October 2007

Essential Practices for Information Technology Examination Manual
IT Section

Glossary

Acceptable Use Policy	A policy that documents permitted system uses and activities for a specific user and the consequences of noncompliance. May also be referred to as an AUP.
Acceptance Testing	A formal evaluation of a hardware or software product performed by the customer or user to verify that the product is performing according to specifications.
Accounting Management	Tracking of costs associated with network usage. Network accounting systems can be an automated tool to control costs and may provide the ability to identify misuse and abuse of services, allocate costs by department, report unusual requests, or look for anomalies, etc.
Alternative Site	An alternative operating location (computer center, work area) to be used by business functions when the primary facilities are inaccessible.
Anti-virus Engine	Computer software that is used to protect an organization's computer network against virus attacks from mass e-mail viruses, worms, and other e-mail based attacks. The software, or engine, scans e-mail for identified viruses and other e-mail threats. See also, "anti-virus software."
Anti-virus Software	Specialized software that detects malicious code and then disables the destructive code before further damage occurs to the computer system or network device. See also, "anti-virus engine." A variety of anti-virus software packages exist and operate in many different ways, depending upon the vendor's software implementation. All the packages use virus profiles (also called "signature files" or "definition files") to look for patterns in a computer's files or memory that indicate the possible presence of a known virus. The vendor provides these virus profiles and updates.
Audit Log	An organized record-keeping system that documents information or events in sequential order. Also referred to as a "log."
Authentication	The verification of a user's identity by a system based on the presentation of unique credentials to that system. Can also refer to the verification of a piece data.
Authorized	Allowed access to specific equipment, information, or physical areas of the business or system. An individual's level of access or authorization is typically based on the business needs and the role of the individual within the business.
Availability	Ensuring that authorized users have access to information and associated assets when required.
Biometrics	Authentication techniques that rely on measurable physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints or speech.
Bridge	A device that connects networks using the same communications protocols so that information can be passed from one to the other.
Bug	An unexpected defect, fault, flaw, or imperfection.
Cabling	The power and telecommunications lines that carry data or supporting information services internally and externally for an organization. The cabling, or wiring, may be in several forms, such as copper (twisted pair) circuits, T-1 lines, or fiber optic cables.

Glossary

Change Management (or Change Control)	The process of managing changes to an existing information systems infrastructure in order to minimize the likelihood of disruption, unauthorized alterations and errors. An established system of controls should exist in order to provide for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure.
"Clear and Conspicuous" Disclosure	A disclosure, whether in paper or electronic form, which is readily understandable and designed to call attention to the nature and significance of the information presented. A customer or a visitor to an institution's web site should be able to easily locate a disclosure.
Communications Protocol	A set of rules or standards designed to enable computers to connect with one another and to exchange information with as little error as possible.
Competence	Having the requisite ability or qualifications. The staff assigned to conduct an audit or review should collectively possess adequate professional proficiency for the tasks required.
Comprehensive	Thorough; complete; covering the entire organization.
Confidentiality	Ensuring that information is accessible only to those authorized to have access.
Configuration	In relation to networks, the entire interconnected set of hardware, or the way in which a network is laid out - the manner in which elements are connected.
Control Expectations	Outline of controls to be used to prevent, detect, or correct errors, omissions, and unauthorized intrusion.
Cookie	Information placed on a consumer's computer hard drive by a web site's server that allows the web site to monitor the user's visit to the site.
Critical Functions	Business activities or information that could not be interrupted or unavailable without significantly jeopardizing operation of the organization.
Data Classification System	An organization-defined system that categorizes data or information by varying degrees of sensitivity and criticality. The classification designation indicates the need, priority, and degree of protection necessary for each piece of data. It is a shorthand way of determining how information is to be handled and protected. The classification of any given data item is not necessarily fixed, but may change in accordance with some predetermined policy.
Definition Files	Also referred to as "virus profiles" or "signature files." Anti-virus software uses definition files to look for patterns in a computer's files or memory that indicate the possible presence of a known virus. The anti-virus software vendor provides definition files and updates to the users of its anti-virus software so the software can look for recently discovered viruses. Therefore, it is important to keep these definition files up to date. See also "anti-virus software."
Denial of Service (DoS)	A term used to describe certain forms of malicious attacks or damage to computer systems. The aim of such an attack is to prevent legitimate users from accessing their services. The action does not destroy data or resources, but prevents access or use. In network operations, "flooding" a node or link with excess data traffic and, thus, preventing legitimate traffic is an effective form of denial of service. Not to be confused with DOS, which stands for Disk Operating System, and particularly the MS-DOS operating system and its variants.

