Information Systems Security Audit

13

This Module includes:

Information Systems Security Audit

SLOB Mapped against the Module

To develop adequate knowledge on information system, its security framework to evaluate whether information systems are safeguarding corporate assets, and maintaining the integrity of stored and communicated data. (CMLO 3c)

Module Learning Objectives:

An IT security audit is a comprehensive examination and assessment of an enterprise's information security system. Conducting regular audits can help identify weak spots and vulnerabilities in IT infrastructure, verify security controls, ensure regulatory compliance, and more. After studying this module, the students will be able to –

- Identify the need for IS Audit in the Business Organisations
- Learn the various compliance and security frameworks of the organisation in an IT Environment
- Differentiate between Cyber Security and Cyber Forensics

Introduction

13

The advancement of information systems and technology offers a vital benefit for businesses. However, it also brings ever-increasing challenges due to the existence of hackers, malware, viruses, cyber crimes, etc. Therefore, frequent and strong follow-up is required via regular information systems security audits.

An information systems security audit (ISSA) is an independent review and examination of system records, activities, and related documents. These audits are intended to improve the level of information security, avoid improper information security designs, and optimize the efficiency of the security safeguards and security processes. The term "security framework" has been used in a variety of ways in security literature over the years, but in 2006, it came to be used as an aggregate term for the various documents, some pieces of software, and the variety of sources that advise on topics related to information systems security, in particular, about the planning, managing or auditing of overall information security practices for a given institution.

Although security is a never-ending process that requires continued follow-up, it is still in its infancy. Also, a security audit is an unexplored area and requires a simple framework to guide the process.

Overview

13.1

An IT security audit is a comprehensive examination and assessment of an enterprise's information security system. Conducting regular audits can help identify weak spots and vulnerabilities in IT infrastructure, verify security controls, ensure regulatory compliance, and more.

IT security audits involve how they can help the organisation achieve its security and compliance goals.

First and foremost, a comprehensive IT security audit enables to verification of the security status of the company's infrastructure: hardware, software, services, networks, and data centers.

An audit can help to answer the following critical questions:

Are there any weak spots and vulnerabilities in current security?

Are there any extraneous tools or processes that don't perform a useful security function?

Are equipped to fend off security threats and recover business capabilities in the event of a system outage or data breach?

If discovered security flaws, what concrete actions can take to address them?

A thorough audit can also help remain in compliance with data security laws. Many national and international regulations, require an IT security audit to ensure that information systems meet their standards for the collection, usage, retention, and destruction of sensitive or personal data.

A Compliance Audit is typically conducted by a certified security auditor from either the applicable regulatory agency or an independent third-party vendor. In some cases, though, personnel within the company may perform an internal audit to check the company's regulatory compliance or overall security posture.

If an organisation performing an audit for either general cyber security or regulatory compliance purposes, follow these steps and best practices to ensure an efficient, effective process.

The Steps in an IT Security Audit

A cyber security audit consists of five steps:

- Define the objectives.
- Plan the audit.
- Perform the auditing work.
- Report the results.
- Take necessary action for the deficiencies.

Define the Objectives:

Layout the goals that the auditing team aims to achieve by conducting the IT security audit. Make sure to clarify the business value of each objective so that specific goals of the audit align with the larger goals of the company.

List of questions as a starting point for brainstorming and refining of objectives for the audit.

- Which systems and services do want to test and evaluate?
- Do audit digital IT infrastructure, physical equipment, and facilities, or both?
- Is disaster recovery on the list of concerns? What specific risks are involved?
- Does the audit need to be geared towards proving compliance with a particular regulation?

Plan the Audit:

A thoughtful and well-organized plan is crucial to success in an IT security audit.

Define the roles and responsibilities of the management team and the IT system administrators assigned to perform the auditing tasks, as well as the schedule and methodology for the process. Identify, monitor, report, and data classification tools that the team will use and any logistical issues they may face, like taking equipment offline for evaluation.

Once decided on all the details, document and circulate the plan to ensure that all staff members have a common understanding of the process before the audit begins.

Perform the Auditing Work:

The auditing team should conduct the audit according to the plan and methodologies agreed upon during the planning phase. This will typically include running scans on IT resources like file-sharing services, database servers, and SaaS applications like Office 365 to assess network security, data access levels, user access rights, and other system configurations. Also physically inspect the data center for resilience to fires, floods, and power surges as part of a disaster recovery evaluation.

