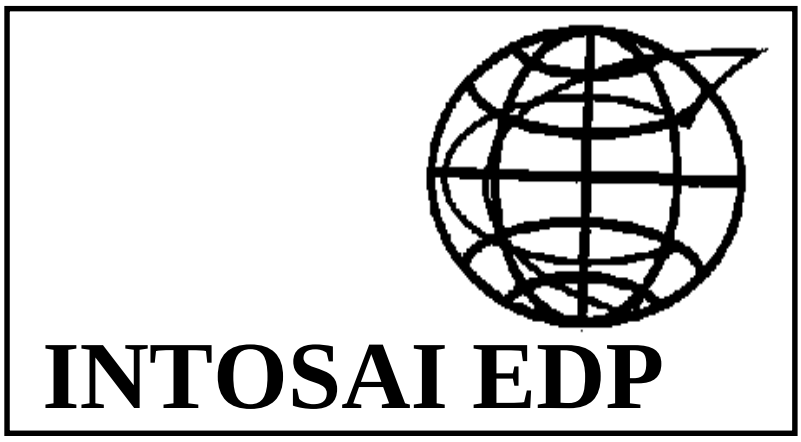

Information Systems Auditing

Glossary of Terms

Version 3, August 2001

Information Systems Auditing – Glossary of ICT Terms

Introduction

This glossary of terms is designed to help auditors who use the INTOSAI *Guide to IT Infrastructure Audit* - and other IT-related guides - to understand the terminology. Although the Glossary contains many definitions it is not a comprehensive dictionary. If the term you are looking for is not listed, we suggest that you try the excellent on-line dictionaries at …….

http://www.zdwebopedia.com or

http://whatis.techtarget.com/

The definitions provided here are those that are normally used in the context of managing IT-enabled projects and programmes, and in IT services and security. However, a word of caution! Some of the terms listed can mean different things in different contexts - for example the term 'network' can refer to a data communications network, or to a network diagram used in connection with planning the sequence of tasks in a project.

