Control, Audit and Security of Information System

Audit of Information System

- Information audit is the element of information management that is responsible to ensure that the information within an organization is managed and well organized.
- Information audit is the process to discover, monitor, analyze and evaluate the information flow within an organization so as to implement, maintain and improve the organizational information management.

Benefits of Information Audit:

- It examines the information against the criteria under the identified purpose of the audit to meet the standard compliance.
- It determines the user information needs.
- It lists the information resources available within an organization.
- It identifies the costs and benefits of the information resources available.
- It provides information about the working structure of the information system of an organization.
- It produces report that recommends for the information handling problems.
- It helps organization to make use of information for strategic planning and implementations.
- It aids in decision making and support.
- It enables organization to be dynamic i.e. adapt to necessary changes.
- Information audit helps to identify problems like data redundancy, duplication, inconsistency and cost to store and utilize data and information.
- Information audit helps to identify hidden assets of an organization, skills and expertise of staffs, market for further expansion and so on that would expand organizational opportunities.

Methodological Approach to Information Audit

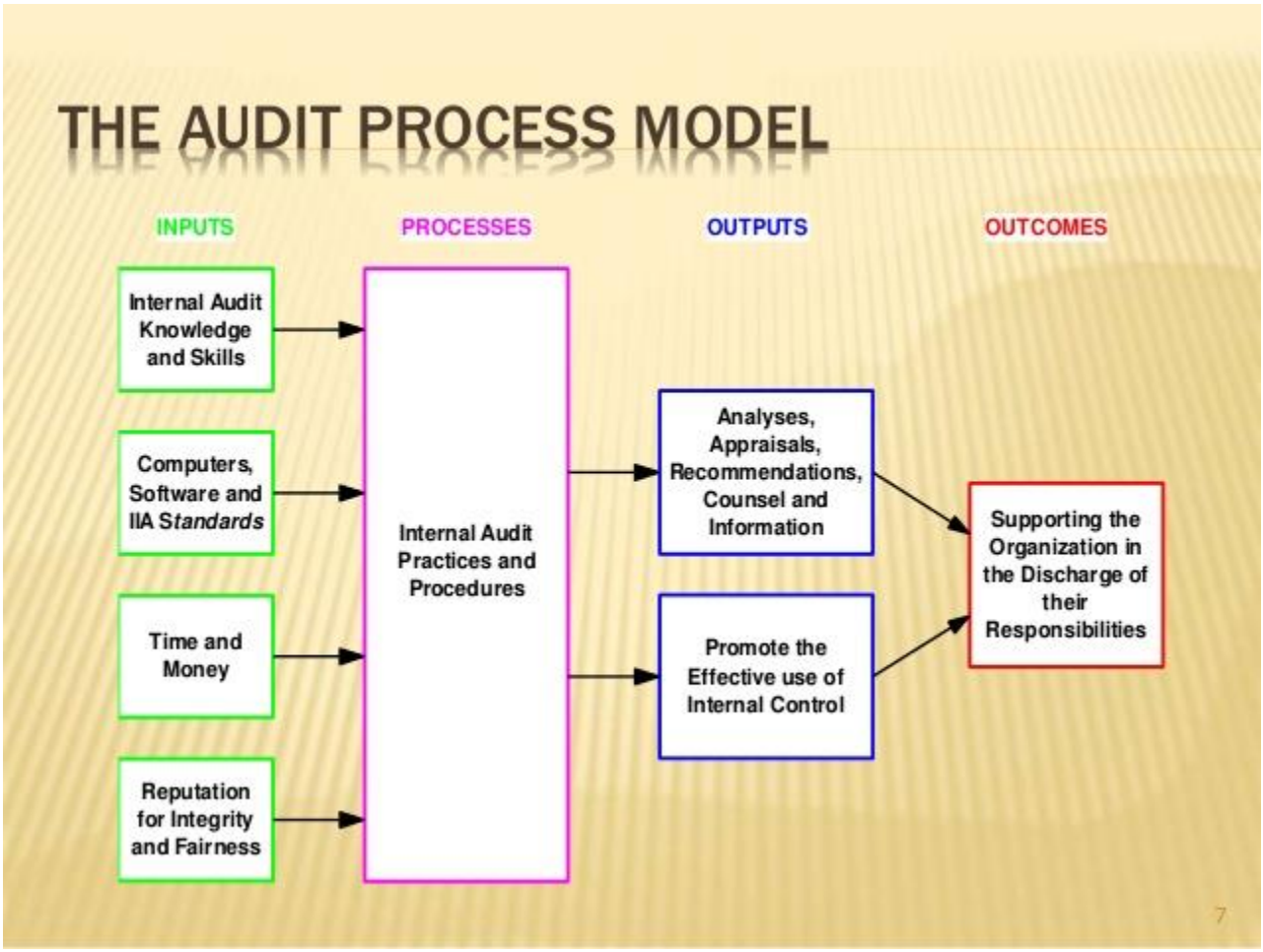
1. Cost Benefit Method:
- It lists information system options and compares them on the basis of their cost and perceived benefits.