During this process, interview employees outside the IT team to assess their knowledge of security concerns and adherence to company security policy, so any holes in the company's security procedures can be addressed moving forward.

Report the Results:

Compile audit-related documentation into a formal report that can be given to management stakeholders or the regulatory agency. The report should include a list of any security risks and vulnerabilities detected in IT systems, as well as actions that IT staff recommend to mitigate them.

Take Necessary Action:

Follow through with the recommendations outlined in the audit report. Examples of security-enhancement actions can include:

- Performing remediation procedures to fix a specific security flaw or weak spot/s.
- Training employees in data security compliance and security awareness.
- Adopting additional best practices for handling sensitive data and recognizing signs of malware and phishing attacks.
- Acquiring new technologies to strengthen existing systems and regularly monitor infrastructure for security risk.

Difference Between a Security Audit and a Risk Assessment

A security audit and a risk assessment each involve a process of examining and evaluating security risks for an organisation. The differences between them have to do with their timing and scope.

A risk assessment is often performed at the start of an IT initiative before tools and technologies have been deployed. It's also performed every time the internal or external threat landscape changes-for example when there is a sudden rise of ransomware attacks or a massive shift to remote working. In organisations with mature security processes, risk assessment is performed regularly to assess new risks and re-evaluate risks that were previously identified. The goal of a risk assessment is to determine how best to build IT infrastructure to address known security risks. Hence, this activity is focused on outward factors and how they affect infrastructure.

A security audit, on the other hand, is performed on an existing IT infrastructure to test and evaluate the security of current systems and operations. As a best practice, schedule security audits to be performed at regular intervals so that overall security posture is on an ongoing basis.

To make sure that security audit is effective in identifying flaws and weaknesses in the IT system, follow these best practices.

Establish Clear Objectives

Clearly defining goals and scope keeps the audit on track to be measurable, actionable, and successful. And when all members of the auditing team stick to the defined objectives, they can stay focused on critical tasks and avoid wasting valuable time and resources on irrelevant or unnecessary issues.

Obtain Buy-in from Key Stakeholders

For an infrastructural initiative like a security audit to be successful, there is a need for support and advocacy from the top levels of the organisation, including the chief security officer and chief information officer. Management sponsorship will help ensure that the audit gets the time and resources that are required.

Define Clear Action Items Based on the Audit Results

It's not enough just to publish a report of findings. The audit should contribute to the security of the organisation by providing clear and practical guidelines for making cybersecurity improvements. If there's a system vulnerability, create a plan for how to remediate it. If a file or data system is out of regulatory compliance, take the necessary measures to bring it into compliance.

Security Audit Solutions

IT security auditing is most useful and effective when conducted regularly. Create a schedule to periodically audit the entire system portfolio to assess compliance with data regulations and maintain operational readiness for cyber attacks.

Compliance and Security Framework

13.2

Since the entire banking heavily relies on electronic platforms and online transactions, cyber security is imperative. Hence, RBI expects banks to assess their Cyber Security preparedness. RBI mandates that a Top to Down approach in information security governance must be followed which starts from the Bank's operating board to IT and IS committee, and to level further down in the hierarchy. RBI also expects the Banks to report to the Cyber Security and Information Technology Examination (CSITE) Cell of the Department of Banking Supervision, with the following details.

- Gap analysis against the published Cyber Security / Resilience Framework.
- Information security controls.
- Effectiveness of the implemented controls.
- Plan of action to mitigate risks.
- Role of Chief Information Security Officer (CISO).

How RBI Audit is performed for a bank?

- The audit is conducted as an in-depth technical assessment.
- Includes information security process audit.
- Includes applicability of cyber security controls.
- By checking evidence and logs on servers.
- Includes checking all norms of technical requirements as per RBI.

RBI Audit Report

- A detailed gap analysis report.
- The report will provide who needs to do what activities to be compliant with RBI.
- Wherever possible, the report will include details on what exactly needs to be done and by which team or person.

RBI Cyber Security Framework Domains

RBI has provided clear guidelines for controls implementation, for the baseline cyber security and resilience framework. Following are the Baseline controls:

- Inventory Management of Business.