Hyperlinks are embedded to help navigate the Glossary - please ensure that you select the MS Word "web" toolbar option (View, toolbars, web) before using the Glossary.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Access controls	*Controls* that are designed specifically to reduce the risk of the unauthorised use of resources (including the use of resources in an unauthorised way), or damage to, or theft of resources. Access control mechanisms include a combination of *physical* (barriers, CCTV, security guards), *technical* (e.g. *passwords*, *biometrics*, computer logs) and *administrative* (e.g. personnel vetting, management supervision) controls (see *physical access*; *logical access*).
Accountability	An *information security* principle whereby *system* users are uniquely identifiable and are held responsible for their actions. Being able to identify users uniquely enables security violations to be traced to individuals; sharing *passwords* defeats this objective.
Active-X	Active X is an integration technology developed by Microsoft. Its main use is for *web pages*, which it can make more useful and, visually, more exciting. However, *Active X controls* have powerful processing ability, and the onus lies on the user whether or not to accept them. *Web browser* settings control whether Active X controls are to be downloaded and run, or whether they are blocked; however, blocking *Active X* may limit the *information* provided by the *web page* the user is trying access.
Active X controls	(See also *Active X*). Active X controls are objects in a *web page* that allow interactive between the user and the *web server*. Besides enlivening web pages for aesthetic value, controls can be used to create interactive forms for ordering merchandise, collecting *information*, and other purposes.
Activity	The lowest level of a *work breakdown structure*. A packet of work that forms the basic building block of a plan or *network*.
After image	See - *Before and after image*.
Algorithm	In computing, a finite set of well defined rules for the solution of a problem in a finite number of steps (see *encryption algorithm*).
Applet	A small *Java program* that can be embedded in an *HTML* page. Applets differ from full-fledged Java applications in that they are supposed to be restricted to provide some security to the user.
Application	A *system* that has been developed to serve a specified purpose, for example to pay suppliers' invoices, place orders with suppliers and maintain stock records. An application incorporates both clerical and computerised procedures; *controls* over *transaction* input, processing and output; and *file* management. It should also maintain an *audit trail* (see also *system software*; *program*).
Approval to Proceed	This approval is given by the *project board* at *project initiation* and at each end *stage* assessment prior to commencement of the next stage. It represents a commitment to a further expenditure up to the end of the next stage in a *project*.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
ASCII	**American Standard Code for Information Interchange**. ASCII was developed to *standardise* data transmission among disparate hardware and *software* systems, and is built into most mini and personal computers. It is a coding scheme using 7 or 8 *bits* that assigns numeric values to up to 256 characters. These include letters, numerals, punctuation marks, control characters and other symbols. ASCII text is often referred to as a "plain text" (see *EBCDIC*).
ASCII file	A document *file* in *ASCII* format, containing characters, spaces, punctuation, carriage returns, tabs and an end-of-file marker, but no formatting information. Also sometimes referred to as a text file, text-only file or plain text.
Asset	In *Information Security*, the *information* or information processing resources that are to be protected by the application of *controls*.
Asymmetric encryption	A cryptographic *algorithm* that employs a *public key* for *encryption* and a *private key* (see *secret key*) for *decryption*; or in *authentication*, a private key for signing and a public key for signature verification. Public and private *keys* are related and form an asymmetric key set.
Audit trail	A chronological set of *records* that collectively provide documentary evidence of processing, sufficient to enable reconstruction, review and examination of an activity.
Authenticity	The attribute of genuineness. For evidence to be authentic it must be all that it purports to be.
Authentication	(1) The act of determining that a *message* has not been changed since leaving its point of origin. **(**2) A process that verifies the claimed identity of an individual.
Availability	The ability to access and use a *system*, resource or *file*, where and when required.
Backup	A duplicate copy (e.g. of a *program*, of an entire disc or of *data*) made either for archiving purposes or for safeguarding valuable *files* from loss should the active copy be damaged or destroyed. A backup is an "insurance" copy.
Back door	see *Trapdoor*.
Bandwidth	A measurement of how much *data* can be sent across a communications circuit at the same time. It is usually measured in *bits* per second (BPS).
Baseline (1)	In configuration management, a snapshot of the state of a *CI* and any component CIs, frozen at a point in time for a particular purpose.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Baseline (2)	In *project management*, a set of dates and costs frozen at the start of a *project* and used as a basis for comparison as the project progresses.
Bastion host	A specific *host* that is used to intercept *packets* entering or leaving a *network* and the *system* that any outsider must normally connect with to access a *service* or a *system* that lies within an organisation's *firewall*.
Before and after image	In *database* updating, the *transaction* is first applied to a copy of the *record* to be updated (the "before image") held in memory to produce an image of the record after updating (the "after image"). The updated image is then *committed* to the database, after which the after image is compared with the database record. If they do not match the process can be *rolled back* by the *DBMS*.
Benefits	The enhanced efficiency, economy and effectiveness of future business operations to be delivered by a *programme*.
Benefits management	A formal process with *programme management* for planning, managing, delivering and measuring the set of benefits which a *programme* is to provide.
Benefits Management Plan	A component of the *Programme Definition Statement*, which specifies who is responsible for achieving the benefits set out in the *Benefits Profiles* and how achievement is to be managed, measured and monitored.
Benefits Profiles	A component of the *Programme Definition Statement* which describes the planned benefits to be realised by a *programme* and states where, how, and when they are to be realised.
Biometrics	In *access control*, automated methods of verifying or recognising a person based upon behavioural or physical characteristics (e.g. fingerprints, handwriting, and facial or retina geometry).
BIOS	**Basic Input/Output System**. The set of essential *software* routines that test hardware at start-up, start the *operating system* and support the transfer of *data* among hardware *devices*. On PC-compatible computers, the BIOS is stored in read-only memory (*ROM*) so that it can be executed when the computer is turned on. Although critical to performance, the BIOS is usually invisible to computer users.
Bit	Shortened term for binary digit. It is the smallest unit of *information* handled by a computer. One bit expresses a 1 or a 0 in a binary numeral, or a true or false logical condition, and is represented physically by an element such as a high or low voltage at one point in a circuit or a small spot on a disk magnetised one way or the other. A single bit conveys little information a human would consider meaningful. A group of 8 bits, however, makes up a *byte*, which can be used to represent many types of information, such as a letter of the alphabet, a decimal digit or other character.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Black box testing	Testing that involves no knowledge of the internal structure or logic of a *system*.
Boot	The process of starting or resetting a computer. When first turned on (cold boot) or reset (warm boot), the computer executes important *software* that loads and starts the computer's *operating system* and prepares it for use. Thus, the computer can be said to pull itself up by its own "bootstraps".
Boot disk	A floppy disc that contains key system files from the *operating system* and that can *boot*, or start, the PC. A *boot* disk must be inserted in the primary floppy disc drive (usually drive A:) and is used when there is some problem with starting the PC from the hard disc, from which the computer generally boots.
BSI	**British Standards Institution**. The UK national *standards* body. Widely used standards first developed and published by the BSI include ISO 9001 (BS5750 – *quality* management systems) and ISO 17799 (BS 7799 – *information security* management).
BS 7799	A UK *standard* published by the *BSI*. It consists of two parts. Part 1 (*A Code of Practice for Information Security Management*) provides a baseline set of *information security controls*. Part 2 contains the auditing criteria against which formal certification against the standard may be obtained.
Browser	See *web browser*.
Browsing	Searching through storage to locate or acquire *information*, without necessarily knowing of the existence or the format of the *data* being sought.
Buffer	(1) In computing, an area of storage that is temporarily reserved for use in performing an input/output operation, into which *data* is read or from which it is written. (2) In data communications, a storage area used to compensate for differences in the rate of flow of data, or time of occurrence of events, when transferring data from one *device* to another.
Bug	An error in *programming code* that produces an undesirable variation from design performance in a *program* during execution.
Business	A commercial or government enterprise, and the people who comprise it.
Business Case	A document that provides justification for the commitment of resources to a *project* or *programme*.
Business Change Manager	A role in the *programme* executive responsible for *benefits management*, the programme's *Business Case*, transition plan and the management of change and risk.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Business continuity	A formal plan, or integrated set of plans, designed to enable key business processes to continue in operation following a major system failure or disaster. Essential ingredients include the identification of key business *processes*, adequate system *backups* and a workable continuity *strategy*.
Business impact review	In *business continuity* planning, a review designed to identify the impacts (over time) of loosing *information systems*.
Byte	A unit of *data* generally comprising 8 *bits*. A byte can represent a single character, such as a letter, a digit or a punctuation mark. Because a byte represents only a small amount of *information*, amounts of computer memory and storage are usually given in kilobytes (1,024 bytes), megabytes (1,048,576 bytes), or gigabytes (1,073,741,824 bytes).
Call centre	A central point where customer and other telephone calls are handled by an organisation, usually assisted by some amount of computer automation. Typically, a call centre has the ability to handle a considerable volume of calls at the same time, to classify calls and forward them to someone qualified to handle them, and to record calls. Call centres commonly handle such activities as customer services, order entry, reservations, *help desk* facilities, dispatch systems, telesales and collections. Telephone banking, insurance and share dealing are among financial applications.
CASE	**Computer Aided Systems Engineering**. *Software* tools that support *systems* analysis, design and construction.
Central Processing Unit	(CPU) computer hardware that houses the electronic circuits that control/direct all a computer's operations.
Certification authority	In cryptography, an authority trusted by all users to create and assign *digital certificates*. The role is generally performed by large public institutions, such as the Post Office, BT and clearing banks (e.g. Barclays).
Change Control	In *project management*, uncontrolled changes are one of the most common causes of delay and failure. Change Control is the process of implementing procedures which ensure that proposed changes are properly assessed and, if approved, incorporated into the project plan.
Change management	IN IT service management, the *process* of *controlling* and managing requests to change an *IT Infrastructure* or *IT service*, and then controlling and managing the implementation of the changes that are subsequently approved.
Channel	In data communications, a path along which signals can be sent. The term may also refer to a mechanism by which the path is effected.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
CI	**Configuration Item**. In *configuration management*, a component associated with an *IT infrastructure* that is under the control of the Configuration Manager. CIs vary widely in complexity, size and type. They can range from an entire *system* (including all its hardware and documentation) to a single *program* module or a minor hardware component.
Ciphertext	In *cryptography*, unintelligible text produced through the use of *encryption*.
Classification	The process of formally identifying *incidents*, *problems* and *known errors* by origin, symptoms and cause.
Client	(1) A computer that interacts with another computer, usually referred to as the *server*, using a client *program*. E-mail is an example - an e-mail client connects to an e-mail server to send and receive *messages*. (2) A term sometimes used by auditors to refer to an audited organisation.
Close Out	The completion of *project* work once a project has been implemented. It is the phase at the end of the project lifecycle just before live operations begin. Confusingly this period is often called Start-Up, since this refers to the start-up of the facility.
Code	*Program* instructions written by a programmer in a programming language.
Cold site	In *business continuity*, a site that is suitable for the installation of computer equipment and its environmental and ancillary support.
Commit	In databases, a command to update the physical *database* with the *transactions* input to the system and held in temporary storage (or *buffer*).
Confidentiality	In *information security*, the property that *information* is not made available or disclosed to unauthorised individuals, entities or processes.
Configuration	The complete technical description required to build, test, accept, install, operate, maintain and support a *system*.
Configuration audit	Verifying the completeness and correctness of CI*s*. This involves verifying that all items are present in their correct *version* and, where computer *files* are concerned, their integrity is sound; and that no extraneous items have been introduced (e.g. unauthorised equipment; unauthorised and/or unlicensed *software*).
Configuration Item	See CI.
Configuration Management	The process of identifying and defining the *CIs* in a *system*; recording and reporting their status; and verifying their completeness and correctness.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Controls	In *information security*, *policies*, *procedures* and mechanisms designed to ensure that activities achieve their authorised objectives. Controls can be preventive (e.g. a 'no smoking' policy is enforced), detective (e.g. a smoke detector), corrective (e.g. a sprinkler system) or restorative in character (e.g. a disaster recovery plan).
CMDB	**Configuration Management Database** – a *database* that contains details about the attributes and the history of each *CI*, and details of the important relationships between CIs.
CRAMM	The CCTA Risk Analysis and Management Methodology. A software-supported method for identifying and justifying security measures for both current and future IT systems. The method provides assistance with *risk assessment*, and the identification of cost-effective *controls* (see *risk management*). The *software package* assists in recording review information, provides *audit trails* between recommended controls and related *risks*, and provides a "what if?" facility.
Critical Path	The longest sequence of *activities* in a *network*.
Critical Path Analysis	A simple calculation of a *network* of *activities* that results in a date which is the earliest possible completion of the *project* taking time and logic only, into account. It results in the calculation of a *critical path*.
Cryptography	The discipline that embodies principles, means and methods for the transformation of *data* in order to hide its *information* contents, prevent its undetected modification, and/or prevent its unauthorised use.
Customer	The individual or organisation that buys a product or *service* (see *user*).
Cyberspace	The virtual space created by the technology of computer systems enabling people to communicate with other users worldwide.
Data	In computing, (1) a representation of facts, concepts, *information*, or instructions in a manner that is suitable for processing by an *information system*. (2) The building blocks of information.
Data dictionary	In *databases*, a centralised repository of *information* about the stored *data*, providing details of its meaning, relationship (to other data), origin, usage and format.
Data file	A *file* consisting of *data* in the form of text, numbers or graphics, as distinct from a *program* file containing commands and instructions. Data files may also be called documents or spreadsheets.
Database	An extensive and comprehensive set of *records* collected and organised in a meaningful manner to serve a particular purpose.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Data Protection Act (UK)	Legislation designed to protect the rights of individuals whose personal *data* are stored in either manual or computerised systems. Systems covered by the Act are those where (1) personal data is held (data relating to a living individual who can be identified from the data, or from the data and other *information* that the data user has access to. And (2), the *files* holding the data are structured in the same way. The Act contains a strict code of conduct, which includes an obligation to protect personal data against loss, destruction, damage or disclosure. Both civil and criminal penalties can apply to contravention of the Act.
DBMS	**Database Management System**. *Software* that handles *database* access requests from *application* processes. Essentially a DBMS handles storage, access, *data* sharing among multiple users, and database administration tasks (e.g. controlling what data an application *user* can view and update).
Decrypt	In *cryptography*, to convert by use of the appropriate *key*, *encrypted* text (see ciphertext) into its equivalent plaintext.
Definitive Software Library	**DSL.** A secure library where quality-controlled versions of all *software CIs* that have been accepted from the developer or supplier are held in their definitive form.
Device	A generic term for printers, scanners, mice, keyboards, serial ports, video adapters, disk drives and other computer subsystems. Such devices frequently require their own controlling *software*, called *device drivers*.
Device driver	A *software* component that permits the computer system to communicate with a *device*. Many devices, especially video adapters on microcomputers, will not work properly, if at all, without the correct device drivers installed in the *operating system*.
Digital certificate	In *cryptography*, a message that guarantees the authenticity of the data contained within it. In *public key cryptography* it is important that anyone using a public key can be sure about its *authenticity*. Such a guarantee may be issued by a *Certification Authority* trusted by the users, and based on assurances obtained from applicants for digital certificates. A certificate generally contains the public key owner's identity, the public key itself and its expiry date. A user supplies the certificate and the recipient *decrypts* it using the certification authority's public key (often performed automatically by the recipient's *browser*/e-mail software). The recipient gains assurance that a trusted authority has signed the user identity and corresponding public key.
Digital signature	A *data* block appended to a *file* or *message* (or a complete *encrypted* file or message) such that the recipient can *authenticate* the file or message contents and/or prove that it could only have originated with the purported sender.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Document	*Information* in readable form. The medium on which the document is held (e.g. paper, fiche, film and magnetic disk) is not important. See also *record*.
DSDM	**Dynamic Systems Development Methodology**. A formal method for developing *information systems* quickly using *RAD* techniques.
Dump	In computing, the act of copying raw *data* from one place to another with little or no formatting for readability. It usually refers to copying data from main memory to a display screen or a printer. Dumps are useful for diagnosing *bugs*. After a *program* fails, a dump can be used to analyse the contents of memory at the time of the failure.
EBCDIC	**Extended Binary Coded Decimal Interchange Code**. Developed by IBM, and mostly used by *mainframe* systems, EBCDIC is a standard way of representing text symbols using binary numbers (see also *ASCII*).
E-business	See *electronic business*.
E-commerce	See *electronic commerce*.
E-government	See *electronic government*.
EDI	**Electronic Data Interchange**. In computing and communications, the transmission of documents from one computer to another over a *network*. Although EDI is sometimes carried out over direct links between trading partners (and increasingly the *Internet*), it is more usual to involve a value added supplier to operate an electronic mailbox through which documents are exchanged on a store and collect basis, similar to e-mail. The ability of communicating computer systems to exchange and process *information* in this way can significantly speed up processing and reduce manual transcription errors.
EFT	**Electronic Funds transfer**. *Systems* designed to move funds between banks using electronic communications rather than paper media. Common EFT systems include BACS (Bankers' Automated Clearing Services) and CHAPS (Clearing House Payment System).
Electronic business	Using an electronic *network* to simplify and speed up all stages of the business process including such as activities as design and manufacturing; buying, selling and delivering; and transacting government business.
Electronic commerce	Using an electronic *network* to simplify and speed up the process of buying, selling and delivering.
Electronic government	Using an electronic *network* to deliver government *information* to, and transact government business with other departments of state, citizens and businesses, and other governments.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Encryption	(Also encipher). The process of transforming *information* into an unintelligible form in such a way that the original information cannot be obtained ("one-way" encryption) or cannot be obtained without using the inverse *decryption* process ("two-way" encryption).
Encryption algorithm	A set of mathematically expressed rules implemented in either *firmware* or *software*, and used in conjunction with a *secret key* for *encrypting* plaintext and decrypting *ciphertext*.
End user computing	Refers to the use of non-centralised (i.e. non-IT department) data processing using automated procedures developed by end-users, generally with the aid of *software packages* (e.g. spreadsheet and database) and enquiry *software*. End-user processes can be sophisticated and become an extremely important source of management information. Whether they are adequately tested and documented may be questionable.
Error	(1) In *IT Service Management*, a condition identified by successful diagnosis of the root cause of a *problem* when it is confirmed that a *CI* is at fault. (2) In *quality* management, any non-conformance between *software* and either its *specification*, design or implementation, or its behaviour as stated or implied by *users* and operations staff.
Error control	In IT Service Management, the process of identifying, recording, classifying and progressing *known errors*. This includes the resolution phase until successful implementation of an amendment or replacement *CI* is confirmed.
ETHERNET	A common *LAN* technology that employs CSMA/CD (carrier sense multiple access with collision detection) over either coaxial cable or twisted pair wiring. CSMA/CD allows computers to transmit when the *network* is free.
Facilities management	In computing, the management, operation and support of an organisation's computers and/or networks by an external provider under a contract, and at agreed levels of service (see *Service Level Agreement*; *outsource*).
File	A complete, named and collection of *information*. (1) In computing, a *file* can contain program *code*, *data* (e.g. *transactions* to be processed by a *program*), or user-created data (e.g. a word processor file). Most commonly, however, the term refers to data (numbers, words, or images) that a user has created and then saved for subsequent retrieval, editing or printing. (2) In *information systems*, a collection of *documents*. The medium on which the documents are stored (e.g. paper, fiche, microfilm, magnetic disks) is not important.
File server	In a local area *network* (*LAN*), a computer that provides access to *files* for *workstations* that are connected to the network.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Firewall	A security system used to prevent unauthorised access between networks (both internal/internal, and internal/external) by examining and filtering IP data *packets*. A firewall will allow only approved traffic in and/or out by filtering packets based on source/destination *IP address*, source/destination port. The firewall inspects the identification information associated with all communication attempts and compares it to a rule-set consistent with the organisation's security policy. Its decision to accept or deny the communication is then recorded in an electronic log.
Firmware	Programming that is inserted into Programmable Read-Only Memory (PROM), thus becoming a permanent part of a computing *device*. Firmware is created and tested like other *software*. It can also be distributed like other software and installed in the PROM by the user. Firmware is sometimes distributed for printers, *modems* and other computer *devices*.
Float	A measure of the time flexibility available in the performance of an *activity* (see also *free float*, *negative float* and *independent float*).
Fourth Generation Language	Any programming language that uses English terminology and allows rapid *software* development. With 4GLs the user specifies what is required and the programming language works out what actions are needed to carry out the required task. *Structured Query Language* (SQL) is a commonly used 4GL.
Frame-Relay	A *packet-switched wide area network* technology that provides faster performance than other packet-switched WAN technologies (such as *X-25* networks) because it was designed for more recent and reliable circuits that require less rigorous error detection. Fame-relay is best suited to data and image transfers. Because of its variable-length packet architecture, it is not the most efficient technology for real-time voice and video. In a frame-relay network, end nodes establish a connection via a *Permanent Virtual Circuit* (PVC).
Free float	The amount of time an *activity* may be delayed without causing any knock on delay to following activities.
FTP	**File Transfer Protocol**. In communications, a *protocol* that ensures the error-free transmission of *program* and *data files* via a data communications link.
Function Point Analysis	In planning and estimating, a technique used to determine the size of a development task. It entails breaking a *project* down into function points (factors such as inputs, outputs, enquiries, logical internal sites, etc.), which are then classified by degree of complexity. Factors are then applied from which time estimates may be developed.
Gateway	A computer or other *device* that links two *networks*, routing and often converting *protocols* or *messages* from one network to the