Glossary

Desk Review	One method of testing a specific component of the business continuity plan. Typically, the owner or author of the component reviews it for accuracy and completeness and signs off.
Digital Certificates	Electronic files to which a digital or electronic signature is attached. A trusted third party, a Certificate Authority, which verifies the identity of the certificate's holder, issues the certificates.
Disaster Declaration	A formal announcement by pre-authorized personnel that a disaster or disruption is predicted or has occurred and that triggers pre-arranged mitigating actions.
Edit Check	A function of the computer software that reviews data input to see if it matches certain requirements.
Electronic Commerce (E-commerce)	Buying, selling, or working in an electronic medium. The following is a small sample of items considered E-commerce: • Lending (on-line banking, on-line applications, automated telephone transactions); • Employee Services (Human Resources, time tracking, 401(k), employee benefits, health care information); • Related Services (crop insurance filings, credit life insurance, tax information, collateral searches, UCC filings, credit reporting services); • Reporting (posting Shareholder Reports or other compliance-related issues on a web site); • Business-to-Business Activity (servicing of and reporting on loan participations, pricing/funds ordering, submission of loan data, FTP transmissions); • Marketing/Advertising (web sites, third party dealers); and • Communications (Internet E-mail, Extranets, Value Added Networks or VANs)
Electronic Signature	Also referred to as a digital signature. An electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. The electronic or digital signature is a piece of data that is sent with an encoded message to uniquely identify the originator and to verify that the message has not been altered since it was sent. It also supports non-repudiation. In other words, it may legally be used to resolve disputes between parties in a transaction, should one party deny that the transaction occurred.
Encryption	The process of encoding data to prevent unauthorized access, especially during transmission. Encryption is usually based on a key that is essential for decoding.
Engine	When used in relation to the term "anti-virus," this refers to an anti-virus software product. The software is used to protect an organization's computer network against virus attacks from mass e-mail viruses, worms, and other e-mail based attacks. The software, or engine, scans e-mail for identified viruses and other e-mail threats. See also "anti-virus engine" and "anti-virus software."
Equipment	The technology-related fixed assets of a business enterprise.
Fault	A physical defect, such as a loose connection, that prevents a system or device from operating as it should.

Glossary

Firewall	A device or collection of components (computers, routers, and software) that enforces a boundary between two or more networks.
Firewall Architecture	The design and structure of the components of a firewall or firewall system and how they connect and interact with one another.
Gateway	A device that connects networks using different communications protocols so that information can be passed from one to the other. A gateway both transfers information and converts it to a form compatible with the protocols used by the receiving network.
Hyperlink	An electronic pathway that may be displayed in the form of highlighted text, graphics, or a button that connects one web page with another web page address.
Impact Analysis	An analysis showing the quantification of the effect an action had.
Independence	The quality or state of being independent; not subject to control by others; not looking to others for opinion or guidance. In all matters relating to the audit or review work, auditors/reviewers should be free from personal and external impairments to independence, should be organizationally/functionally independent, and should maintain an independent attitude and image.
Interface	The point at which a connection is made between two elements so that they can work with each other. Sometimes a card, plug, or other device that connects pieces of hardware with the computer so information can be moved from place to place.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Internet	A global network that connects millions of computers. More than 100 countries are linked into exchanges of data, news, and opinions. The Internet is decentralized by design. Each Internet computer, called a "host," is independent. Its operators can choose which Internet services to use and which local services to make available to the global Internet community. The Internet is **not** synonymous with "World Wide Web." Not all Internet servers are part of the World Wide Web.
Internet Domain Name	A unique identifier for an Internet site that can be compared to a mailing address for a physical location. A domain name often includes two or more parts separated by periods. Common suffixes (called "top-level domains") include .com, .net and .org, in addition to country-related domains such as .us for the United States. Separate registration is required for ownership of each variation of a domain name (e.g., bankname.com, bankname.net and bankname.org).
Intrusion Detection System (IDS)	A system of hardware and software that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Though they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