2. Geographical Approach:
- It identifies the components of information system and maps them in relation to one another to identify and meet system needs.

3. Hybrid Approach:
- It takes both geographical approach and cost benefit method into consideration.
- It emphasizes on the control and management procedures for organizational strategy.

4. Management Information Audit:
- It focuses on reports related to the management information.

5. Operational Information Audit:
- It focuses on the efficiency and effectiveness with which information resources are used and accounted for.
- It measures reliability of information system and compliance with obligations, regulations and standards.



Problems in Information Audit

- Support of senior management is very crucial for information audit and in most cases such support is not provided.
- It is difficult to decide whether to use internal auditors or external consultants.
- It is very tedious task to collect and gather necessary information for auditing.
- The information audit time span depends up on the size of an organization.
- It is difficult to establish costs and value of information

---

Security of Information System

Threats to Information System:

- Information system is subjected to threats because it is easy and safe to get information which can benefit for the hackers.
- It is very easy to get information from the system if the system is not properly secured.
- Such attacks are less prone to tracing as there is no necessity of physical presence.

- The various threats to information system are as follows:
1. Phising
2. DDOS Attack
3. Spyware
4. Key Logging
5. Man-in-the middle attack
6. SQL Injection
7. Session Hijacking
8. Payload
9. Identity Theft

Layered Security Strategy

Layered Security

- Layered security is the practice of combining multiple mitigating security controls to protect the resources and data.
- It assures that the information possessed by an organization is not compromised with the attackers.
Multiple levels of security is provided to make the information system secure from various cyber threats.

Consumer Layered Security Strategy:

1. Extended Validation SSL Certificate
2. Two factor Authentication
3. Single sign-on

4. Fraud detection
5. Secure web

Enterprise Layered Security Strategy:

1. Workstation application whitelisting
2. Workstation system restore solution
3. Workstation and network authentication
4. File, disk and removable media encryption
5. Remote access authentication
6. Network folder encryption
7. Secured end-to-end messaging
8. Content control and policy based encryption

Extended Validation and SSL Certificate

SSL

- SSL stands for Secured Socket Layer.
- It provides a secure transport connection between web server and client.
- It enhances security of data transfer by developing a dedicated communication path between server and client through which encrypted data are communicated between client and server.
- Generally, SSL is used to transfer sensitive data which when compromised can lead to disastrous results.
- Such data includes log in details, credit card details, payment details and so on.
- The communication path itself is encrypted such that no one can listen to that path expect for the client and server certified by the SSL certificate.
- The website secured using SSL certificate gets https instead of http.
- The SSL certificate consists of server name, its public key, IP number, and an expiration date.
- The certificate is signed with a 1024 bit key by the certificate

authority.
- All traffic within the SSL communication is encrypted.

Working of SSL:

- The browser attempts to connect to a web server secured with SSL by requesting for the web server's identity.
- The web server then sends the browser a copy of its SSL certificates.
- The browser checks whether or not it can trusts the SSL certificate. If so, it sends a message to the web server.
- The web server then sends back a digitally signed acknowledgement to start an SSL encrypted session.
- The encrypted data is then shared between the browser and the web server via a dedicated and encrypted communication channel.

Extended Validation:

- Extended validation is a certificate used for HTTPS websites and software that proves the legal entity controlling the websites or software package.
- To obtain EV certificate, verification of the requesting entity's identity is required by a certificate authority.
- It increases the security due to the identity validation process, which is indicated within the certificate by the policy identifier.

