Accounting information system

| CH 8: Authentication: Process of verifying the identity of the person or device attempting to access the | | system. The objective is to ensure that only legitimate users can access the system. Three different | | credentials are PINs(password), ID badge, or biometrics. Authorization: Process of restricting access of | | authenticated users to specific portions of the system and limiting what actions they are permitted to | | perform. Access control matrix: shows that access controls of each user or device in your company to see | | who have what privileges.

Best Practice of Passwords: Must have at least 8 characters in length, must have| | multiple character types (upper-lower case, numbers, and special characters), Randomness (not be words | | found in dictionary), and changed frequently (every 30 for sensitive of 90 for most users). Physical | | Access Controls: Only have one unlocked door during business hours (none after hours), safe lock all | | devices (computers, phones, and PDA devices), and physical access controls must be cost-effective. Access | | to the wiring used in the org’s LANs needs to be restricted in order to prevent wiretapping.

Firewall: | | behind the border router (connects an orgs information system to the internet), and is either a | | special-purpose hardware device or software running on a general-purpose computer. The demiliarized is a | | seperate network that permits controlled access from the internet to selected resources, such as the | | organizarion’s e-commerce Web server. Intrusion Prevention System: Monitors patterns in the traffic flow, | | rather than only inspecting individual packets, to identify and automatically block attacks.

Examining | | pattern traffic is often the only way to identify undesirable activity. Intrusion Detection System | | consists of a set of sensors and a central monitoring unit that create logs of network traffic that was | | permitted to pass the firewall and then analyze those logs for signs of attempted or successful | | intrusions. The difference between the two is that the IPS only produces a warning alert when it detects a| | suspicious pattern of network traffic, whereas the IDS not only issues an alert but also automatically | | takes steps to stop a suspected attack.

Preventive controls that deter problems before they arise. | | Effective preventive controls include hiring qualified accounting personnel; appropriately segregating | | employee duties; and effectively controlling physical access to assets, facilities, and information | | Detective controls enhance security by monitoring the effectiveness of preventive controls and detecting | | incidents in which preventive controls have been successfully circumvented. Corrective are procedures that| | correct problems that have occurred.

Social Engineering: Attackers will often try to use the information | | obtained during their initial reconnaissance to trick an unsuspecting employee into granting them access. | | | | | | CH 9: Encryption: The process of transforming normal content, called plaintext, into unreadable gibberish,| | called ciphertext.

This is a type of preventive control. Public key to encryption is widely distributed | | and available to everyone. Decryption reverses this process, transforming ciphertext back into plaintext. | | Hashing: The process that takes plaintext of any length and transform it into a short code called a hash. | | Digital Signatures: A hash of a document or file that is encrypted using the document creator’s private | | key. This provides proof about two important issues: 1. That a copy of a document or file has not been | | altered 2.

Who created the original version of a digital document or file. Digital certificate: An | | electronic document that contains an entity’s public key and certifies the identity of the owner of that | | particular public key. It is issued by certificate authority. Thus, digital certificates function like the| | digital equivalent of a driver’s license or passport. It can also be the very sign logo on certain website| | to show that this is a trusted site. Virtual Private Networks: Encrypting information while it transverses| | the Internet creates a VPN.

It provides the functionality of a privately owned secure network without the | | associated costs of leased telephone lines, satellites, and other communication equipment. Private | | communication channels, often referred to as tunnels, which are accessible only to those parties | | possessing that appropriate encryption and decryption keys. | | | | CH 10: Field Check determines whether the characters in a field are of the proper type. Sign Check | | determines whether the data in a field have the appropriate arithmetic sign.

Limit Check tests a numerical| | amount against a fixed value. Range Check tests whether a numerical amount falls between predetermined | | whether all required data items have been entered. A Completeness Check on each input record determines | | whether all required data items have been entered. Validity Check compares the ID code or account number | | in transaction data with similar data in the master file to verify that the account exists. Reasonableness| | Test determines the correctness of the logical relationship between two data items.

Batch Totals | | summarizes important values for a batch of input records. The following are three commonly used batch | | totals: 1. Financial totals sums a field that contains monetary values, such as the total dollar amount of | | all sales for a batch of sales transactions 2. Hash total sums a nonfinancial numeric field, such as the | | total of the quantity ordered field in a batch of sales transactions 3. Record count is the number of | | records in a batch. Processing Controls: 1.

