** A fully operational system that performs all the functions it was designed to accomplish.
**media** The various physical forms (e.g., disk, tape, diskette) on which data is recorded in machine-readable formats.
**megabyte (MB)** The equivalent of 1,048,576 bytes.
**memory** The area in a computer that serves as temporary storage for programs and data during program execution.
**memory address** The location of a byte or word of storage in computer memory.
**memory bounds** The limits in the range of storage addresses for a protected region in memory.
**memory chips** A small integrated circuit chip with a semiconductor matrix used as computer memory.
**menu** A section of the computer program—usually the top-level module—that controls the order of execution of other program modules. Also, online options displayed to a user, prompting the user for specific input.
**MICR (magnetic ink character recognition)** An input method under which data is encoded in special ink containing iron particles. These particles can be magnetized and sensed by special machines and converted into computer input.
**microcomputer** A small microprocessor-based computer built to handle input, output, processing, and storage functions.
**microfilm** A film for recording alphanumeric and graphic output that has been greatly reduced in size.
**microprocessor** A single small chip containing circuitry and components for arithmetic, logical, and control operations.
**minicomputer** Typically a word-oriented computer whose memory size and processing speed falls between that of a microcomputer and medium-sized computer.
**multiaccess rights terminal** A terminal that may be used by more than one class of users; for example, users with different access rights to data or files.
**multiprocessing** A computer operating method under which two or more processors are linked and execute multiple programs simultaneously.
**multiprogramming** A computer operating environment in which several programs can be placed in memory and executed concurrently.
**mutually suspicious** Pertaining to a state that exists between interactive processes (systems or programs), each of which contains sensitive data and is assumed to be designed to extract data from the other and to protect its own data.

**nak attack** A penetration technique that capitalizes on an operating system's inability to handle asynchronous interrupts properly.
**natural language** A language that is used in communication with computers and that closely resembles English syntax.
**network** An integrated, communicating aggregation of computers and peripherals linked through communications facilities.
**networking** A method of linking distributed data processing activities through communication facilities.
**nonprocedural language** A programming language with fixed logic, which allows the programmer to specify processing operations without concern for processing logic.
**numeric test** An input control method to verify that a field of data contains only numeric digits.

**object program** A program that has been translated from a higher-level source code into machine language.

**office automation** The application of computer and other related technologies to office procedures.
**online processing** Often called interactive processing, an operation in which the user works at a terminal or other device that is directly attached or linked to the computer.
**operand** The portion of a computer instruction that references the memory address of an item to be processed.
**operating system** The various sets of computer programs and other software that monitor and operate the computer hardware and firmware to facilitate its use.
**operation code** The portion of the computer instruction that identifies the specific processing operation to be performed.
**optical character recognition (OCR)** An input method, under which handwritten, typewritten, or printed text can be read by photosensitive devices for input to computer.
**output controls** Techniques and methods for verifying that the results of processing conform to expectations and are communicated only to authorized users.
**overlapped processing** The simultaneous execution of input, processing, and output functions by a computer system.
**overwriting** The obliteration of recorded data by recording different data on the same surface.

**paging** A method of dividing a program into parts called pages and introducing a given page into memory as the processing on the page is required for program execution.
**parallel conversion** The concurrent use of old and new systems to validate the processing capability of the new system by its users.
**parity bit** A bit attached to a byte, used to check the accuracy of data storage.
**partition** A memory area assigned to a computer program during its execution.
**Pascal** A computer programming language designed especially for writing structured programs. This language is based on the use of a minimum set of logical control structures.
**passive wiretapping** The monitoring or recording of data while it is being transmitted over a communications link.
**password** A protected word or string of characters that identifies or authenticates a user, a specific resource, or an access type.
**penetration** A successful unauthorized access to a computer system.
**penetration profile** A delineation of the activities required to effect a penetration.
**penetration signature** The description of a situation or set of conditions in which a penetration might occur.
**penetration testing** The use of special programmer/analyst teams to attempt to penetrate a system in order to identify security weaknesses.
**performance monitor** A set of systems software that tracks service levels provided by a computer system.
**phased conversion** The system installation procedure that involves a stey-by-step approach for the incremental installation of one portion of a new system at a time.
**physical organization** The packaging of data into fields, records, files, and other structures to make them accessible to a computer system.
**piggyback entry** Unauthorized access to a computer system that is gained through another user's legitimate connection.
**PL/1 (Programming Language/1)** A general-purpose, high-level language that combines business and scientific processing features. The language contains advanced features for experienced programmers yet can be easily learned by novice programmers.
**plaintext** Intelligible text or signals that have meaning and can be read or acted upon without being decrypted.
**plotter** A graphic output device in which the computer drives a pen that draws on paper.
**preprocessors** Software tools that perform preliminary work on a draft computer program before it is completely tested on the computer.