Remote Access Authentication

- Remote access authentication is the process by which a certified computer user can securely have network access and privileges even if the network is geographically separated.
- It makes use of the digital certificate that contains information to identify the user to the server and provides the credentials.
- The remote connection should be established to the network by the

user as the network and the user computer are not physically connected to each other. Such remote connected is initiated by dial up connection or connection through Internet or connection through wireless medium.
- Once the credentials within the digital certificate is verified by the server, the server provides access to the remote computer to access its resources and services.

Steps to obtain remote access authentication:

1. Temporary network connection:
- To initiate remote access to the server, the user computer must establish a temporary network connection to the server.
- It may be through dial up, Internet or wireless connection.
- The network connection is established securely using encryption for remote access protocols.
- Proper encryption of communication channel is established to prevent from hijacking of authorized sessions and authorized user's credentials.

2. Establishing proper privileges:
- Once the network connection is successful, proper privileges to the requesting user should be established.
- For this, three steps are performed namely authentication, authorization and accounting.
- The server provides user identification to its user, computer or network device to enable remote access.
- Authentication is the process by which the server checks whether the user which requests for the remote access is eligible for the purpose or not by matching the user supplied identification credentials to the stored credentials.
- Authentication is generally accomplished via username and password system. Other methods include tokens, static biometrics like fingerprints and dynamic biometrics like voice matching.
- Authorization is the process of determining the permissions that are granted to the authenticated users. It determines whether an

authenticated user has permission to use a particular resource of the server or not.

Telnet:

- Telnet is the TCP/IP protocol standard that allows users to log on remotely and access resources as if the user had a local terminal connection to the server.
- The major threat of using Telnet is that it uses TCP/IP connection for information flow that has less security.
- The Telnet uses TCP port 23 for connection.

Secure Shell (SSH)

- SSH is a remote access system that provides a secure transport between machines using an SSH daemon at each end for secure login and secure file transfer.
- SSH provides higher level of security as it supports different encryption protocols, cryptographic host authentication and integrity protection.
- The authentication services are host based.

Content Control / Content Filtering

- Content filtering is the process of controlling what content is permitted to the user.
- It is generally used to restrict material delivered over the Internet via Web, email or other means.
- It determines what content to make available or what content to block.

Implementation of content filtering

The content filtering can be implemented in various ways as follows:

1. Browser based filter:
- It is implemented by using the third party browser extension.
- On implementing such filters, the browser blocks the restricted content to be displayed to the users.

2. E-mail filter:
- It is used to filter the information contained in the mail body or in the mail header.
- The e-mail header or body or attachments are classified into accepted or rejected using the predefined rules or through artificial intelligence.
- Only the accepted mails are shown to the users.
- In most cases, the rejected messages are sent to the spam for manual review from the users.

3. Client side filter:
- It is generally installed on each client computer to allow content filtering.
- Such filter can be managed, disabled or uninstalled by the user having administrative privileges on the system.

4. Content-limited ISP:
- It includes the ISP that offer access to only a portion of Internet content.
- Any users who pursue services from such ISP are subjected to restrictions.

5. Network based filtering:
- It is implemented at transport layer (transport proxy) or application layer (web proxy).
- It filters outbound as well as inbound information within a certain network.
- All the clients of such network should accept the protocols and are subjected to restrictions.

6. Search engine filters:
- Search engine itself provides the facility for safety filter.
- When safety filter is activated, the inappropriate links that appears in the search lists are filtered out.

Policy Based Encryption

- Policy based encryption is the service that allows customers to set up filters based on the content of the messages.
- The customers are able to set criteria for acceptance of the messages.
- The messages get encrypted only if they meet the defined criteria.
- All the messages to external recipients are first routed to the special gateway.
- The gateway checks the compliance of all the messages to policy settings.
- Based on the defined conditions or policies, the messages are encrypted, send to the receiver, discarded or returned to the sender.

Security in e-commerce transaction

1. Network security
2. Proper identification
3. Encryption
4. Authorization
5. Host and application security
6. Transaction security
7. Human error and malice
8. Communication security