Glossary

ISO	The International Organization for Standardization together with the International Electrotechnical Commission (IEC) for the specialized system for worldwide standardization. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 percent of the national bodies casting a vote.
Limit Test	A test of specified amount fields against stipulated high or low limits of acceptability. When both high and low values are used, the test may be called a range check.
Local Area Network (LAN)	A data communications system that connects intelligent computer devices, peripherals, and software over a relatively limited area, so users can communicate and share resources.
Log	An organized record-keeping system that documents information or events in sequential order. Also referred to as an "audit log."
Logical Access	The ability to use computer resources, which is usually controlled by a user identification and authorization system.
Logical Security	The standards and procedures designed to protect data against accidental or intentional unauthorized disclosure, modification, or destruction.
Malicious Code	Any program that acts in unexpected and potentially damaging ways. Common types of malicious code are viruses, worms, and Trojan horses.
Media	Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).
Mission Critical Applications	Computer applications and databases identified by an institution as absolutely necessary to the organization in order to perform their core business processes.
Network	A group of computers and associated devices that are connected by communications facilities.
Network Architecture	The underlying structure of a computer network including hardware, interfaces, and protocols used to establish communication and ensure the reliable transfer of information.
Non-repudiation	In reference to digital security, non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message.
Parallel Testing	The process of feeding test data into two systems, the modified system and an alternate system (possibly the original system), and comparing results.
Passwords and Personal Identification Numbers (PINs)	Unique string of characters assigned to the authorized user. The system compared the code against a stored list of authorized passwords or PINS and users. If the code is legitimate, the system allows the user access at whatever security level has been approved for the owner of the password or PIN.

Glossary

Patch	A piece of software code that is inserted into a program to fix a defect temporarily. Patches are developed and released by software vendors when vulnerabilities are discovered.
Performance Monitor	A process or program that appraises and records status information about various system devices and other processes.
Physical Security	The various measures or controls that protect an organization from a loss of computer processing capability that is caused by theft, fire, flood, malicious destruction, mechanical failure, or power failure.
Production System	A group of interdependent computers (hardware and software) that interact regularly to perform a task.
Prototyping	The creation of a working model of a new computer system or program for testing and refinement. Prototyping is used in the development of both new hardware and software systems and new systems of information management. Tools used in the former include both hardware and support software; tools used in the latter can include databases, screen mockups, and simulations that, in some cases, can be developed into a final product.
Public Key Infrastructure	A system of digital certificates, certificate authorities, and other registration processes used to verify and authenticate the validity of each party involved in an electronic transaction. An asymmetric scheme that uses a pair of keys for encryption: the public key encrypts data, and a corresponding secret key decrypts it. For digital signatures, the process is reversed: the sender uses the secret key to create a unique electronic number that can be read by anyone possessing the corresponding public key, which verifies that the message is truly from the sender.
Real-time Monitoring	Monitoring of activity as it occurs rather than storing the information for later review.
Reasonableness Test	A comparison of data to predefined reasonability limits or occurrence rates established for the data.
Regression Testing	A thorough test of any changes to existing programs may include regression testing (testing of unchanged code). The analysis and specifications must clearly identify user needs and expectations within the proposed application. The selective retesting of a software system that has been modified to ensure that any bugs have been fixed and that no other previously- working functions have failed as a result of the changes and that newly added features have not created problems with previous versions of the software. Also referred to as “verification testing.” Regression testing is initiated after a programmer has attempted to fix a recognized problem or has added source code to a program that may have inadvertently introduced errors. It is a quality control measure to ensure that the newly modified code still complies with its specified requirements and that unmodified code has not been affected by the maintenance activity.
Remediation	Contract provision that attempts to resolve problems in an expeditious manner as well as provide for continuation of services during the dispute resolution process.
Requirements Definition	The requirements definition converts the system concepts into detailed specifications. The analysis and specifications must clearly identify user needs and expectations within the proposed application.

