Auditing infrastructure and operations

Key success factors for an effective Information Technology Risk Management Program are as follows:
(i) Leadership direction and management support.
(ii) Management accountability and authority to effect change.
(iii) Close alignment with the corporate culture.
(iv) Consistent and standardized risk management processes supported by tools and technology.
(v) Measurable results.
(vi) Periodic review and updation of Information Technology Risk Management Program.

(b) The **responsibilities of the information technology risk management function** include:
(i) Establishing the risk framework for information technology management.
(ii) Educating all concerned persons about information technology policies, guidelines and regulatory requirements.
(iii) Information technology risk reporting.
(iv) Appropriate use of monitoring tools and technologies.
(v) Interfacing with regulators/auditors.
(vi) Independent review of risk governance and management processes.

Case study: As the use of mobile devices like smart phones and tablets is gaining popularity, many organisations allow their staff to connect their personal mobile devices to the company's network by directly connecting to its LAN or through Internet.
Required:
(a) Identify the primary security and control issues to which an organisation may be exposed to in the above stated situation. (02)

(a) If employees access their company's network through their personal mobile devices then the company may be exposed to following primary security and control issues:
(i) Protection of sensitive data and intellectual property.
(ii) Malware protection.

(b) List the steps that an organisation may need to take in order to address the risks that may arise in the above stated situation, with regard to:
(i) Network access
(ii) Device management
(iii) Application security management (09)

(b) **Network access**
(i) Protect the network with a properly configured firewall.
(ii) Determine which devices are allowed on the network.
(iii) Keep list of authorized users updated.
(iv) Data flowing between personal mobile devices and the organization's server should be encrypted.

Device management
(i) Keep updated inventory of authorized devices.
(ii) Create mandatory and acceptable endpoint security components (e.g., updated and functional antivirus software, updated security patch, level of browser security settings) to be present on these devices.
(iii) Confidential or sensitive data stored on personal mobile devices should be encrypted in accordance with the organization's IS policies.
(iv) Take appropriate steps to ensure the availability / recovery of data in case of loss of device.

Application security management
(i) Determine which operating systems and versions are allowed on the network.

(ii) Determine which applications are mandatory (or prohibited) for each device.
(iii) Access to application may be on a need-to know basis.

Following **information** should be maintained by the **helpdesk** for each complaint:
(i) Complaint Number
(ii) Error date
(iii) Error code / description
(iv) Source of error
(v) Escalation date and time
(vi) Initials of the individual responsible for maintaining the log
(vii) Initials of the individual responsible for closing the log entry
(viii) Department / center responsible for error resolution
(ix) Status code of problem resolution (i.e. problem open, problem close, pending etc.)
(x) Error resolution description

(b) Following **responsibilities** could be assigned to the **helpdesk staff**:
(i) Answering enquiries regarding specific systems.
(ii) Filtering complaints and forwarding them either to the IT department or to the vendor.
(iii) Maintaining documentation of vendor software including issuance of new releases and problem fixes, as well as documentation of systems developed in house and utilities.
(iv) Follow up the vendor, IT department or the concerned department for resolution of the issue.
(v) In case of problems that remain unresolved for a defined period of time, escalating such problems to the next level of support.

NOTE FOR THE MANAGEMENT
I have carried out the IS Audit of your company. During the audit, I have identified few licensing violations. In order **to minimize software licensing violations**, following suggested **controls** may be implemented:
(i) Centralizing control and automated distribution and installation of software.
(ii) Requiring that all PCs be diskless workstations and access applications from a secure LAN.
(iii) Installing metering software on the LAN and requiring all PC's to access application through the metered software
(iv) Make a licensing agreement with vendors which is based on the number of users who access the network rather than a license agreement being attached to a specific user or machine.
(v) Put in place properly documented policies and procedures to guard against unauthorized use or copying of software.
(vi) Keep an updated list of all types of software in use or in inventory.
(vii) Regularly scanning user PCs, either from the LAN or directly, to ensure that unauthorized copies of software have not been loaded on the PC.

Yours sincerely,
— Sd —
IS Auditor

<u>Case study:</u> Manifold Corporation Limited (MCL) provides services of various nature including data entry, data archiving, bulk printing, customised software development and web hosting. Recently there has been an increase in the number of complaints regarding slow response, lost data, long call handling times and even breach of some service level agreements during evening hours. The Customer Services Director believes that over a period of time, the systems deployed at MCL have been over burdened and need significant upgrading. Consequently, the management intends to carry out a capacity management audit before reaching a final decision.
Required:
Briefly describe:
 the concept of capacity management and when it is undertaken.
 how could a capacity management audit be useful for MCL at this stage?
 the type of information you would like to gather while carrying out the capacity management audit. (10 marks)

 Concept of Capacity Management and when it is undertaken:
It is the planning and monitoring of the computer resources to ensure that sufficient resources are available and are being used efficiently and effectively.
Initially, this process is undertaken at the design stage as part of companies' strategic planning. However, it is a continuous process and should be carried out at regular intervals.