**principle of least privilege** A security procedure under which users are granted only the minimum access authorization they need to perform required tasks.

**print suppress** The elimination of the printing of characters to preserve their secrecy; for example, the characters of a password as it is keyed by a user at a terminal or station on the network.

**Privacy Act of 1974** The federal law that allows individuals to know what information about them is on file and how it is used by all government agencies and their contractors.

**privacy protection** The establishment of appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of data records against anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

**privileged instructions** A set of instructions generally executable only when the computer system is operating in the executive state; for example, while handling interrrupts. These special instructions are typically designed to control the protection features of a computer system, such as the storage protection features.

**procedural language** A computer programming language in which the programmer must determine the logical sequence of program execution as well as the processing required.

**procedure division** A section of a COBOL program that contains statements that direct computer processing operations.

**process control** The activities involved in monitoring and controlling production and manufacturing processes.

**process description** A narrative that describes in sequence the processing activities that take place in a computer system and the procedures for completing each activity.

**processing controls** Techniques and methods used to make sure that processing produces correct results.

**processor** The hardware unit containing the functions of memory and the central processing unit.

**program analyzers** Software tools that modify or monitor the operation of an application program to allow information about its operating characteristics to be collected automatically.

**program development process** The activities involved in developing computer programs, including problem analysis, program design, process design, program coding, debugging, and testing.

**program maintenance** The process of altering program code or instructions to meet new or changing requirements.

**programmer** The individual who designs and develops computer programs.

**programmer/analyst** The individual who analyzes processing requirements and then designs and develops computer programs to direct processing.

**programming language** A language with special syntax and style conventions for coding computer programs.

**programming specifications** The complete description of input, processing, output, and storage requirements necessary to code a computer program.

**proof of correctness** The use of mathematical logic to infer that a relation between program variables assumed true at the program entry implies that another relation between program variables holds at program exit.

**protection ring** A hierarchy of access modes through which a computer system enforces the access rights granted to each user, program, and process, ensuring that each operates only within its authorized access mode.

**pseudoflaw** An apparent loophole deliberately implanted in an operating system program as a trap for intruders.

**PROM (programmable read-only memory)** Computer memory chips that can be programmed permanently to carry out a defined process.

**pseudocode** Program processing specifications that can be prepared as structured English-like statements, which can then be easily converted into source code.

**purging** The orderly review of storage and removal of inactive or obsolete data files.

**queue** A waiting line in which a set of computer programs are in secondary storage awaiting processing.

**RAM (random access memory)** Computer memory chips used to store programs and data temporarily during processing—a technology that is used heavily in microcomputers.
**random access** A method that allows records to be read from and written to a disk media without regard to the order of their record keys.
**real-time processing** Computer processing that generates output fast enough to support multiple activities being performed concurrently.
**real-time reaction** A response to a penetration attempt that, because the attempt is detected and diagnosed in time, can prevent actual penetration.
**record block** A group or collection of records appearing between interblock gaps on magnetic storage media. This group of records is handled as a single entity in computer processing.
**record blocking** A technique of writing several records to magnetic storage media in between interblock gaps or spaces.
**recovery** The restoration of the information processing facility or other related assets following physical destruction or damage.
**recovery procedures** The action necessary to restore a system's computational capability and data files after system failure or penetration.
**regression testing** The rerunning of test cases, which a program has previously executed correctly, to detect errors created during software correction or modification.
**remanence** The residual magnetism that remains on magnetic storage media after degaussing.
**report** Printed or displayed output that communicates the content of files and other activities. The output is typically organized and easily read.
**report program generator (RPG)** A nonprocedural programming language used for many business applications.
**report writing** The process of accessing data from files and generating it as information in the form of output.
**residue** Data left in storage after processing operations and before degaussing or rewriting has occurred.
**resource** In a computer system, any function, device, or data collection that can be allocated to users or programs.
**resource sharing** In a computer system, the concurrent use of a resource by more than one user, job, or program.
**risk analysis** An analysis that examines an organization's information resources, its existing controls, and its remaining organization and computer system vulnerabilities. It combines the loss potential for each resource or combination of resources with an estimated rate of occurrence to establish a potential level of damage in dollars or other assets.
**risk assessment** Synonymous with **risk analysis.**
**robotics** The use of automated equipment for production work and other mechanical tasks.
**ROM (read-only memory)** Computer memory chips with preprogrammed circuits for storing software such as word processors and spreadsheets.