Glossary

Repeater	A hardware device that passes all traffic in both directions between the LAN segments they link.
Risk Assessment	A process to identify threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes. Information security risk assessment is the process used to identify and understand risks to the ***confidentiality***, ***integrity***, and ***availability*** of information and information systems. An adequate assessment identifies the value and sensitivity of information and system components, and then balances that knowledge with the exposure from threats and vulnerabilities. A risk assessment is a necessary pre-requisite for creating strategies to guide the institution as it develops, implements, tests, and maintains its information systems security posture. An initial risk assessment may involve a significant one-time effort, but the risk assessment process should be an ongoing part of the information security program.
Risk-based Examination	An examination approach that seeks to stay abreast of risk in an individual institution and focus examination efforts and resources in areas that could materially impact the safety and soundness of the institution. This does not mean that certain examination areas are ignored. In fact, all applicable areas are initially considered for examination during institutional examination planning and on an ongoing basis as new information is obtained. The result is a dynamic examination scope that concentrates examination effort on the specific areas, within each of the CAMEL factors, which materially impact the condition of the institution. The depth of testing in each area within the examination scope is also risk-based. Depth of testing is determined by the need to complete sufficient work to reach a conclusion. The flexibility exists to modify both scope and depth of testing based on new information obtained or preliminary results achieved. The examiner uses sound judgment in making these determinations.
Risk Management	The process of identifying, controlling and minimizing or eliminating risks that may affect information systems, for an acceptable cost.
Router	A hardware device that joins two networks. A router distinguishes data packets by their protocol type and forwards traffic according to the logical or protocol address.
SAS 70	Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally includes controls over information technology and related processes. SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' audits in a uniform reporting format. A SAS 70 report cannot include objectives related to Disaster Recovery/Continuity Planning or other forward-looking statements.
Schematic	A diagram that uses lines and standard symbols to represent the components of a network and the connections between them.
Security Event	An event that compromises the ***confidentiality***, ***integrity***, or ***availability*** of an information system.

Glossary

Secure Socket Layer (SSL)	Secure Socket Layer is a standard for establishing a secure communications channel to prevent the interception of critical information, such as credit card numbers. The primary purpose of SSL is to enable secure electronic financial transactions on the Web.
Segregation of Duties	Also referred to as "separation of duties." A basic control that prevents or detects errors and irregularities by assigning responsibility for initiating transactions, recording transactions, and custody of assets to separate individuals. Used in IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.
Service Level Agreement (SLA)	Contractually binding clauses documenting the performance standard and service quality agreed to by the institution and service provider. The SLA's primary purpose is to specify and clarify performance expectations, as well as establish accountability. A well-designed SLA will recognize and reward, or at least acknowledge, good service. It will also provide the measurement structure—or performance metric—to identify substandard service and trigger correction or cancellation provisions as warranted. In today's environment, incentives or penalties in the SLA can be an effective tool for managing service. If services received do not measure up to expectations, direct consequences, such as reduced levels of compensation or a credit on future services, would result.
Server	A computer or other device that manages a network service. An example is a print server, a device that manages network printing.
Simulation	One method of testing the business continuity plan in which one or more teams are performed under conditions that simulate "disaster mode". The testing may or may not be performed at the designated alternate location.
Siting	Location.
Social Engineering	Obtaining information from individuals by trickery. By using persuasion, being aggressive, or using other interpersonal skills, an attacker may encourage a legitimate user or other authorized person to give them authentication credentials.
Source Program	Initially, a programmer writes a program in a particular programming language. This form of the program is called the *source program,* or more generically, *source code.* To execute the program, however, the programmer must translate it into machine language, the language that the computer understands. The first step of this translation process is usually performed by a utility called a compiler. The compiler translates the source code into a form called object code. Sometimes the object code is the same as machine code; sometimes it needs to be translated into machine language by a utility called an assembler.
Source Code	Human-readable program statements written in a high-level or assembly language that is not directly readable by a computer.
Systems Development Life Cycle (SDLC)	A documented approach to developing an information system or software product that is characterized by a linear sequence of steps that progress from start to finish.
Tokens	Small physic al devices that are usually used in conjunction with a password to gain entry to a computer system.
Topology	The shape or the way that the various individual parts of the network are connected.