File Labels ensure correct and most current file is being | | updated 2. Batch Total Recalculation compares calculated batch total after processing to input totals | | 3. Cross-Footing and Zero Balance Tests compute totals using multiple methods to ensure the same results | | 4. Concurrent Update locks records or fields when they are being updated so multiple users are not updating| | at the same time. Output Controls: 1. Management Review verifies reasonableness, completeness, and if | | routed to intended individual 2.

Reconciliation: All transactions and other system updates should be | | reconciled to control reports, file status/update reports, or other control mechanisms. In additions, | | general ledger accounts should be reconciled to subsidiary account totals on a regular basis. Also, | | database totals should periodically be reconciled with data maintained outside the system. (Match employee| | files in payroll to that in the HR department to see if any fake names were created. 3.

Data Transmission | | Controls: Check sums is a hash of file transmitted, comparison made of hash before and after transmission. | | Parity checking is a bit added to each character transmitted, the characters can then be verified for | | accuracy. Data Backup Procedures: 1. Incremental Backup involves copying only the data items that have | | changed since the last partial backup. This produces a set of incremental backup files, each containing | | the results of one day's transactions 2. Differential Backup copies all changes made since the last full | | backup.

Thus, each new differential backup file contains the cumulative effects of all activity since the | | last full backup. Daily differential backups take longer than incremental backups. Disaster Recovery Plan | | outlines the procedures to restore an organization's IT functions in the event that its data center is | | destroyed by a natural disaster or act of terrorism. Cold site is the first option, which is an empty | | building that is prewired for necessary telephone and internet access, plus a contract with one or more | | vendors to provide all necessary equipment with a specified period of time.

Hot site is the second option,| | which is a facility that is not only prewired for telephone and Internet access but also contains all the | | computing and office equipment the org needs to perform its essential business activities. (shorter RTO | | time that cold site) Business Continuity Plan specifies how to resume not only IT operations, but all | | business processes, including relocation to new offices and hiring temp replacements, in the event that a | | major calamity destroys not only an org's data center but also its main headquarters.

Having a DRP and BCP| | can mean the difference between sustaining a major catastrophe and going out of business. Cloud computing | | typically utilizes banks of redundant servers in multiple locations, thereby reducing the risk that a | | single catastrophe could result in system downtime and the loss of all data. However if the public cloud | | goes out of business, it will be difficult to retrieve any information. Change control is the formal | | process used to ensure that modifications to hardware, software or processes do not reduce system | | reliability. | CH 7: Internal Control: The process implemented to prove reasonable assurance that the following control | | objectives are achieved: 1. Safeguard assets: prevent or detect their unauthorized acquisition, use, or | | disposition. 2. Maintain records in sufficient detail to report company assets accurately and fairly | | 3. Provide accurate and reliable information 4. prepare financial reports in accordance with established | | criteria 5. Promote and improve operational efficiency 6. Encourage adherence to prescribed managerial | | policies 7.

Comply with applicable laws and regulations. Internal controls perform three important | | functions: 1. Preventive controls (most important) defer problems before they arise. Examples include | | hiring qualified personnel, segregating employee duties, and controlling physical access to assets and | | information 2. Detective controls discover problems that are not prevented. Examples include duplicate | | checking of calculations and preparing bank reconciliations and monthly trial balances 3.

Corrective | | controls identify and correct problems as well as correct and recover from the resulting errors. Examples | | include maintaining backup copies of files, correcting data entry errors, and resubmitting transactions | |

for subsequent processing. Segregation of duties: No one employee should be given too much responsibility | | 1. Authorization: Approving transactions and decisions 2. Recording: Preparaing source documents; entering | | data into online systems; maintaining journals, ledgers, files or databases; and preparing reconciliations| | and performance reports 3.

Custody: Handling cash, tools, inventory, or fixed assets; receiving incoming | | customer checks; writing checks. SOX 2002: Designed to prevent financial statement fraud, make financial | | reports more transparent, protect investors, strengthen internal controls, and punish executives who | | perpetrate fraud 1. Created PCAOB to control the auditing profession 2. New Auditing Rules: Partners must | | rotate periodically and prohibits auditors from performing certain nonaudit services, such as information | | systems design and implementation 3.

New Roles for Audit Committee: Must be part of board of directors and | | be independent, one member must be a financial expert and oversees external auditors . The audit committee| | is responsible for financial reporting, regulatory compliance, internal control, and hiring and overseeing| | internal and external auditors4. New Rules for Management: Financial statements and disclosures are fairly | | presented, were reviewed by management, and are not misleading; the auditors were told about all material | | internal control weak-ness and fraud 5.