- IT Assets Preventing execution of unauthorized software.
- Application Security Life Cycle (ASLC).
- Patch/Vulnerability & Change Management.
- Vendor Risk Management.
- Removable Media.
- Maintenance, Monitoring, and Analysis of Audit Logs.
- Audit Log settings.
- Metrics.
- Forensics.
- Environmental Controls.
- Network Management and Security.
- User Access Control / Management.
- Authentication Framework for Customers.
- Advanced Real-time Threat Defense and Management.
- Anti-Phishing.
- Vulnerability Assessment and Penetration Test.
- Red Team Exercises.
- Incident Response & Management.
- User / Employee/ Management Awareness.
- Customer Education and Awareness.
- Secure Configuration.
- Secure mail and messaging systems.
- Data Leak prevention strategy.
- Risk-based transaction monitoring.

Besides these controls, the Banks are mandated to implement controls based on their level as decided by RBI. Those controls are as below:

Level 1 Banks Cyber Security

- Baseline Cyber Security and Resilience Requirement.
- Vendor/Outsourcing Risk Management.

Level 2 Banks Cyber Security

- Network Management and Security.
- Secure Configuration.

- Application Security Life Cycle (ASLC).
- Change Management.
- Periodic Testing.
- User Access Control / Management.
- Authentication Framework for Customers.
- Anti-Phishing.
- Data Leak Prevention Strategy.
- Audit Logs.
- Incident Response and Management.

Level 3 Banks Cyber Security

- Network Management and Security.
- Secure Configuration.
- Application Security Life Cycle (ASLC).
- User Access Control.
- Advanced Real-time Threat Defense and Management.
- Maintenance, Monitoring, and Analysis of Audit Logs.
- Incident Response and Management.
- User / Employee/ Management Awareness.
- Risk-based transaction monitoring.

Level 4 Banks Cyber Security

- Arrangement for continuous surveillance-Setting up of Cyber Security Operation Centre (C-SOC).
- Participation in Cyber Drills.
- Incident Response and Management.
- Forensics and Metrics.
- IT Strategy and Policy.
- IT and IS Governance Framework.
- Chief Information Security Officer (CISO).
- Information Security Committee.
- Audit Committee of Board (ACB).

Cyber Security and Cyber Forensics

13.3

At first glance, computer forensics and cyber security may seem similar, but there are key differences between the two professions. Computer forensics focuses on uncovering and preserving encrypted or lost data, while cyber security is about preventing data loss or cybercrimes from occurring. In short, one is reactionary while the other is preventative.

What is Cyber Security?

Cyber security is a professional discipline that is about creating defensive measures to protect against cyber attacks. People working in this industry may have a wide range of information technology (IT) skills including programming, operating systems, and networking. The primary goal of any cyber security professional is to create a network or system that is impossible to breach, thereby protecting the information within the network.

One important note about cyber security is that it is almost entirely about prevention. Even more niche positions, like ethical hackers, only use their offensive skills to test networks and improve them.

Cyber security encompasses many protocols that are used in the real world. Things like setting user permissions, establishing file transfer protocols (FTP), and requiring secure, frequently changing passwords are all vital elements of cyber security. It's not just up to one individual, everyone in an organisation needs to practice safe computer usage for security to be maintained.

What is Computer Forensics?

Computer forensics is the practice of recovering data from a device, often to uncover evidence of criminal activity. The practice itself is reactionary, meaning that it only takes place after an incident has occurred and is not concerned with preventing the incident itself.

Computer forensics jobs typically serve one of two purposes. They either assist with an investigation or help people and companies recover data that has been lost. In the first instance, a computer forensics specialist will be given access to a suspect's device, such as a laptop, desktop, or smartphone. Once they have the device, they begin using a variety of skills, such as programming, hardware knowledge, and software knowledge, to locate valuable data. In a law enforcement case, they will ideally uncover data that is of value to the prosecution and can be presented in a court of law. To do this, the data must be recovered in a very particular manner that does not violate the suspect's rights.

Sometimes, computer forensics specialists are called in to help a company recover lost data. While the purpose of the assignment differs greatly from uncovering evidence of criminal activities, the processes used to recover the lost data are very similar. The main difference in the execution of these tasks is that the particular processes required to create court-admissible evidence do not need to be followed in this case. In some cases, if the data is lost as a result of cybercrime, the computer forensics expert may be tasked with recovering the data and identifying the perpetrator of the crime.