Subject/term/acronym	Description
	other. The term can also refer to a system capability that provides direct access to other remote networks or *services*.
GANTT Chart	A bar chart plotting the phases or *activities* of a *project* against a predefined timeline to completion.
Gigabyte	(**GB**) 1,024 megabytes (2^{30} *bytes*). Often interpreted, though, as approximately one million *bytes*.
Hash total	A figure obtained by some operations upon all the items in a collection of *data* and used for control purposes. A recalculation of the hash total, and comparison with a previously computed value, provides a check on the loss or corruption of the data.
Help Desk	Sometimes called a "service desk", provides a focal point for providing first line *incident* support; help with using IT-based business systems; and management reporting on *IT service quality*.
Hexadecimal	A numbering system that uses a base of 16 and requires 16 digits (0 through 9, and A through F).
Host	A computer connected to a *network* that offers services to one or more users.
Hot site	In *business continuity*, a fully equipped computer installation designated for standby purposes. *Data* will need to be loaded; and *software* may need to be installed and configured.
HTML	**Hypertext Markup Language**. The programming language used for *web pages*. It is called a "mark-up" language because it is used to describe the formatting to be used to display the document. The html file contains both the text and *code* (called tags). It is read by a web browser, which interprets the code and displays the web pages in the format specified by the HTML.
HTTP	**Hypertext Transfer Protocol** is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the *World Wide Web*. By comparison with the *TCP/IP* suite of *protocols*, which forms the basis of *information* exchange across the *Internet*, HTTP is an *application* protocol.
Hub	A *device* that connects several devices (terminals, printers, etc.) to a *network*.
ICT	**Information and Communications Technology**. The acquisition, processing, storage and dissemination of *information* using a combination of computer and telecommunications technologies.
IETF	The **Internet Engineering Task Force**: a large open international community of *network* designers, operators, vendors, and researchers concerned with the evolution of the

