Information Technology Management, Audit & Control (S-15)
(Suggested Answers)

Answer 1

(a)

(i) An integrated Supply Chain Management (SCM) application helps in improving relationship with customers and suppliers by:

- Quick order processing and delivery of goods.
- Ensuring availability of goods.
- Correct product and price information.
- Timely payments.

(ii) The SCM application helps in reducing costs of operation by:

- Reducing manpower requirements through greater automation.
- Lowering the levels of inventory.

(iii) The SCM application helps in greater co-ordination within the departments by providing single source of information which results in:

- timely response among departments; and
- lesser conflicts in views.

(b) The company is expected to undertake the following changes in order to implement a Supply Chain Management System:

(i) Implementation of international e-business standards.
(ii) Standardization of taxonomies, terms and semantics, both general as well as industry specific.
(iii) Integrating the system with suppliers and customers.
(iv) Developing the ability to deal with different languages, laws and customs.
(v) Ensuring 24 X 7 availability of systems.
(vi) Enhancing logical and physical controls on data.
(vii) Centralized storage of information.
(viii) Hardware and software upgrades.
(ix) Training of existing staff.

Answer 2

(a) Alternative Processing Arrangements

- Hot sites
- Warm sites
- Cold sites
- Reciprocal arrangements with other companies
- Duplicate information processing facilities

The following types of off-site backup hardware facilities are available:

Hot Sites are fully configured and ready to operate within several hours. The equipment and systems software must be compatible with the primary installation being backed up. The only additional needs are staff, programs, data files and documentation.

Costs associated with the use of a third-party hot site are usually high but are often cost justifiable for critical applications. When properly planned, insurance coverage will usually offset the costs incurred for using this type of facility. Costs include a basic subscription cost, monthly fee and activation 'costs that may apply when the site is used for an actual emergency an hourly or daily use charges. Pricing structures vary between vendors.

The hot site is intended for emergency operations of a limited time period and not for long-term extended

use. Long-term use would impair the protection of other subscribers. Therefore, the hot site should be viewed as a means of accomplishing the continuation of essential operations for a period of up to several weeks following a disaster or major emergency. Further plans are still necessary to provide for subsequent operations. Several vendors offer warm or cold site facilities for a subscriber to migrate to after recovery of operations has been completed. This will free the hot site for use by other subscribers.

Warm Sites are partially configured, usually with network connections and selected peripheral equipment such as disk drives, tape drives and controllers, but without the main computer. Sometimes a warm site is equipped with a less powerful CPU than the on generally used. The assumption behind the warm site concept is that the computer can usually be obtained quickly for emergency installation (provided it is a widely used model) and since, the computer is the most expensive unit, such an arrangement is less costly than a hot site. After the 'installation of the needed components the site can be ready for service within hours; however the location and installation of the CPU and other missing units could take several days or weeks.

Cold Sites have only the basic environment (electrical wiring; air conditioning, flooring, etc.) to operate an information processing facility. The cold site is ready to receive equipment but does not offer any components at the site in advance of the need. Activation of the site may take several weeks.

Duplicate Information Processing Facilities are dedicated, self-developed recovery sites that can back up critical applications. The assumption is that there are fewer problems in coordinating compatibility and availability in the case of duplicate information processing facility sites. However, larger organizations may experience problems similar to those encountered by reciprocal agreements between unrelated companies. Several principles must be in place to ensure the viability of this approach:

- The site chosen should not be subject to the same natural disaster(s) as the original (primary) site.
- There must be a coordination of hardware/software strategies. A reasonable degree of compatibility must exist to serve as a basis for backup.
- Resource availability must be assured. The workloads of the sites must be monitored to ensure that availability for emergency backup use would not be impaired.
- Regular testing is necessary. Even though duplicate sites are under common ownership and even if the sites are under the same management, testing of the backup operation is necessary.
- Reciprocal Agreements are between two or more, organizations with similar equipment or applications, under the typical agreement, participants promise to provide computer time to each other when an emergency arises.

b)

	Resource	Nature of backup
1.	Personnel	Training and rotation of duties among IS staff, so they can take the place of others Arrangement with another company for provision of staff
2.	Hardware	Redundant hardware Arrangement with another company for provision of Hardware
3.	Facilities	Company's own alternative processing facilities arrangements. Arrangement with another company for provision of alternative processing facilities arrangements.
4.	Documentation	Inventory of documentation stored securely on site and off site.
5.	Supplies	Inventory of supplies stored securely on site and off site with list of vendors of all supplies.
6.	Data/Information	Inventory of files stored securely on site and off site.
7.	Application Software	Inventory of Application software stored securely on site and off site.
8.	System Software	Inventory of system software stored securely on site and off site.