Cyber Security vs. Computer Forensics

In short, cyber security is focused on prevention while computer forensics is about recovery and reaction. Despite their differences, both are meant to protect data, programs, networks, and other digital assets. Cyber security helps to prevent cyber crimes from happening, while computer forensics helps recover data when an attack does occur and also helps identify the culprit behind the crime.

It helps to think of cyber security professionals as a security company, and to think of computer forensics experts as investigators.

What Specializations are Available in Cyber Security and Computer Forensics?

Cyber security and computer forensics both have a few specializations that focus on specific areas of the practice. Cyber security has far more specializations, such as systems architecture, software security, access management, ethical hacking, and vulnerability assessment.

Computer forensics specializations tend to be related to the reason why the data is being recovered. The main specializations are criminal investigations, in which the expert is tasked with uncovering data that is relevant to a crime, and data recovery.

Data recovery specialists are mostly concerned with getting data back in the hands of its rightful owner, though they may also perform an audit to find evidence of a data breach if the data was stolen rather than lost through a technical issue.

IT Audit in Banking Sector

13.4

The objectives of IS audit are to identify the risks that an organisation is exposed to in the computerized environment. IS audit evaluates the adequacy of the security controls and informs the Management with suitable conclusions and recommendations. IS audit is an independent subset of the normal audit exercise in an organisation. The overall objectives of the normal audit exercise do not change, when applied to the computerized environment. The major objectives of IS audit include, among others, the following:

(a) Safeguarding of Information System Assets/Resources.

(b) Maintenance of Data Integrity.

(c) Maintenance of System Effectiveness.

(d) Ensuring System Efficiency.

Safeguarding of Information System Assets/Resources

The Information System Assets of the organisation must be protected by a system of internal controls. It includes the protection of hardware, software, facilities, people (knowledge), data files, system documentation, and supplies. This is because hardware can be damaged maliciously, software and data files can be stolen, deleted, or altered and supplies of negotiable forms can be used for unauthorized purposes. Safeguarding of the Information System Assets is a very important function of each organisation.

The term IT infrastructure is a generic one used to describe the physical computer installations, the system software, and the Information Systems process that support them. The IS auditor will require to review the physical security over the facilities, the security over the systems software, and the adequacy of the internal controls. The IT facilities must be protected against all hazards. The hazards can be accidental hazards or intentional hazards.

Accidental hazards include fire, flood, power failure, etc. Fire starts accidentally or is the result of a deliberate attack. All computer installations should take adequate precautions to ensure that fire can be prevented, detected, and extinguished. Flooding can cause extensive damage to computer systems. The power supply for the computer installation is a vital service need and the uninterrupted availability thereof has to be ensured to facilitate continuity in processing.

Maintenance of Data Integrity

Data Integrity includes the safeguarding of the information against unauthorized addition, deletion, modification, or alteration. This includes items such as accounting records, backup, documentation, etc. Information Systems are used to capture, store, process, retrieve and transmit the data securely and efficiently. The emphasis is on the accuracy of the data and its transmission in a secured manner. Data Integrity also implies that during the various phases of electronic processing, various features of the data viz. Accuracy, Confidentiality, Completeness, Up-to-date status, Reliability, Availability, Timeliness, and Effectiveness are not compromised. In other words, data should remain accurate during electronic processing.

The desired features of the data are described hereunder:

(a) **Accuracy:** Data should be accurate. Inaccurate data may lead to wrong decisions and thereby, hindering the business development process.

(b) **Confidentiality:** Information should not lose its confidentiality. It should be protected from being read or copied by anyone who is not authorized to do so. It also includes protecting the individual pieces of information that may seem harmless by the owner but can be used to infer other confidential information.

(c) **Completeness:** Data should be complete. Incomplete data loses its significance and importance.

(d) **Up-to-date Status:** Data should be updated regularly. If the information is not up-to-date, it presents a false picture of the organisation.

(e) **Reliability:** Data should be reliable because all business decisions are taken based on the current database.

(f) **Availability:** Data should be available when an authorized user needs it. It should be ensured that the information services are unavailable to unauthorized users.

(g) **Timeliness:** Timeliness of the data is very important because if data is not available when required, the very purpose of maintaining the database gets defeated.

(h) **Effectiveness:** Information should be effective so that it helps in the process of business development and expansion.

If data integrity is not maintained, an organisation loses its true representation. Poor data integrity could lead to the loss of competitive advantage. The corruption of data would affect many users in a networked environment. If the data is valuable to a competitor, its loss may undermine an organisation's competitive position.