Subject/term/acronym	Description
	Internet architecture and the smooth operation of the Internet. It is open to any interested individual.
Impact	In *information security*, the damage to an organisation resulting from a *threat* exploiting a *vulnerability*. The business consequences may result from unauthorised disclosure of sensitive *information*; or modification or unavailability of information; or a combination of these impacts. Impact generally has financial implications, but depending on the circumstances and the nature of the information at risk, other consequences might be *loss of credibility*, *contravention of the law*, *personal injury* and/or *loss of life* (e.g. as in medical records, patient management and safety critical control systems).
Impact code	A simple code assigned to *incidents* showing the extent of deterioration in normal user service levels. It is the major means of assigning priority for dealing with incidents.
Implement	Install, utilise or bring into operation.
Incident	An operational event that is not part of the normal operation of a *system*. It will have an impact on the system, although this may be slight or transparent to the *users*.
Incident control	The process of identifying, recording, classifying and progressing *incidents* until affected services return to normal operation. Collection of *data* to identify causes of incidents is a secondary objective, although this may be necessary to effect incident resolution.
Independent Float	The degree of flexibility that an *activity* has that does not affect the *float* available on any preceding or succeeding activities.
Information	Knowledge that was unknown to the recipient prior to its receipt. Information is derived from *data*, which to be of value needs to be valid (e.g. not duplicated or fraudulent), complete, accurate, relevant and timely.
Information security	The result of any system of policies and procedures for identifying, controlling and protecting *information* against unauthorised disclosure, manipulation, modification; unavailability and destruction. Unauthorised disclosure refers to information that is, for example, commercially sensitive, nationally classified or subject to *data protection* legislation. Manipulation is concerned with changing some attribute of the *data*, such as *file* ownership, security classification, destination, etc. Modification involves unauthorised alteration of the data itself, which can take place without leaving any trace. Unavailability refers to an inability to access and process the data (e.g. due to computer or communications failure). Data can be destroyed quickly and efficiently in electronic or magnetic storage *devices* (e.g. by degaussing, powering down *volatile* storage and overwriting).