**safeguard** Synonymous with **control.**
**sanitizing** The degaussing or overwriting of sensitive information in magnetic or other storage media.
**scavenging** The searching of residue for the purpose of unauthorized data acquisition.
**scheduling program** A systems program that schedules and monitors the processing of production jobs in the computer system.
**secure operating system** An operating system that effectively controls hardware, software, and firmware functions in order to provide the level of protection appropriate to the value of the data resources managed by this operating system.

**security audit** An examination of data security procedures and measures to evaluate their adequacy and compliance with established policy.

**security controls** Techniques and methods to ensure that only authorized users can access the computer information system and its resources.

**security filter** A set of software or firmware routines and techniques employed in a computer system to prevent automatic forwarding of specified data over unprotected links or to unauthorized persons.

**security kernel** The central part of a computer system (hardware, software, or firmware) that implements the fundamental security procedures for controlling access to system resources.

**security program** A systems program that controls access to data in files and permits only authorized use of terminals and other related equipment. Control is usually exercised through various levels of safeguards assigned on the basis of need to know.

**seepage** The accidental flow, to unauthorized individuals, of data or information that is presumed to be protected by computer security safeguards.

**selection** A program control structure, created in response to a condition test, in which one of two or more processing paths can be taken.

**semiconductor** Materials, used in electronic components, that possess electrical conducting qualities of conductors and resistors.

**sensitive information** Any information that requires protection and that should not be made generally available.

**sequential organization** The physical arrangement of records in a sequence that corresponds with their logical key.

**serial organization** The physical arrangement of records in sequence.

**serial processing** The processing of records in the physical order in which they appear in a file or on an input device.

**service program** An operating system program that provides a variety of common processing services to users, such as utility programs, librarian programs, and other software.

**simulation** The use of an executable model to represent the behavior of an object. During testing, the computational hardware, the external environment, and even the coding segments may be simulated.

**simultaneous processing** The execution of two or more computer program instructions at the same time in a multiprocessing environment.

**slave computer** A front-end processor that handles input and output functions for a host computer.

**software** Computer programs, procedures, rules, and possibly documentation and data pertaining to the operation of the computer system.

**software lifecycle** The period of time beginning when a software product is conceived and ending when the product is no longer available for use. The software life cycle is typically broken into phases, such as requirements, design, programming, testing, conversion, operations, and maintenance.

**sort** The arrangement of data into ascending or descending, alphabetic or numeric order.

**source document** The form that is used for the initial recording of data prior to system input.

**source program** The computer program that is coded in an assembler or higher-level programming language.

**spoofing** The deliberate inducement of a user or a resource to take incorrect action.

**spooling** A technique that maximizes processing speed through the temporary use of high-speed storage devices. Input files are transferred from slower, permanent storage and queued in the high-speed devices to await processing, or output files are queued in high-speed devices to await transfer to slower storage devices.

**stacked-job processing** A computer processing technique in which programs and data awaiting processing are placed into a queue and executed sequentially.

**standards audit** The check to ensure that applicable standards are properly used.

**statement testing** A test method of satisfying the criterion that each statement in a program be executed at least once during the program testing.

**static analysis** The direct analysis of the form and structure of a product that does not require its execution. It can be applied to the requirements, design, or code.

**storage media** Physical hardware on which programs and data are maintained over time in machine-readable format.
**structured design** A methodology for designing systems and programs through a top-down, hierarchical segmentation.
**structured programming** The process of writing computer programs, using logical, hierarchical control structures to carry out processing.
**subroutine** A segment of code that can be called up by a program and executed at any time from any point.
**subscript** A value used in programming to reference an item of data stored in a table.
**swapping** A method of computer processing in which programs not actively being processed are held on special storage devices and alternated in and out of memory with other programs by priority.
**symbolic evaluation** The process of analyzing the path of program execution through the use of symbolic expressions.
**symbolic execution** The analytical technique of dissecting each program path.
**syntax** The statement formats and rules for the use of a programming language.
**system integrity** The state that exists when there is complete assurance that, under all conditions, a computer system is based on the logical correctness and reliability of the operating system and the logical completeness of the hardware, software, and firmware that implement the protection mechanisms and data integrity.
**system integrity procedures** The procedure established to ensure that hardware, software, firmware, and data in a computer system maintain their state of original integrity and are not tampered with by unauthorized personnel.
**system test** The process of testing an integrated hardware/software system to verify that the system meets its specified requirements.
**systems analysis** The process of studying information requirements and preparing a set of functional specifications that identify what a new or replacement system should accomplish.
**systems design** The development of a plan for implementing a set of functional requirements as an operational system.
**systems software** The programs and other processing routines that control and activate the computer hardware facilitating its use.