Maintenance of System Effectiveness

An effective Information System significantly contributes to the achievement of the goals of an organisation. Therefore, one of the objectives of IS audit is to verify system effectiveness. It provides input to decide when what and how the system should be improved so that its utility to the management is maximum.

The main objective of introducing computerization in organisations in the banking and financial sector is to achieve the goals effectively and efficiently. The IS auditor's responsibility is to examine how the Information Systems assist in the achievement of each organisation's goals. System Effectiveness is a ratio of the actual output to the standard (budgeted) output. If it is more than 100%, effectiveness is achieved; or else, it shall be deemed that ineffectiveness has been introduced in the business process. Major goals and criteria of computerization are:

(a) **Improved Task Accomplishments**: The Information Systems should improve the task accomplishment capacity of its users by enabling them to become more productive.

(b) **Improved Quality**: It should improve the overall quality of work and services by increasing the accuracy of information. It should also reduce the time required for the retrieval of information.

(c) **Operational Effectiveness**: The Information System should be operationally effective and easy to use. It should be frequently used and users must be satisfied with its performance.

(d) **Technical Effectiveness**: The Information System should be equipped and upgraded with appropriate hardware and software from time to time.

(e) **Economic Effectiveness**: The Information System should be fully utilized. Benefits derived should exceed the cost of procurement, implementation, operation, and maintenance.

Ensuring System Efficiency

The resources used by the Information Systems such as the machines, computer peripherals, software, etc. are scarce and costly. Efficient Information Systems use minimum resources to achieve the desired objectives. When a computer no longer has excess capacity, system efficiency becomes important. It becomes necessary to know whether the available capacity has been exhausted or the existing allocation of the computer resources is causing the bottlenecks.

The ratio of the output to the input is known as efficiency. If the output is more with the same or less actual input, system efficiency is achieved; or else, the system is inefficient. If computerization results in the degradation of efficiency, the effort for making the process automated stands defeated. Hence, the assessment of the capabilities of the hardware and software against the workload of the environment is very essential. The IS auditors are responsible to examine how efficient the application software is about the users and the workload of the environment. The system should assist in management planning and efficient execution thereof. The organisation should get maximum output using minimum resources. In this context, the efficient use of the hardware resources and their upgradation, as per requirements, is very essential. Automation should deliver the planned results with less consumption of computer hardware, software, computerized operations, and computer personnel.

Other Objectives

The following could be, among others, considered the other objectives of IS audit:

(a) Identify the risks that the organisation is exposed to in the existing computerized environment and prioritize such risks for remedial action.

(b) The implementation of Information Technology in the organisation is as per the parameters laid down in the Security Policy, as approved by the Board of Directors of the organisation.

(c) Verify whether the Information System procedures and policies have been devised for the entire organisation and that the organisation's systems, procedures, and practices are adhered to and that due prudence is exercised at all times by the circulars and instructions for a computerized environment, issued by the management of the organisation.

(d) Verify whether proper security policies/procedures have been formulated and implemented regarding the duties of the system administrators, system maintainers, and persons operating the system for daily operations.

(e) Contribute effectively towards the minimization of computer abuses/ crimes by suggesting steps for removing any laxity observed in the physical and logical controls.

(f) Suggest improvements in the security controls for the Information Systems.

(g) Act as an advisor to the management of the organisation for improving security and IT implementation standards.

(h) Adhere to the established norms of ethics and professional standards to ensure the quality and consistency of audit work.

Scope of IS Audit

The IS audit should cover all the computerized departments/offices of the organisation. The scope of IS audit should include the collection and evaluation of evidence/information to determine whether the Information Systems in use safeguard the assets, maintain data security, integrity, and availability, achieve the organisational goals effectively, and utilize the resources efficiently. The scope of IS audit should also include the processes for the planning and organisation of the Information Systems activity, the processes for the monitoring of such activity, and the examination of the adequacy of the organisation and management of the IS specialist staff and the non-specialists with IS responsibilities to address the exposures of the organisation.

Information Systems Audit Approaches

There are three approaches for conducting Information Systems Audit viz. auditing around the computer, auditing through the computer, and auditing with the computer.