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Information security policy	A formal statement that defines top management intentions on *information security*, and provides general direction for protecting the *confidentiality*, *integrity* *and* *availability* of corporate *information*.
Information system	The means for organising, collecting, processing, transmitting, and disseminating *information* in accordance with defined *policies* and *procedures*, whether by automated or manual means.
Input controls	Techniques and procedures used to verify, validate and edit *data* to ensure that only correct data is entered into a computer *system*.
Integrity	In *information security*, the property that *information* is valid, complete and accurate.
Internet	A worldwide system of linked computer *networks* that enables data communication *services* (based on *TCP/IP*) such as remote logon, file transfer, electronic mail, and newsgroups. The Internet is not a discrete computer network, but rather a way of connecting existing computer networks that greatly extends the reach of each participating system. It is not single service, has no real central hub, and is not owned by any one group (see also IETF).
Intranet	A private *network* inside an organisation that uses the same kinds of *software* and *protocols* found on the *Internet*. Intranets may or may not be connected to the Internet.
IP	**Internet Protocol**. A *protocol* that defines and routes data across the *Internet*. It uses *packet switching* and makes a best effort to deliver its *packets* (see also *TCP/IP*).
IP address	Every computer on the *Internet* is assigned a unique number so it can be identified. *IP* addresses are 4 dot-separated numbers (for example, 205.243.76.2) that specify both the *network* the computer is connected to and the *host*.
ISDN	**Integrated Services Digital Network**. A medium speed, digital connection. It provides up to 128kbps *bandwidth* over two *channels*. Like normal phone lines, it has a number that can be dialled into and it can dial out to any other ISDN number, unlike leased lines which are strictly point-to-point. Like leased lines, ISDN provides a reliable digital *service* that is not normally affected by line noise and other ailments that modems can experience.
ISO	**International Standards Organisation**. An agency of the United Nations concerned with international standardisation across a broad field of industrial products. An example of an ISO *standard* against which some audit clients (or their external providers) are formally certified is that governing *quality* management *systems*, ISO 9001.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Island of Stability	A review point at the end of a tranche, when progress is reviewed and the next tranche is planned.
IS Steering Committee	The top management group responsible for the overall direction of *information systems* (IS). The ISSC owns, commissions, directs and agrees their organisation's *IS Strategy*.
IS Strategy	An organisation's master plan for directing, developing, installing and operating the *information systems* necessary to satisfy its business needs. An IS strategy should be supported by a business case to provide purpose and economic justification for what is proposed. It should also include measurable performance targets and deadlines against which its success can be monitored. Due to the delay generally involved in bringing new *IT infrastructure* into operation, an IS strategy usually covers a three to five year planning period. It should, however, be monitored and updated frequently to ensure that it continues to represent an effective and workable plan. See *IS Steering Committee*.
IT infrastructure	The hardware, software, computer-related communications, documentation and skills that are required to support the provision of *IT services*, together with the environmental infrastructure on which it is built.
IT infrastructure management	The *processes* that are required to manage an *IT infrastructure*. They comprise processes covering *service* management, hardware and software *release*, *incident* and *problem* resolution, *customer* and supplier management, and overall control of *assets* (see *change* and *configuration* management).
IT service	(1) In *IT Service Management*, an operational IT service comprises the *IT infrastructure* necessary to provide a designated group of *users* or *customers* with access to one or more designated *applications,* often within the terms of a *service level agreement*. (2) In computing, the provision of data processing facilities.
IT service management	Sometimes shortened to "Service Management", is the totality of (a) *IT service* provision and (b) *IT infrastructure management* (the term is synonymous with "IT systems management" and "IT Service Delivery").
Java	A *programming* language, similar to C++, created by Sun Microsystems for developing that are capable of running on any computer regardless of the *operating system*.
Key	In *cryptography*, a symbol or sequence of symbols that controls the operations of *encryption* and *decryption*. It is essential that keys are protected against unauthorised disclosure.
Known error	In *IT Service Management*, a condition identified by successful diagnosis of the root cause of a *problem* when it is confirmed that a *CI* is at fault.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
LAN	**Local Area Network**. A *network* that connects PCs and other computers within a limited geographic area by high-performance cables so that users can exchange information, share expensive peripherals, and draw on the resources of a massive secondary storage unit, call a *file server*. See also *WAN*.
Lights out operating	Sometimes known as "darkroom" operating, is where the computer room is not staffed, but people are available to control the system via one or more terminals or consoles connected to the system, often as part of an *Operations Bridge*.
Log	In computing, a *record* (or "journal") of a sequence of events (1) relating to the jobs run through a computer. Job logs generally contain chronologically listed information on when jobs start and end, the resources they access (and whether or not access was successful), together with any *messages* generated from within the *applications* that are running. (2) A chronological record of the activities performed (or attempted) by individuals when using a computer system.
Logical	In computing, conceptual or virtual (i.e. within the computer; in *cyberspace*), as compared with physical or actual (i.e. outside the computer; real world).
Logical access	The act of gaining access to computer *data*. Access may be limited to "read only", but more extensive access rights include the ability to amend data, create new *records*, and delete existing records (see also *physical access*).
Login	The act of connecting to a computer and being *authenticated* as a legitimate user. The usual requirements are a valid user name (or user ID) and password, but in higher *risk* scenarios a user may also have to insert a physical token (e.g. a *smartcard*) and/or provide *biometric* proof of identity.
Mainframe	A high-level computer designed for the most intensive computational tasks. Mainframe computers are often shared by multiple *users* connected to the computer by terminals.
Macro	A macro is a list of actions to be performed that is saved under a short key code or name. *Software* can then carry out the macro's instructions whenever the user calls it by typing its short key code or specifying the macro name.
Media	The physical material, such as paper, disc and tape, used for storing computer-based *information*.
Memory	Memory generally refers to the fast semiconductor storage (Random Access memory, or *RAM*) directly connected to the *processor* that is dependent on electrical power for activation. Memory is often differentiated from computer storage (e.g., hard disks, floppy disks, CD-*ROM* disks) that is not dependent on

Subject/term/acronym	Description
	electricity and is therefore a more permanent means for holding *data*.
Memory chip	Or “chip”, is an integrated circuit devoted to memory storage. The memory storage can be *volatile* and hold *data* temporarily, such as *RAM*, or non-volatile and hold data permanently, such as *ROM*, EPROM, EEPROM or PROM.
Message	In data communications, an electronic communication containing one or more *transactions* or one or more items of related *information*.
Message header	The additional *information* attached to e-mail *messages* that provides information about the e-mail; who sent it, where it came from, what path it took, when it happened.
Messaging	Also called electronic messaging, is the creation, storage, exchange, and management of text, images, voice, telex, fax, e-mail, paging, and *EDI* over a communications *network*.
MICR	**Magnetic Ink Character Recognition**. A technique for the identification of characters printed with ink that contains particles of a magnetic material. Used widely in the banking industry to capture sort codes and account numbers on cheques.
Microprocessor	A central processing unit (*CPU*) on a single microchip. A microprocessor is designed to perform arithmetic and logic operations that make use of small number-holding areas called *registers*. Typical microprocessor operations include adding, subtracting, comparing two numbers, and moving numbers from one area to another. These operations are the result of a set of instructions that are part of the microprocessor design. A modern microprocessor can have more than one million transistors in an integrated-circuit package that is roughly one inch square. Microprocessors are at the heart of all computers, from *mainframes* down to *smartcards*.
Middleware	*Software* that is neither part of the *operating system*, nor an *application*. It occupies a layer between the two, providing applications with an interface for receiving services. Common examples are communications *programs* and *transaction* processing monitors.
Milestone	An *activity* of zero duration which represents a significant deliverable or *stage* in a *project*.
Modem	A communications *device* that enables a computer to transmit *information* over a standard telephone line. Because a computer is digital (it works with discrete electrical signals representing binary numbers 1 and 0) and a telephone line is analogue (carries a signal that can have any of a large number of variations), modems are needed to convert digital to analogue and vice versa. The term is short for MOdulator/DEModulator.