New Internal Control Requirements: Management is responsible for | | establishing and maintaining an adequate internal control system. COBIT: consolidates control standards | | from 36 different sources into a single framework that allows 1. Management to benchmark security and | | control practices of IT environments 2. Users to be assured that adequate IT security and control exist | | 3. Auditors to substantiate their internal control opinions and to advise on IT security and control | | matters. COBIT Framework addresses: 1. Business objectives 2. IT resources 3. IT processes.

COSO - authority | | on internal controls and is incorporated into policies, rules, and regulations used to control business | | activities. Five components of the IC framework: 1. Control environment 2. Control activities 3. Risk | | assessment 4. Information and communication 5. Monitoring. COSO Enterprise Risk Management: second control | | framework developed by COSO. It is the process the board of directors and management use to set strategy, | | identify events that may affect the entity, assess and manage risk, and provide reasonable assurance that | | the company achieves its objectives and goals. | | | CH 11: Auditing: The systematic process of obtaining and evaluating evidence regarding assertions about | | economic actions and events in order to determine how well they correspond with established criteria. | | Internal auditing is an independent, objective assurance and consulting activity designed to add value and| | improve organizational effectiveness and efficiency, including assisting in the design and implementation | | of an AIS.

Audit Process: 1. Audit Planning 2. Collection of Audit Evidence 3. Evaluation of Audit Evidence | | 4. Communication of Audit Results. Audit Plan: Why, when, how and whom. Work targeted to area with greatest| | risk: Inherent is the chance of risk in the absence of controls Control: is the risk a misstatement will | | not be caught by the internal control system Detection is the chance that a misstatement will not by | | caught by auditors or their procedures.

Collections of Audit Evidence: Review of documentation to | | understand how a particular process or internal control sytem is supposed to function; Physical | | examination of the quality and/or condition of tangible assets, such as equipment and inventory; Vouching | | for validity of a transaction by exmaining supporting document; Analytical review of relationships and | | trends among information to detect items that should be further investigated Evaluation of Audit Evidence:| | Does evidence support favorable or unfavorable conclusion?

It is material (How significant is the impact | | of the evidence)? Reasonable Assurance (some risk remains that the audit conclusion is incorrect) | | Communication of Audit Conclusion: Written report summarizing audit finding and recommendations to | | management, the audit committee, the board of directors and other appropriate parties. Types of Audits: | | 1. Financial examines the reliability and integrity of financial transactions, accounting records, and | | financial statements 2.

Information System reviews the controls of an AIS to access compliance with | | internal control policies and procedures and effectiveness in safeguarding assets 3. Operational is | | concerned with economical and efficient use of resources and the accomplishments of established goals and | | objectives 4. Compliance determines whether entities are complying with applicable laws, regulations, | | policies and procedures. Risk-based Audit: 1. Determine the threats (fraud and errors) facing the company. | Accidental or intentional abuse and damage to which the system is exposed 2. Identify the control | |

procedures that prevent, detect, or correct the threats. These are all the controls that management has | | put into place and that auditors should review and test, to minimize the threats 3. Evaluate control | | procedures using two ways, a system review (are control procedures in place) and tests of controls (are | | existing controls working) 4.

Evaluate control weaknesses to determine their effect on the nature, timing | | or extent of auditing procedures. The minimum number of samples to be selected for IT control is only 1. | | CAATS(audit software) uses auditor-supplied specifications to generate a program that performs audit | | functions, thereby automating or simplying the audit process | | | | SA 2: Physical access controls- 1.

Alternate power sources 2. Flood Management 3. Data backup 4. Fences are | | physical barrier to deter casual trespassers5. Human Guards to watch doors etc. 6. Physical Locks 7. Fire | | Suppression systems 8. Biometrics 9. Location of assets 10. Man traps 11. Alarm systems 12. Steel cages | | around wiring system to prevent wiretapping Logical Access Controls – 1. firewall or screening router that | | makes pass/block decisions based upon the type of traffic, origin, and destination 2. n application that | | first authenticates a user by requiring a user ID and password before permitting the user to access the | | application 3. Authentication, Authorization | | | | Preventive Controls: Training, user access controls (authentication and authorization), physical access | | controls (locks, guards, etc.), Network access controls (firewalls, intrusion prevention systems, etc.), | | Device and software hardening controls (configuration options).

Detective Controls: Log analysis, | | intrusion detection system, security testing and audits, and managerial reports. Corrective Controls: | | Computer incident response teams (CIRT), Chief information security officer (CISO), and patch management. | | | | | | | | | | |