Auditing around the Computer

Under this approach, the emphasis is on checking the correctness of the output data/documents concerning the input of a process without going into the details of the processing involved. This approach is preferred, where auditors themselves do not have the desired level of technical skills to adopt the other approaches. This is also preferred, when high reliance is placed on the users rather than the computer controls to safeguard the assets, maintain data integrity and attain effectiveness and efficiency objectives. The focus is on procedural controls rather than computer controls. This approach can be used in the following circumstances:

When an application system is simple, logic is straightforward, and a clear audit trail exists, this approach can be adopted. The process generates the audit trails such as the generation of exception reports along with the main reports. Such systems have very low inherent risk i.e., they are unlikely to be susceptible to material errors or irregularities or to be associated with significant ineffectiveness or inefficiencies in operations. Input transactions in such systems are in batch mode and control is maintained using traditional methods like the separation of duties and management supervision. Further, the task environment in such systems is relatively constant and the system itself is rarely modified.

This approach may be used when an application system uses a generalized package that is well tested and used by many users as its software platform. If the package has been provided by a reputed vendor, has received widespread use, and appears error-free, the auditors may decide to adopt this approach. Auditors should ensure that the organisation has not modified the package and adequate controls exist over the source code and documentation to prevent unauthorized modification of the package.

When high reliance is placed on the users rather than the computer controls to safeguard the assets, maintain data integrity and attain effectiveness and efficiency objectives, this approach can be adopted.

Auditing around the computer is a simple approach. It does not provide any information about the system's ability to cope with the changes. Systems can be designed and programs can be written in certain ways to inhibit their degradation when user requirements change. Further, this method cannot be used for complex systems. Otherwise, the auditors might fail to understand some aspects of a system that could have a significant effect on the audit approach.

Auditing through the Computer

Auditing through the computer requires a fair knowledge of the operating system, hardware being used, and certain technical expertise in systems development. Under this approach, the computer programs and the data constitute the target of IS audit. Compliance and substantive tests are performed on the computer system, its software (both operating system and application system), and the data. IS auditors can test the application system effectively using this approach. The IS auditors can use a computer to test logic and controls existing within the system and also records produced by the system. This approach increases the IS auditor's confidence in the reliability and applicability of the evidence/information collected and evaluated. This approach is time-consuming, as it needs an understanding of the internal working of an application system. It also needs some technical expertise.

Auditing with the Computer

Under this approach, the computer system and its programs are used as tools in the audit process. The objective is to perform substantive tests using the computers and their programs. The data from the auditee's computer system

are retrieved in an independent environment. Audit interrogation and the query are carried out on such data, using special programs designed for the purpose. This method is used where:

(a) Application system consists of a large volume of inputs, producing a large volume of outputs and where the direct examination of the inputs/outputs is difficult.

(b) Logic of the system is complex.

(c) There are substantial gaps in the visible trails.

Computers are quite useful in the testing of transactions. Some of the software tools used for this purpose are briefly described hereunder:

Computer Assisted Audit Tools (CAATs) are efficient and effective ways to audit system-generated files, records, and documents and to evaluate internal controls of an accounting system in many Information Systems. Computer Assisted Audit Tools are a practical means for conducting an audit, wherever the information is available on the magnetic media alone. The technical papers relating to the use of the CAATs should be kept separate from the other audit working papers. The IS audit documentation should contain the description of the CAAT application.

Audit Software: It is a program, used by the auditors, to process data of audit significance from the auditee's accounting system. There are three types of such programs as under:

(a) Package programs are designed to perform processing functions, creating data files and reports in a format specified by the auditor.

(b) Special Purpose Programs are used to perform the audit tasks in specific circumstances and are prepared by the auditors or an outside programmer, engaged by the auditor.

(c) Utility Programs are used to perform common data processing functions such as sorting, creating, and printing files.

Test Data Techniques: A sample of data transactions is entered into the auditee's computer system and the results are compared with the predetermined results. CAATs are used to test the details of the sample transactions, the balances of the accounts, to identify unusual fluctuations if any, and general EDP controls like accessing the program libraries.

General Audit Software: It is the most widely used technique in conducting IS audits. Its use is limited by the skills of the personnel conducting the audit. Audit Command Language (ACL) is one such software. It is a tool for data analysis. It has the capabilities for Compliance and Substantive testing.

ACL is used to access, analyse, summarize or report data. Advantages of the ACL are as under:

(a) It creates flexible reports and documents.

(b) Auditors are independent of the technical experts for the data, access, and process.