Answer 3

(a) Segregation of duties means that important responsibilities are distributed between two or more individuals. As a result check and balances are created as work of one person is checked by the other.

If adequate segregation of duties does not exist, the following could occur:

- Misappropriation of assets **OR** Chances to fraud increases.
- Inaccurate information (i.e. errors or irregularities remain undetected).
- Modification of data could go undetected.

Suggested best practices for preventing and detecting frauds that may be committed by key information systems personnel are as follows:

(i) **Carry out periodic enterprise-wide risk assessments**
Periodic risk assessment procedure helps to identify risks which may result in loss to the organization.

(ii) **Clearly document insider threat controls.**
Clear documentation helps to ensure fewer gaps for attack and better understanding by employees.

(iii) **Carry out periodic security awareness training for all employees**
If the employees are trained and understand security policies and procedures, and why they exist, they will be encouraged and able to avert security lapses.

(iv) **Third Party Audits**
Third Party Audits can helps us to ensure the reliability on our system, e.g SysTrust etc

(v) **Log, monitor, and audit online actions of the employees**
Periodic logging, monitoring and auditing discourages and discovers inappropriate actions.

(vi) **Use extra caution with system administrators and privileged users**
Typically, logging and monitoring is performed by a combination of system administrators and privileged users. Therefore, additional vigilance must be devoted to those users.

(vii) **Monitor and respond to suspicious or disruptive behavior**
Policies and procedures should be in place for all employees to report such behavior, with required follow-up by management.

(viii) **Physical controls**
Close circuit cameras, biometrics and digital door locks etc. serve a good physical control against insiders' threat.

(ix) **Deactivate computer access immediately after termination**
Immediate deactivation policy will discourage losses due to lapses and slackness.

(x) **Forced leave policy**
Mandatory leave policy helps in successful succession planning. It also tests the organization's preparedness in case its key IT personnel left.

(xi) **Restricted use of removable media**
This practice helps in minimizing the chances of virus and worms in the system. It also mitigates the chances of theft of sensitive data.

(xii) **Access to sensitive data/ information on need to have basis**
This practice enhances the security and confidentiality of data. Since access to data is allowed on proper authorization, track of any modification to it can be detected easily.

Answer 4

Evaluation of Security at Offsite Facility

The security of the offsite facility should be evaluated to ensure that it has the proper physical and environmental access control. These controls include the ability to limit access to only authorized users of the facility, secure flooring, humidity controls, temperature controls, specialized circuit , Uninterruptible power supply, water detection devices, smoke detectors and an appropriate fire Extinguishing system. The IS auditor should examine the equipment for current inspection and Calibration tags, this review should also consider the security requirements of media transportation.

Threats and vulnerabilities of wireless systems

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and is transmitted between two wireless devices may be intercepted and disclosed.
- DoS attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.

Firewall Issues

Problems that may be faced by organizations with firewalls may include:

- False sense of security may exist where management feels that no further security checks and controls are needed.
- The majority of incidents are caused by insiders, who are not controlled by firewalls (firewall assumes "bad guys are outside").
- Misconfigured firewalls may allow unknown and dangerous services to execute.
- Firewall policies may not be maintained regularly.
- Monitoring activities may not occur on regular basis (i .e. log creation utilities may not be appropriately applied and reviewed).
- Host firewalls operate at the network layer; therefore, they do not stop any application-layer input-based attacks.

Evaluation of Controls over interconnection of Portable machines with Company's network

1. Evaluate whether the Installation and configuration of application software on Portable machines (e.g. Smart Phones and Laptops) do comply with the existing company standards for information security.
2. Evaluate whether documented procedures exist for Addition, deletion or modification of any application. Review whether these procedures are known to and followed by users.
3. Evaluate whether Employees are instructed to exercise due care during travel as well as within office environment.
4. Evaluate whether employees are aware of immediate incident reporting procedures if any loss or theft of an assets occurs.
5. Evaluate whether a trust list of remote access points existed, documented, followed, logged and reviewed.
6. Evaluate whether appropriate authentication mechanisms are available, and users are made aware of common security issues.
7. Evaluate whether appropriate Data Communication controls existed, documented, followed, logged and reviewed (e.g. encryption, PKI, Digital signatures etc)

8. Evaluate whether server access logs are generated regularly and reviewed periodically.
9. Evaluate whether all machines are with updated antivirus software.
10. Evaluate whether properly configured firewall is installed and maintained.
11. Evaluate whether an intrusion detection system is installed and maintained in the company system.