**table** An area of computer memory containing multiple storage locations that can be referenced by the same name.
**table driven** An indexed file in which tables containing record keys (disk addresses) are used to retrieve records.
**tape management system** Systems software that assesses the given information on jobs to be run and produces information to operators and librarians regarding which data resources (e.g., tapes, disks) are needed for job execution.
**task management system** The systems software that allocates the processor unit resources according to priority scheme or other assignment methods.
**technological attack** An attack that can be perpetrated by circumventing or nullifying hardware, software, and firmware access control mechanisms rather than by subverting system personnel or other users.
**telecommunications** Any transmission, emission, or reception of signs, signals, writing, images, sounds, or other information by wire, radio, visual, satellite, or electromagnetic systems.
**teleprocessing** Information processing and transmission performed by an integrated system of telecommunications, computers, and person-machine interface equipment.
**teleprocessing security** The protection that results from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure or acquisition of information stored in or transmitted by a teleprocessing system.
**terminal identification** The means used to establish the unique identification of a terminal by a computer system or network.
**test data** Data that simulates actual data both in form and content and is used in evaluating a system or program before it is put into operation.
**test data generators** Computer software tools that help generate files of data that can be used to test the execution and logic of application programs.



**testing** The examination of the behavior of a program through its execution on sample data sets.
**threat monitoring** The analysis, assessment, and review of audit trails and other data collected to search out system events that may constitute violations or precipitate incidents involving data privacy.
**throughput** The process of measuring the amount of work a computer system can handle within a specified time frame.
**time-dependent password** A password that is valid only at a certain time of the day or during a specified interval of time.
**traffic flow security** The protection that results from those features in some cryptography equipment that conceal the presence of valid messages on a communications circuit, usually by causing the circuit to appear busy at all times or by encrypting the source and destination addresses of valid messages.
**transaction file** A collection of records containing data generated from the current business activity.
**transactional processing** The processing of transactions as they occur rather than in batches.
**trap door** A breach created intentionally in a computer system to collect, alter, or destroy data.
**Trojan horse** A computer program that is apparently or actually useful and contains a trap door.

**unit testing** The testing of a module for typographic, syntactic, and logical errors and for correct implementation of its design and satisfaction of its requirements.
**Universal Product Code (UPC)** An array of varied-width lines that can be read by special machines, such as OCR devices and converted into alphanumeric data. This method is used to mark merchandise for direct input of sales transactions.
**update** The file processing activity in which master records are altered to reflect the current business activity contained in transactional files.

**validation** The determination of the correctness, with respect to the user needs and requirements, of the final program or software produced from a development project.
**validation, verification, and test** Validation, verification, and testing, used as an entity to define a procedure of review, analysis, and testing throughout the software life cycle to discover errors, determine that functions operate as specified, and ensure the production of quality software.
**verification** The demonstration of consistency, completeness, and correctness of the software at and between each stage of the development life cycle.
**verify** The process of ensuring that transcribed data has been accurately keyboarded.
**virtual memory** A method of extending computer memory by using secondary storage devices to store program pages that are not being executed at the time.
**voice synthesizer** An input/output device that can either interpret and convert human speech into digital signals for computer processing or convert digital signals into audible signals that resemble human speech.

**walkthrough** A manual analysis technique in which the module author or developer describes the module's structure and logic to colleagues.
**word** In computer memory, a contiguous set of bits used as a basic unit of storage. Words are usually 8, 16, 32, or 64 bits long.
**word processing** The use of computers or other technology for the storage, editing, correction, revision, and production of textual files in the form of letters, reports, and documents.

---

Frederick Gallegos, CISA, CDE, is manager of Management Science Group, US General Accounting Office, Los Angeles, and a lecturer for Computer Information Systems Department, California State Polytechnic University, Pomona CA.

## NOTES