(c) It increases audit coverage.

(d) It saves time, money, and effort.

(e) It helps gain control over and confidence in the audit results.

(f) General Audit Software is not useful at the application level.

Any Computer Assisted Audit Tool (CAAT) is as good as a data mining tool, which is used for extracting data from a data warehouse for MIS / Audit purposes.

Information Systems Audit Methodology

Audit Methodology:

The IS audit work includes manual procedures, computer-assisted procedures, and fully automated procedures, depending on whether it is around, though, with, or a combination of all these types of audits. In many cases, a combination of these techniques is required. The IS auditors may utilize the manual procedures when they are more effective than the other alternatives or when these procedures cannot be partially or fully automated. He/she should also use computer-assisted procedures known as Computer Assisted Audit Tools (CAATs) because they permit the IS auditors to switch from the procedures based on limited, random, and statistical samples of records in a file to a procedure that includes every record in a file.

Audit activity is broadly divided into 5 major steps for the convenience and effective conduct of the audit.

(a) Planning IS Audit.

(b) Tests of Controls.

(c) Tests of Transactions.

(d) Tests of Balances.

(e) Completion of Audit.

(a) Planning IS audit:

Planning is the first step of the IS audit. IS auditors should plan the audit work in a manner appropriate for meeting the audit objectives. As a part of the planning process, IS auditors should obtain an understanding of the auditee department/ office/organisation and its processes. It includes an understanding of the objectives to be accomplished in the audit, collecting background information, assigning appropriate staff keeping in mind skills, aptitude, etc., and identifying the areas of risk. Risk analysis of the operating system is carried out to identify the system with the highest risks, considering the critical nature of the information processed through such system as well as the number and the value of the transactions processed. This is to identify the systems having the highest risk and to decide on the extent of the detailed analysis and testing to be conducted on those systems.

In this phase, IS auditors are required to understand the internal controls used within an organisation. Various techniques can be used to understand the internal controls viz. review of previous audit reports/papers, interview/ interaction with the management and Information Systems personnel, observation of activities carried out within the Information Systems function, and review of Information Systems documentation.

(b) Tests of Controls:

During this phase of IS audit, Internal Controls are tested to evaluate whether they operate effectively. This includes testing of management controls and application controls. The objective is to evaluate the reliability of the controls and find out weaknesses of the controls for meeting the IS audit objectives. IS auditor is required to make recommendations to rectify the weaknesses, observed during an IS audit.

While carrying out tests of controls, the IS auditors should satisfy themselves regarding the following aspects of controls.

- **Identification:** Organisation should identify the controls to minimize the occurrence of unlawful events.
- **Implementation:** Identified controls should be implemented.
- **Existence:** Sometimes it happens that controls have been implemented, but in reality, they do not exist due to various reasons. For example, the organisation may have stipulated that the users should change their passwords every week. But, in reality, this may not be happening. The physical existence of the controls is equally important.

- **Adequacy:** IS auditors should examine the adequacy of the controls. They should see that the controls are adequate to cover all possible threats.
- **Documentation:** All controls should be documented to make them effective.
- **Maintenance:** Controls should be maintained intact continuously. For example, only the provision and installation of the fire extinguishers, smoke detectors, UPS, etc. do not solve the problem. These instruments should be properly maintained, so that they serve the purpose, as and when needed.
- **Monitoring:** Controls should be monitored using strict supervision, surprise checks, periodic inspection, etc.

(c) Tests of Transactions:

Tests of Transactions are used to evaluate whether erroneous transactions have led to a material misstatement of the financial information and whether the transactions have been handled effectively and efficiently. The objective is to evaluate data integrity. Some of such tests include the tracing of journal entries to their source documents, the examination of the price files, the testing of computational accuracy, the study of the transaction log, etc. These tests are used to indicate the database system's effectiveness. CAATs are quite useful to perform these tests.

(d) Tests of Balances:

During this phase of IS audit, final judgment is made on the extent of the losses or account misstatement that occur when Information Systems fail to safeguard assets, maintain data integrity and achieve system effectiveness and efficiency goals. As regards the safeguarding of assets and data integrity objectives, the typical substantive tests used are confirmation of the receivables, physical verification of inventory, and recalculation of depreciation on the fixed assets. Regarding the system effectiveness and system efficiency objectives, the tests to be conducted are in the process of evolution. For example, the shortcomings in the Information Systems Planning may have resulted in the purchase of inappropriate hardware. The system may provide outputs, but not of the required standards to make high-quality decisions. During this phase of the IS audit, computer support is often required. General Audit Software can be used to select and print confirmations; expert systems can be used to estimate the likely bad debts and so on.