Answer 5

Following documents may be reviewed to gain an understanding of the GL application:

Documents describing user requirements

These documents help in identifying the essential system components.

Documents describing cost benefit analysis

These documents help in understanding the need and objective of each module and functionality of the application.

Functional design specifications

This document provides a detailed explanation of the application.

Documents describing modifications in program

Such documents will help in evaluating whether the application has been working satisfactorily, understanding the change in user requirements and change management controls.

User manuals

A review of the user manual will allow us to determine whether it contains appropriate guidance for the users.

Technical reference manual

Its review helps in understanding access rules and logic of the application.

(b)Input Controls

Terminal/Client's workstation identification check

This check is used to limit input to specific terminals as well as to individuals. Client workstations in a network can be configured with a unique form of identification, such as serial number or computer name, that is authenticated by the system.

Effectiveness testing

(i) Check if list of authorized terminals is in place and is updated.
(ii) Attempt accessing the system from unauthorized terminal.
(iii) Observe process of input and review source documents for evidence of authorization.

OR

Completeness check

Fields like national identity card number accepts data of standard length. If incomplete card number is entered, an alert is generated to complete the entry. At record level, when we want to move on next record without entering mandatory fields' value, an alert will be generated to complete the record entries.

Effectiveness testing

(i) Observing the data entry process.
(ii) Input some records on test basis and intentionally skipping mandatory fields blank while adding new records.

OR

Authorization on source document

Authorized person's signature in an appropriate area of the source document provides evidence of proper authorization.

Effectiveness testing

Review some source documents corresponding to records present in the system and verify the authorized signatures.

Processing Controls

Exception reports

Such reports are generated when some transaction or data appear to be incorrect.

Effectiveness testing

Review exception reports and check if these were reviewed by the concerned user and the evidence of actions taken thereof.

OR

Reconciliation of control totals

It involves checking of totals produced by the computer with those determined manually.

Effectiveness testing

(i) Assessing whether the reconciliations are being prepared as appropriate.
(ii) Checking calculations as appearing on the reconciliations.

OR

File Version Check

For correct processing, the system ensures that transaction should be applied to the most current database.

Effectiveness testing

Process some sample transactions and compare the results with current version of the database.

Output Controls

Printing and storage of output reports

Critical output reports should be produced and maintained in a secure area in an authorized manner.

Effectiveness testing

(i) Review of the access rules
(ii) Reviewing and assessing the procedures adopted by the management for monitoring the output.
(iii) Reconciliation of total pages printed with the readings as shown on the counter installed in the printer.

OR

Distribution of reports

Authorized distribution parameters are set for output reports. All reports are logged prior to distribution. Recipient is required to sign the distribution log as evidence of receipt of output.

Effectiveness testing

(i) Observation and review of distribution output logs.
(ii) Verifying recipients'' signatures on distribution log.

General Controls

Segregation of duties

Segregation of duties means that important responsibilities are distributed between two or more individuals which result in creating checks and balances as work of one person is checked by the other. If a single person is responsible for many activities it becomes easy for him to commit fraud or for errors to remain undetected.

Effectiveness testing

(i) Observation and review of job description.
(ii) Review of authorization levels and procedures.

Error control and correction reports

They provide evidence of appropriate review, research, timely correction and resubmission.

Effectiveness testing

(i) Assessing and testing whether appropriate reports are being generated.
(ii) Checking the consequent corrections and their authorizations.

OR

Access to authorized personnel only

Access to information/data should be based upon job descriptions.

Effectiveness testing

(i) Review of access rules to ensure that these are appropriately based on the requirements.
(ii) Testing the compliance to access rules.

Backup and Recovery
Automatic back up of enables to recover from any unforeseen breakdown and mitigates the effects of data corruption.
Effectiveness testing
Observe the auto backup procedure.
Attempt to restore the system from recent backup at an alternative location.