Glossary

Trojan Horse	Malicious code that is hidden in software that appears to be beneficial or harmless.
Unauthorized	Not allowed access to specific equipment, information, or physical areas of the business or system. This could refer to an outside intruder or to an employee whose business needs or role does not include use of the specified equipment, information, or physical areas of the business or system.
Unauthorized Modification	The act of changing data or computer programming code without the authority or permission to do so.
Uniform Resource Locator (URL)	The global address of a document and other resources on the World Wide Web. The first part of the address indicates what protocol to use; the second part specifies the IP address or the domain name where the resource is located.
User Education Program	A formal training program for all employees that teaches staff about their security roles and responsibilities within the organization. Training should support security awareness, strengthen compliance with the organization's security policy(ies), and be updated regularly.
User Testing	Independent verification of test results by user representatives.
Virus	Malicious code that replicates itself within a computer.
Virtualization	Virtualization is a broad term that refers to the abstraction of computer resources. One useful definition is "a technique for hiding the physical characteristics of computing resources from the way in which other systems, applications, or end users interact with those resources. This includes making a single physical resource (such as a server, an operating system, an application, or storage device) appear to function as multiple logical resources; or it can include making multiple physical resources (such as storage devices or servers) appear as a single logical resource.
Weblinking Relationship	A relationship with a third party that involves both the institution's web site and the third party's web site. When an institution customer accesses a third party web site from the institution's web site, the customer gains access through a hyperlink.
Web Page	A document on the World Wide Web. A viewable screen displaying information presented through a web browser in a single view sometimes requiring the user to scroll to review the entire page. A bank web page may display the institution's logo, provide information about institution products and services, or allow a customer to interact with the institution or third parties that have contracted with the institution. Every web page is identified by a unique URL (Uniform Resource Locator).
Web Site	A site (location) on the World Wide Web. Each web site contains a home page, which is the first document that users see when they enter the site. The site might also contain additional documents and files. A person can view the pages of a web site in any order, as he or she would a magazine. Each site is owned and managed by an individual, company, or organization.
Wireless Access Point	A device that permits wireless access to a computer network through a physical connection to the network.
Wiring Closet	A secured location that represents the transition between vertical and horizontal wiring within the network infrastructure for each floor of the building.

Glossary

Wide Area Network (WAN)	A communications network that connects geographically separated areas.
World Wide Web (www)	A system of Internet servers that support specially formatted documents. The World Wide Web, or simply Web, is a way of accessing information over the medium of the Internet. The documents are formatted in a script called HTML, "HyperText Markup Language," that supports links to other documents, as well as graphics, audio, and video files. This allows a user to jump from one document to another simply by clicking on hot spots. World Wide Web is **not** synonymous with "the Internet." Not all Internet servers are part of the World Wide Web.
Worm	Malicious code that infects computers across a network without user intervention.