Subject/term/acronym	Description
Multiplexor	Equipment that takes one or more *data channels* and combines the signals into one common channel for transmission. At the receiving end a demultiplexor extracts each of the original signals.
Negative Float	Where a path in a *network* becomes hypercritical the *activities* on that path have a float of less than zero. The quantity of float then indicates the amount of time that must be recovered in order to achieve a target date.
Network (1)	In data communications, a computer-based communications and data exchange *system* created by physically connecting two or more computers. The smallest *networks*, called local area networks (*LAN*'s), may connect just two or three computers so that they can share an expensive peripheral, such as a laser printer, but some LAN's connect hundreds of computers. Larger networks, call wide area networks (*WAN*s), employ telephone lines or other long-distance communications media to link computers.
Network (2)	A diagram that shows the logical relationships between *activities*.
Node (1)	In a *LAN*, a connection point that can create, receive, or repeat a message. Nodes include repeaters, *file servers*, and shared peripheral *devices*. In common usage the term node often relates to a *workstation* or terminal.
Node (2)	In planning and estimating, the node at the start of an *activity* in an activity on arrow *network*.
Normalisation	In *database* design, the elimination of redundant/superflous *data*.
Object	(1) In computer security, a passive entity that contains or receives *information*. For example, *records*, *files*, *programs*, printers, and *nodes*. (2) In object-oriented *programming*, an entity that encapsulates within itself both the *data* describing the object and the instructions for operating on those data.
Objective	A desired goal, or end result.
OCR	**Optical Character Recognition**. Techniques and equipment for reading printed, and possibly hand-written, characters on a *document* and converting them to digital code (e.g. *ASCII*) for input to a computer.
Off-the-shelf	A packaged item ready for sale. The term can refer to hardware, *software* or both.
On-line	Generally describes a computer that is connected to a *network* and is thereby ready for operation or interaction over the network. It may also refer to the ability to connect to the *Internet* by virtue of having an Internet account.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Operations bridge	The combination in one physical location of computer operations, *network* control and the *Help Desk*.
Operating system	In computing, a collection of *software* designed to directly control the hardware of a computer (e.g. input/output requests, resource allocation, data management), and on which all other *programs* (including *application programs*) running on the computer generally depend.
Organisation	See *business*.
Output controls	*Controls* whose objectives are to ensure that computer outputs are complete and accurate, are securely held until distribution (they may include financial instruments), and are distributed to the intended recipient(s) in a timely manner.
Outsource	The use of an external contractor to provide (1) both the IT *systems* and the personnel required to run them (see also *facilities management*). (2) support *services*, such as hardware maintenance.
Package release	In *IT Service management*, a set of *software* that is *CIs* that are tested and introduced into the live environment together.
Packet	(Sometimes referred to as a 'frame') in communications, a packet comprises a well-defined block of bytes consisting of 'header', *'data'* and 'trailer'. Packets can be transmitted across *networks* or over telephone lines. The format of a packet depends on the *protocol* that created it. Various communications *standards* and *protocols* use special purpose packets to monitor and control a communications session. For example, the *X.25* standard uses diagnostic, call clear and reset packets (among others), as well as data packets.
Packet switching	A transmission method in which *packets* are sent across a shared medium from source to destination. The transmission may use any available path or circuit, and the circuit is available as soon as the packet has been sent. The next packet in the transmission may take a different path, and packets may not arrive at the destination in the order in which they were sent.
Password	In *Access Control*, confidential *authentication information*, usually composed of a string of characters, that may be used to control access to physical areas and to *data*.
Patch	A piece of programming *code* that is added to an existing *program* to repair a deficiency in the functionality of an existing routine or program. It is generally provided in response to an unforeseen need or set of circumstances. Patching is also a common means of adding a new feature or function to a program until the next major version of the *software* is released.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
PD0005	**A Code of Practice for IT Service Management**. A guide published by the *BSI*, that is designed to provide advice and recommendations for *IT service management*. The subjects dealt with include managing incidents, *problems*, *system* configuration and system *change*.
PD0008	**A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored electronically**. A *BSI* guide on the management of *systems* in which original paper *documents* are scanned to form electronic images. The object is to ensure that the images so formed may be regarded as *authentic*, for example in a court of law or by external regulators or auditors.
Permanent Virtual Circuit	(PVC) is a software-defined logical connection in a network such as a frame relay network. A feature of frame relay that makes it a highly flexible network technology is that users can define logical connections and required bandwidth between end points and let the frame relay network technology worry about how the physical network is used to achieve the defined connections and manage the traffic. In frame relay, the end points and a stated bandwidth called a Committed Information Rate constitute a PVC, which is defined to the frame relay network *devices*. The bandwidth may not exceed the possible physical bandwidth. Typically, multiple PVCs share the same physical paths at the same time. To manage the variation in bandwidth requirements expressed in the CIRs, the frame relay devices use a technique called *statistical multiplexing*.
Phreaking	In communications security, fraudulent use of a telephone system to make calls at the expense of another. Cases brought under English law are prosecuted under the Theft Act.
Physical access	In *access control*, gaining access to physical areas and entities (see *logical access*).
Platform	The computer hardware, and the associated *operating systems software* necessary for its operation, on which *applications software* is run.
Policy	A formally stated course of action to be followed for achieving an *objective* (see *strategy).*
Port	an interface between the CPU and a peripheral *device*.
PRINCE	A methodology for planning, managing and controlling *projects*. PRINCE II is a generic *project management* method, whereas the earlier version (PRINCE) was specifically aimed at IT projects.
Private key	See *secret key*.
Problem	In *IT Service Management*, a condition identified from multiple *incidents* that exhibits common symptoms. It can also arise from a single significant incident that suggests a single *error* for which the cause is unknown.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Problem control	In *IT Service Management*, the process of identifying, recording, classifying and progressing *problems* through investigation and diagnosis until either known *error* status is achieved, or an alternative procedural reason for the problem is revealed.
Problem management	In *IT Service Management*, a generic term used to identify the combined processes of *incident*, *problem* and error control, complemented by the utilisation of associated management information. The primary objective is to make sure that *services* are stable, timely and accurate.
Procedure	A set of instructions for performing a task. Procedures should be consistent with *policy* requirements.
Process	In IT Service Management, a sequence of operations that are intended to achieve a defined objective. Processes require *policy*, people, procedures and *IT infrastructure*.
Processing controls	*Controls* whose objectives are to ensure that only valid *data* is processed, and that processing is both complete and accurate.
Program	In computing, a series of instructions that conform to the syntax of a computer language, that when executed (or "run") on a computer will perform a given task.
Programme	A group of *projects*. The projects that comprise a programme are selected and planned in a co-ordinated way so that, overall, they serve to implement a business *strategy*. Sometimes a large, complex project is described as a programme.
Programme Definition Statement	The agreed statement of objectives and plans between the target business operation, the Programme Director, and the senior management group to whom the Programme Director reports.
Programme Management	The selection and co-ordinated planning of a portfolio of projects so as to achieve a set of defined business objectives, and the efficient execution of these projects within a controlled environment such that they realise maximum benefit for the resulting business operations.
Programme Director	The senior manager with individual responsibility for the overall success of a programme. Is ideally drawn from the management of the target business area.
Project	A temporary management environment, set up to deliver a *specified* business product in accordance with a defined business case.
Project Brief	A statement of the terms of reference for the project, initially provided by the IS Steering Committee and subsequently refined by the *project board* to form part of the *Project Initiation Document*.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Project Board	A board set up to exercise overall control of a *project*. It generally comprises a small group of senior managers that represent major business interests such as Finance, Information Technology and the particular business area that is sponsoring, or will be most affected by the project.
Project Initiation	Management activities that aim to ensure that a *project* is established with clear terms of reference and an adequate management structure. These activities are led by the *Project Board*.
Project Initiation Document	A document that is approved by the *Project Board* at *project initiation*. It defines the terms of reference for the *project*, based on the initial *project brief*, and brings together other key information needed to start the project on a sound basis. (It should answer the questions *why? what? how? who? and when? for the project, and what? why? and when?* for its business products).
Project Manager	The person appointed to take day-to-day responsibility for managing a *project* throughout all its *stages*. A project manager is essentially a non-technical role, with technical management of a project being undertaken by *stage managers*.
Project Management	The managerial task of accomplishing a *project* on time, within budget and to technical specification. The *project manager* is the single point of responsibility for achieving this.
Project Support Office	A central support unit that provides a planning and monitoring service to *project* boards and project managers.
Protocol	A set of rules that must be followed for any data communications to be made. Protocols enable totally different *platforms* (e.g. computers connected to the *Internet*) to communicate with each other. For one computer to communicate with another, both must adhere to the same *protocol(s)*.
Public key	In *cryptography*, the *key*, in an *asymmetric* encryption system, of a user's key set that is known to other users.
Quality	The attributes of a product or *service* that make it fit for its intended use. The term also embraces "value for money", which in turn implies a "satisfied *customer*".
Query	In computing, a specific set of instructions for extracting particular *data* from a *database*.
RAD	**Rapid Application Development**. An approach to *system* development that aims to speed up the development process. RAD focuses on core business requirements to the exclusion of inessential items (the *80/20 rule*), and makes extensive use of the construction of models and prototype systems in place of