Answer 6: (1+9=10)

In Passive Attack, Intruder attempts to learn some characteristics of the data being transmitted. They might be able to read the contents of the data so the privacy and confidentiality of data is violated. Alternatively, although the content of the data itself might remain secure, intruders could read and analyze the clear-text source and destination identifiers attached to a message for routing purposes. They also could examine the lengths and frequency of messages that are transmitted.

In Active Attack, Intruder attempts to insert a message, modify the contents or order of the message, deny a message, delete a message or use techniques to establish spurious associations.

Type of Attack	**Active/ Passive**	**Suggested Control**
Release of Message Contents	**Passive**	Link Encryption End-to-end encryption
Traffic Analysis	**Passive**	Link Encryption
Message Insertion	**Active**	Message Sequence Number
Message deletion	**Active**	Message Sequence Number
Message Modification	**Active**	Message Authentication Code
Changed Message order	**Active**	Message Sequence Number
Message Duplication	**Active**	Message Sequence Number Unique Session Identifier
Denial of message Service	**Active**	Request Response Mechanism
Spurious Association	**Active**	Secure Authentication

Answer 7:

Students are supposed to give 2 KPI for each area. Here is a suggested list of KPIs for each area.

(i) IT Strategic Planning:
- Reach: no of various platforms available over no of platforms covered e.g. in hand held devices android, black-berry, and i-phone etc.
- Return on Investment
- Time to Market : speed of delivering IT projects
- IT Maturity level
- IT R&D Spending: IT's share in developing new products
- Percentage of IT investments of total investment of company

(ii) Management of IT Investment
- No of Projects On-Time
- No of Projects within budget
- Ratio of "IT control & management cost" to "Average Cost of prevented IT incidents"
- Percentage of costs associated to IT maintenance (instead of IT investment in new initiatives) relative to all IT costs within the measurement period.
- Percentage of IT investments of total investment of company

- Ratio of % growth of IT budget versus % growth of revenues: Measures the ratio of IT growth to business growth. When IT growth is less than business growth it can indicate economies of scale, improved efficiencies or underinvestment

(iii) Communication of management aims and directions

- Ratio of total number of New IT Initiatives versus % total number of business initiatives: the measure shows the strategic business alignment of IT projects with business level strategy.
- Employee Satisfaction Index: when employees have clear goals their level of satisfaction with the company increases.

(iv) Human resource management of IT personnel

- Employee Satisfaction Index: When there is stress there is staff turnover, loss of institutional knowledge and resulting drop in productivity and quality.
- Percentage of staff trained in critical risk management techniques

(v) Procurement of IT resources

- % of business suppliers linked to your IT
- Average age of hardware assets.
- Average Age of Facilities
- Percentage of costs associated to IT maintenance (instead of IT investment in new initiatives) relative to all IT costs within the measurement period.

(vi) Change management of IT operations and processes

- Percentage of outage (unavailability) due to implementation of planned changes, relative to the service hours.
- Percentage of unplanned outage (unavailability) due to the implementation of changes into the infrastructure. Unplanned means that the outage (or part of the outage) was not planned before implementation of the change.
- Percentage of backlogged change requests. Backlogged change requests are change requests that should have been implemented but due to for example time/cost constraints are still outstanding.
- Number of unauthorized implemented changes relative to all implemented changes within a given time period.
- Percentage of costs associated to IT maintenance (instead of IT investment in new initiatives) relative to all IT costs within the measurement period.
- Average age of hardware assets.

Answer 8

1. Eradication of communication gap between government and inhabitants by availability of convenient mode of communication with the government.
2. Better Recoveries due to ease of payments.
3. Cost savings in processing charges.
4. Increased documentation of economy.
5. Better Taxpayers to population ratio.
6. Provision of related (tax and Legal) information to citizens centrally.
7. Electronic interaction will result in time savings both for Government and Citizens.

Information Technology Management, Audit & Control (S-15)
(Suggested Answers)

Part B

1. Changes in working methods may trigger active or passive resistance
2. Inter-operability and compatibility issue among various government departments
3. Lack of user authentication e.g. Computerized national identity card is the basic requirement for the success of any other system
4. Data Privacy and confidentiality Challenges
5. Information Security risks
6. Availability of IT infrastructure in remote areas

(The End)