 Since Customer Services Director suggests upgrading the systems, capacity management audit would help to evaluate his suggestion and would give justification for accepting or rejecting the same.

 Following type of **information** is useful to gather while conducting a capacity management audit:
(i) Specification of existing resources
(ii) Current and projected CPU utilization, computer storage utilization, telecommunication and wide area bandwidth utilization
(iii) Information related to response time and processing time
(iv) Average number of users connected during peak and off peak hours
(v) Incident management reports regarding IT infrastructure. More incidents may indicate low capacity systems which might not be meeting the demand.
(vi) Analysis of complaint call log / system log, audit trails etc, according to:
 Types of complaints: an exceptionally high proportion of similar types of complaints may indicate a capacity management issue.
 Timing: a high number of complaints during a specific time may also indicate the issue.
 By customers: an exceptionally high number of complaints from a particular customer or a certain type of customers may be indication of problems of specific nature.
(vii) Report of any such review conducted in past.

Case study: The IT Manager of Correct Cure Limited (CCL) has proposed significant upgrading of the IT hardware in the budget for the forthcoming year. He believes that since most of the IT equipment are more than five years old, they should now be replaced otherwise, CCL may start facing frequent hardware related problems.
Required:
(a) Discuss whether the IT Manager's argument is appropriate for upgrading the hardware or should CCL undertake a capacity management review before acceding to his request. (04)

(a) Replacing hardware merely on the ground that it has been certain number of years old is not appropriate. Replacement of hardware should be on need and usage basis. Capacity management review would determine if sufficient resources are available and are being used efficiently and effectively. Result of this review may help to evaluate IT Manager's suggestion and provide justification for accepting or rejecting the same.

Case Study: The management of Elaaj Hospital (EH) has approached you to conduct a review of their lights out operation (tasks which can take place without human intervention) of IT systems. You have been informed that:
• EH offers round the clock inpatient services and the management ensures the availability of doctors and medical support staff.
• Patients' medical and billing record is maintained on a centralized information system.
• IT support staff is available during office hours only. However, in case of any problem they can be contacted on phone.
• Any problem encountered by the system during lights out operation, or otherwise, is recorded in an Error Reporting System (ERS) by the duty staff.
• All computers and critical electronic systems are supported by UPS and a generator is also available which is equipped with an automatic change over switch.
Required:
List the matters (any ten points) that you would consider while reviewing the lights out operation of EH's IT systems. (10)

I would consider the following ***matters*** while ***reviewing the lights out operations*** of EH's IT systems:
(i) Whether remote access to the master console is granted to IT support personnel for contingency purposes?
(ii) Does sufficient security exist to ensure that the above access is used for authorized purpose only?
(iii) Do contingency plans allow for the proper identification of the disaster in the unattended facility?
(iv) Are the automated operation software and manual contingency procedures documented and tested adequately?
(v) Are tests of the software system performed on a periodic basis, especially after changes or updates?
(vi) Do assurances exist that errors are not hidden by the software i.e., all errors are reported automatically to the support staff?
(vii) Have documented procedures been developed to guide the duty staff in logging and reporting problems in a timely and appropriate manner?
(viii) Whether contact numbers of related IT staff are available to the duty staff during lights out operation? If those numbers are updated?
(ix) Were all lights out operation problems recorded in the ERS reviewed by IT staff and resolved in a timely manner?
(x) Does the ERS log identify significant and recurring problems? If yes, what action has been taken to prevent their recurrence?
(xi) Whether periodic maintenance and testing of UPS and generator is being carried out?

Key objectives of the help desk function are as follows:
• Effective and efficient customer support.
• Effective and timely monitoring.
• Building Knowledgebase

Actions required to achieve the above objectives are explained below:
Effective and efficient customer support
(i) Appoint trustworthy and competent personnel having high level of interpersonal skills as the help desk coordinating officers.
(ii) Train the help desk officers in the diverse range of systems used throughout the organisation.
(iii) Ensure immediate logging of all customers' complaints/queries.
(vi) Unresolved customers' queries should be assigned to support personnel for investigation and resolution.
(vii) Arrange periodic reviews/audits of the services offered and gather customers' opinion through feedback forms and surveys.
Effective and timely monitoring
(i) Assign a time limit for resolution of each reported complaint.
(ii) The system should be able to alert the Customers Services Manager, as soon as the designated time period for unresolved complaints is over.
Building Knowledgebase
(i) Maintain system generated log of all activities undertaken to resolve the reported complaints.
(ii) Use the help desk log to determine the most and least problem areas.
(iii) Train help desk staff to make use of the log to find out how a particular type of problem has been fixed in the past.

Case study: You are working as Manager IT Audit in YEP Consultants. Trade Power (TP), which is a midsized retailing and distribution company, has approached your firm for post-implementation review of its
recently established Virtual Private Network.
Required:
List the steps that you would undertake:
(a) while planning the high level risk assessment of TP's Virtual Private Network; and
(b) in determining the scope and objectives of the above assignment. (06 marks)

(a) I would take the following steps while planning the high-level risk assessment of TP's VPN:
(i) Gather information regarding TP's business and the purpose of installation of VPN.
(ii) Identify the VPN related risks relevant to post implementation stage.