Subject/term/acronym	Description
	formal system analysis and *specification*. It also makes extensive use of *CASE* (see also *DSDM*).
RAM	**Random Access Memory**. Semiconductor-based memory that can be read and written by the central processing unit (CPU) or other hardware *devices*. The term is generally understood to refer to volatile memory that does not permanently hold *data* or *programs*.
Record	(1) In computing, a collection of related *data* treated as a unit. A record is the main unit of storage within a *file*. (2) In record management, anything that provides permanent evidence of, or *information* about past events. Although the term *document* includes records, records are particular types of document that are not subject to amendment, and for which there is often a legal or contractual requirement.
Regression testing	Testing undertaken to prove that a change introduced to a *system* does not affect the way in which the remainder of the system performs.
Relational database	A type of *database* in which data is organised as a collection of two-dimensional tables. Microsoft Access and ORACLE are examples of widely used relational database systems.
Release	In *IT Service Management*, a *CI* that is introduced into the test, and subsequently the live environment. In most cases a release will also include documentation and possibly hardware as well (see also *updates* and *upgrades*).
Release (Delta)	A delta *release* does not replace all component *CIs* of a release unit, but rather includes only those *CIs* that have changed since the last version of the *software*.
Release (Full)	A full *release* replaces all components of a release unit, regardless of whether or not they have changed since the last *version* of the *software*.
RFC	**Request For Change**. (1) In *IT Service Management*, a form or screen, used to record details of an RFC to any component of an *IT infrastructure* or any aspect of an *IT service*. Generally forms the basis of authorisation for the change to take place and as such is an important audit trail item. Although rarely viewed as such, requests to introduce new *users*; alter the *access* permissions of existing users; and delete accounts are also examples. (2) **Request For Comment** on a *specification*.
Risk	In *information security*, the potential that exists for damage or unwanted consequences to arise from a *threat* exploiting a *vulnerability* to cause an *impact*. *Risk management strategies* aim to reduce risk to an acceptable level by implementing *controls* designed to reduce threat, vulnerability or impact, or a combination of these.

Subject/term/acronym	Description
Risk assessment	In *information security*, a study of the *threats* (and their likelihood), *vulnerabilities* and potential *impact*, and the theoretical effectiveness of *controls*. The results of risk assessment are used to develop security requirements and specifications.
Risk management	In *information security*, the total process involved in reducing identified *risks* to a level that is acceptable to an organisation's top management.
Rollback	In *databases*, a technique employed to protect a database against incorrect user action. The state of the database is preserved and subsequent *transactions* stored. If the user decides to implement the total set of transactions a *commit* command is issued. If the rollback command is employed the transactions are aborted and do not affect the database.
ROM	**Read-Only Memory**. A semiconductor circuit into which *code* or *data* is permanently installed by the manufacturing process. ROM contains instructions or data that can be read or executed, but not modified.
Script	A simple *program* consisting of a set of instructions that are designed to perform or automate a task or function.
Secret key	In *cryptography*, the *key* of a user's key set in an *asymmetric* or *public key* cryptographic system, which may be known only to that user.
Server	A computing unit or *node* in a *network* that provides specific *services* to network *users*, e.g. a printer server provides printing facilities to the network, and a *file* server stores users' files.
Service	Performance of a *specified* function. See also *IT service*.
Service Level Agreement	Or **SLA**, is a written agreement between a user and an IT service provider that documents the agreed service levels for an IT service (e.g. hours of operation, maximum downtimes, transaction throughput, terminal response times, security, contingency). An SLA is not normally a contract in itself, but it may form part of a contract.
Severity code	In *IT Service Management*, a simple code assigned to *problems* and *errors* to indicate the seriousness of their effect on the *quality* of an *IT service*. It is the major means of assigning priority for resolution.
Smartcard	A plastic card (of identical dimensions to a credit card) that has electronic logic embedded in it in the case of a *stored data card*, or a *microprocessor* in the case of cards with processing ability. Smartcards are commonly used to perform *digital signatures*, *authenticate* users for *access control* purposes, and *encrypt* or *decrypt* *messages*.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
SMTP	**Simple Mail Transport Protocol**. The *protocol* that is used to move e-mail and any attachments between mail *servers*.
Software	Instructions for the computer. A series of instructions that performs a particular task is called a *program*. The two main types of software are *system software* (*operating system*), which controls the workings of the computer and *application programs*, which perform the tasks for which people use computers. A common misconception is that software is *data*. It is not. Software tells the hardware how to process the data. Software is "run" (or “executed”), whereas data is "processed."
Software package	A *software program* or *application* sold to the public, ready to run, and containing all necessary components and documentation. Also called "shrink wrapped" or "off-the-shelf" software.
Software maintenance	Any modification to a *software* product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a changed environment.
Specification	A detailed description of the requirements for a product or *service*.
Spoofing	In *Information Security*, (1) assuming the characteristics of another computer system for purposes of deception. (2) Malicious *code* that masquerades as the *operating system*, presenting a *login* screen and tricking the user into revealing their *password*.
SQL	Structured Query Language, the traditional language for accessing *data* stored in a relational *database*.
Stage	A sub-section of a *project* that has its own organisational structure, life span and *stage manager*.
Stage Manager	The person who is responsible for the management and successful completion of a stage in a *project*. Generally has technical expertise in the activities being carried out within the particular stage. [see also *project manager*].
Standard	Agreed, and generally widely recognised criteria against which a product or *service* may be evaluated. See *ISO* and *BSI*.
Strategy	A detailed and systematic plan of action (see also *IS strategy*).
Superuser	A user with unrestricted access to user *files* and system *utilities*. For reasons of security, this level of access should only be granted to the minimum number of staff necessary to perform system administration duties.
Symmetric encryption	A form of *data encryption algorithm* that employs the same value of *key* for both encryption and *decryption* processes.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
System	Any collection of components that work together to perform a task. Examples are a hardware system consisting of a *microprocessor*, its allied chips and circuitry, input and output *devices*, and peripheral devices; an *operating system* consisting of a set of *programs* and data *files*; a *database management system* used to process specific kinds of *information*; or an *application system* used to perform a particular business function.
System Development Life Cycle (SDLC).	is the process of developing *information systems* through investigation, analysis, design, implementation, and maintenance.
System software	*Software* primarily concerned with co-ordinating and controlling hardware and communication resources, access to *files* and *records*, and the control and scheduling of *applications* (see also *operating system*).
TCB	**Trusted computing base**. In *Information Security*, the totality of protection mechanisms within a computer *system* (including hardware, *firmware* and *software*) the combination of which is responsible for enforcing a security *policy*.
TCP/IP	**Transmission Control Protocol/Internet Protocol**. A set of *protocols* that make *Internet* services (Telnet, FTP, e-mail, etc.) possible among computers that don't belong to the same *network*.
Telephone call centre	See *call centre*.
Test environment	A computer system or part of a computer system (made up of hardware and *system software*), which is used to run, and sometimes to build, software *releases* for acceptance testing.
Test data	In computing, *data* prepared solely to test the accuracy of the *programming* and logic of a *system*. It is used to prove each branch and combination of branches (within feasible limits) of a system and should, therefore, be as comprehensive as possible.
Threat	In *Information Security*, actions and events that may jeopardise a *system's* objectives (see *vulnerability* and *impact*).
Tranche	A block of work within a *programme*, identified to facilitate the programme's management.
Transaction	A discrete activity within a computer *system*, such as an entry of a customer order or an update of an inventory item. Transactions are usually associated with *applications*.
Trapdoor	A hidden hardware or *software* mechanism that permits *access controls* to be bypassed. Trapdoors often inserted by system developers as a convenient means of testing computer *programs* and diagnosing *bugs*.

Subject/term/acronym	Description
Trojan Horse	In *Information Security*, an apparently useful *program* that performs unauthorised functions by taking advantage of an innocent user's access rights in order to copy, misuse or destroy *data*. For example, a Trojan Horse hidden in a text editor might covertly copy sensitive *information* contained in a *file* being edited to another file that is accessible by the attacker (see also *Virus* and *Worm*).
UNIX	A highly portable, general purpose, multi-user *operating system*, generally used on small and mid-range computers (versions are also available for PCs). There is many common features between the numerous commercial versions of UNIX. UNIX provides facilities for sharing resources (disc space, CPU time, etc.) and for protecting *users' files*. For each file users can allocate individual read, write and execute privileges to themselves, members of groups and all other users. The operating system is also multitasking, which allows users to relegate *programs* that require no interaction to background processing whilst working interactively on other tasks.
Update	A new *release* of an existing *software* product. A software update usually adds relatively minor new features to a product or addresses issues found after the *program* was released. Updates can be indicated by small changes in the *software version* numbers, such as the change from version 4.0 to version 4.0b.
Upgrade	The new or enhanced version of a *software* product that is considered to have major enhancements or improvement to its features or functionality. Software upgrades are typically indicated by a significant (integer) change in the *version* number, such as from version 4.0 to version 5.0.
URL	**Uniform Resource Locator**. A uniform method where a *host* can be accessed at a specific address using a specific *protocol*. An example is http://www.nao.gov.uk/, the URL for the UK National Audit Office.
UPS	In *business continuity* an acronym for Uninterruptible Power Supply. A *device*, connected between a computer (or other electronic equipment) and a power source, that ensures that the computer's power supply is not interrupted. In most cases it also protects the computer against potentially damaging events, such as power surges and brownouts. All UPS units are equipped with a battery and a loss-of-power sensor; if the sensor detects a loss of power, it switches over to the battery so that the user has time to close down the computer in a controlled manner, thus avoiding *data* loss.
User	The individual or organisation that puts an *IT service* to productive use (see also *customer*).
User profile	In *Information Security*, a list of an individual's *access* rights, or of the access rights of a group of people who share common business needs. Access may be to physical areas, such as

Subject/term/acronym	Description
	buildings or rooms within them, or to data held within a computer system (see also *physical access* and *logical access*).
Utility program	*Software* designed to perform maintenance work on a system or on system components (e.g., backing up data; disk and *file* recovery; editing; sorting and merging; file and memory *dumps*).
Version	A particular issue or *release* of a hardware or *software* product. Version numbers are generally represented by an integer (a whole number) combined with a decimal number (for example 3.2). Successive releases of a *program* are assigned increasingly higher numbers. Major releases are reflected with whole number increments; minor releases with decimal increments. When discussing software versions, an "x" is often used after the version integer to designate a range of minor releases. For example, Internet Explorer 5.x refers to all minor releases of Internet Explorer 5.
Virus	A computer *program* designed to carry out unwanted and often damaging operations. It replicates itself by attaching to a host, which depending on the type of virus, may be a program, *macro* file or magnetic disc. In common with a human virus, the effects of a computer virus may not be detectable for a period of days or weeks during which time the virus will attempt to spread to other systems by infecting files and discs. Eventually, the effects manifest themselves when a date or sequence of events triggers the virus. *Impacts* range from prank messages to erratic *system software* performance, even catastrophic erasure of all the *information* on a hard disc.
Virtual Private Network	A VPN is a private data *network*, but one that uses the public telecommunication infrastructure, such as the Internet. It is similar in concept to a system of owned or leased lines, but provides comparable capabilities at much lower cost by using shared rather than private infrastructure. Using a virtual private network involves *encrypting* *data* before sending it through the public network and *decrypting* it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. VPN software is typically installed as part of the organisation's *firewall* server.
Volatile	In *data* storage, a term used to describe any *device* that needs to be powered on in order to function. Most microchip storage technologies are volatile, compared with optical and magnetic storage devices which are non-volatile (although considerably slower to access).
Vulnerability	In *Information Security*, a weakness or flaw (in location, physical layout, organisation, management, procedures, personnel, hardware or software) that may be exploited by a *threat* to cause an *impact*.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Warm site	In *business continuity*, a site that is fully equipped with environmental and ancillary equipment, and partly equipped with computer hardware (generally the less expensive components).
Web browser	Or web client, is *software* designed to navigate the *WWW*, view its *information* resources and, when used interactively, exchange information. Netscape Navigator and Internet Explorer are widely used examples of web browsers.
Web server	An *Internet* *host* computer that stores *web pages* and responds to requests to see them. Web servers talk to *web browsers* by using a language named *HTTP*.
Web site	A location on the World Wide Web (*WWW*). It is synonymous with *web page* and *web server*.
Web page	The basic building block of the World Wide Web (*WWW*). *Information* displayed on a web page can include highly sophisticated graphics, audio and video, the locus of contemporary creativity. Web pages are linked together to form the WWW.
Wide Area Network	(**WAN**) - a telecommunications *network* that is dispersed over a wide geographic area – possible world wide - as distinct from a local area network (*LAN*) that is generally confined to a confined geographic area, such as a building. A wide area network may be privately owned or rented; either way it usually requires the use of public (shared user) networks (e.g. the *Internet*) and/or leased communication circuits. See also VPN.
Windows NT	Often referred to as “NT”, is the high-end member of a family of *operating systems* from Microsoft. It is a completely self-contained with a built-in graphical user interface. NT is a 32-bit, multitasking operating system that features networking, symmetric multiprocessing, multithreading and security. It is a portable operating system that can run on a variety of hardware *platforms* including those based on the Intel 80386, i486 and Pentium *microprocessors* and MIPS microprocessors; it can also run on multiprocessor computers. NT supports up to 4 *gigabytes* of virtual memory and can run MS-DOS, POSIX, and OS/2 (character-mode) *applications*. *Authentication* checks are made during the *login* process (which uses a secure communications *channel*) and also during *network* operations (e.g. when a *user* or process needs access to a *service*).
Work Breakdown Structure	A tree diagram that breaks a *project* down in increasing levels of detail. The lowest level of a work breakdown structure comprises *activities*.
Workstation	This term tends to have different meanings in different contexts. Generally it refers to a high-powered microcomputer, such as a SPARC workstation and other typically single-user but very powerful machines, often running the *UNIX* *operating system*.

Information Systems Auditing – Glossary of Terms

Subject/term/acronym	Description
Worm	(1) In communications, a malicious *program* which, unlike a *virus*, is free-standing (i.e. it does not require a host). Worms replicate themselves across *networks*, cause both traffic congestion and can cause network failure. (2) In computing, Write Once Read Many (**WORM**). A data storage *device* to which *code* or *data* can be written but not altered or erased. They are generally implemented on non-rewritable optical discs, although pseudo-WORM magnetic tape devices are becoming available.
WWW	**World Wide Web**. Refers to the *information* resources of the *Internet* that are accessible via *web pages* using a *web browser*. Technically speaking, the WWW refers to the abstract cyberspace of information whereas the Internet is the physical side of the *network*, i.e. the computers and communications that link computers throughout the World.
XML	**Extensible Markup Language**, is a set of tags and declarations used as a complement to *HTML* in the construction of *web pages*.
X.25	A common communication *standard* for the transfer of *information* between terminals operating in the *packet* mode.
X.400	A communication *standard* for *message* handling systems (e.g. e-mail).
X.500	A *standard* for the storage and retrieval of directory *information* about *hosts* and *users* of distributed systems.