(iii) Identify the relevant framework information criteria that need to be reviewed and confirmed.

(b) To determine the scope and objective for the TP's assignment, I would:
(i) Consult with the management of Trade Power (TP) where appropriate.
(ii) Obtain feasibility study report of the project to gain understanding of users' requirements.
(iii) Consider the information gathered at the planning stage, to determine the scope in a more explicit manner.
(iv) Interview the identified stakeholders and include their key concerns, if any, in the scope and objectives of the review.

Case study: During a recent meeting, the management of Mahir Chemicals Limited (MCL) had noted with serious concern that the knowledge base available with the company is not being used efficiently. Quite frequently, valuable resources are wasted on generating information which is already available with other departments/location. To cope with the situation, a senior executive had suggested creation and maintenance of Knowledge Management System (KMS).
Required:
As the Head of IT, the Management has asked you to explain:
(a) Knowledge Management Systems and their functions. (03)
(b) The advantages of Knowledge Management Systems. (03)
(c) Give three examples of systems that can facilitate:
□ Knowledge distribution
□ Knowledge sharing (03)

(a) Knowledge Management System (KMS) refers to a system for managing knowledge in organizations supporting creation, capture, storage and dissemination of information.

The idea of a KMS is to enable employees to have ready access to the organization's documented facts, sources of information and solutions. Databases are set up containing all the major work done in an organization. An application is then developed allowing the users to access information from the database as needed.

(b) Some of the **advantages** claimed for KMS are:
(i) Valuable organizational information can be shared.
(ii) Can avoid re-inventing the wheel, reducing redundant work. / Time saving.
(iii) May reduce efforts on training of new employees.
(iv) Intellectual information can be retained even after the employee leaves.
(v) Development of important knowledge that can be used to create successful business models
(vi) Benefit of creating a knowledge base which is already tried and tested and can be sold worldwide to franchisees, leading to global operations.

(c) **Facility**	**System**
Knowledge distribution	Word processing, electronic schedulers, desktop databases, email etc.
Knowledge sharing	Intranet, extranet, groupware etc

Q.3 (a) Automated Teller Machines (ATMs) have tremendous utility for banking customers. However, the concerned bank needs to carry out constant review and monitoring of the controls installed as a safeguard against fraudulent activities.
Required:
Identify five major tasks that should be performed during information systems audit of ATM and its overall mechanism. (05)
(b) An effective and efficient management of software inventory is generally carried out with the help of an automated mechanism known as Software Library Management System.
Required:
Identify any five key capabilities of a Software Library Management System that helps in overall management of software inventory. (05)

A.3 (a) (i) Review measures to establish proper customer identification and maintenance of their confidentiality.
(ii) Review file maintenance and retention system.
(iii) Review exception reports.
(iv) Review daily reconciliation of ATM transactions.
(v) Review PIN (key) change management procedures.
(vi) Review the procedures for retained, stolen or lost cards.
(vii) Review the effectiveness of physical controls.

3 (b) (i) Assignment of modification number and version number for each item in software inventory.
(ii) Security over the access to software. OR Limiting the access to software to authorized persons only.
(iii) Provision of facilities like encryption and automatic backup.
(iv) Creating, updating and deleting the profiles of users for access to software inventory.
(v) Maintaining audit trail for access to any item of software inventory.
(vi) Interface with operating system, job scheduling system, access control system and online program management for provision of various features to users.
(vii) Maintaining list of additions, deletions and modifications in overall library catalog.

Q. Right Bank Limited is a leading bank in the country. A large proportion of its business activities involve e-banking. As a member of the IS audit team, you have been assigned to assess effectiveness of the bank's policies as regards audit trails.
Required:
(a) List six key steps involved in carrying out the above assessment. (06)
(b) Identify any three non-financial e-banking transactions, for which maintaining an audit trail is important. (03)

(a) Key steps involved in carrying out the assessment of the bank's policies as regards audit trails include:
(i) Review and assess whether the company's policy regarding maintenance of audit trail is comprehensive and well defined.
(ii) Review the security access control list and assess whether authority levels for managing audit trails are appropriate and well defined.
(iii) Obtain and review the risk assessment document of audit trails.
(iv) Test an appropriate sample of transactions to ensure availability of audit trails according to the defined policies and controls.
(v) Test an appropriate sample of transactions to check whether audit trails of critical transactions are periodically reviewed and assessed.
(vi) Test an appropriate sample of transactions to check whether problems and issues identified by the reviewer of audit trails are adequately addressed.

(b) The maintenance of audit trail may be important for the following non-financial e-banking transactions:
(i) The opening, modification or closing of a customer's account.
(ii) Any granting, modification or revocations of systems access rights or privileges.
(iii) Authorization of changes in credit limits etc.
(iv) Change in password.
(v) Change in personal information (including secret question).