(e) Completion of Audit:

This is the final stage of IS audit. Auditors are required to form their opinion, clearly indicating their findings, analysis, and recommendations. Potential IS audit findings should be discussed with the appropriate/authorized personnel throughout IS auditing. Preliminary conclusions and the audit findings should be presented to the auditee during an exit conference. All potential findings with sufficient merits and preliminary audit recommendations should be included for discussion in the exit conference. The exit meeting should document and include the auditee's comments and questions concerning the preliminary IS audit recommendations. The draft audit report should be the natural extension of the exit conference materials along with the discussions that took place during the exit meeting. Once the auditee's responses have been received, the final audit report should be prepared and submitted to the designated authority/ management of the organisation.

Work papers used in the auditing should be well organized, clearly written, and address all the areas included in IS audit. IS audit work papers should contain sufficient evidence/information of the tasks performed and the conclusions reached, including the results achieved, issues identified, and authorized signatures approving the final opinion.

A typical audit report will include, among others, an introduction to the audit objectives, scope, general approach employed, a summary of the critical findings, the data to support the critical findings, potential consequences of the weaknesses, auditee's responses, and recommendations to rectify the weaknesses.

Sub-system Factoring

IS audit being generally an exercise dealing with complex Information Systems. To understand the complex system, it is always advisable to break the system into sub-systems. A sub-system is a component of a system that performs some basic functions needed by the overall system to attain its basic objectives. The process of breaking a system into sub-systems is called factoring. The process of factoring terminates when it is felt that the system has been broken into sub-systems, small enough to be understood and evaluated. Thus, a complicated system is divided into small sub-systems until it becomes easily understandable.

Once the system has been factored into several easily understandable subsystems, the task of the IS auditors is:

(a) To evaluate the effectiveness of the controls in each sub-system.

(b) To determine the implications of each sub-system's reliability vis-a-vis the overall reliability/effectiveness of the system.

There are two main sets of systems, which require to be further factored into sub-systems for conducting IS audit.

Management Systems

Management Systems provide stable and basic infrastructure facilities on which the Information Systems can be built and operated on a day-to-day basis. Management Systems can be factored into sub-systems that perform Top-level Management, Information Systems Management, Systems Development Management, Programming Management, Data Administration, Quality Assurance Management, Security Administration, and Operations Management.

Top-level Management is responsible for long-term policy decisions on the use of Information Systems in the organisation.

Information Systems Management is responsible for planning and controlling the Information Systems activities in the organisation. It assists the top management in making long-term policies and translates the long-term policies into short-term goals and objectives.

Systems Development Management designs, implements and maintains the application systems.

Programming Management prepares programs for new systems, maintains old systems, and provides general systems support software.

Data Administration addresses the planning and control issues about the use of the database.

Quality Assurance Management ensures that the Information Systems development, implementation, operations, and maintenance conform to the established quality standards.

Security Administration is responsible for access control and physical security over the Information Systems. Operations Management plans and controls the day-to-day operations of the Information Systems.

Application Systems

Application Systems undertake basic transactions processing, management reporting, and decision support. They can be broken into sub-systems that perform boundary, input, communication, processing, database, and output functions.

The boundary sub-system consists of the components that establish an interface between the user and the system. Input sub-system comprises the components that capture, prepare and enter commands and data into the system. The Communications sub-system consists of the components that transmit data among the sub-systems and systems. The processing sub-system includes the components that perform decision making, computation, classification, ordering, and summarization of the data in the system.

Database Sub-system comprises the components that define, add, access, modify and delete data in the system Output Sub-system consists of the components that retrieve and present data to the users of the system.

Broad Framework for Conducting IS Audit

A broad framework can be formed from the basic objectives of IS audit. In addition to this, IS audit evaluates the organisational setup and quality of administration. It should be noted that IS audit is not limited by laid down procedures. It is also important to keep one's eyes and ears open. The IS auditors should, therefore, analyse what they observe and hear. The main issue involved in IS audit is the confidentiality of programs, files, access rights to files and focus on software application packages. The major concerns of the IS audit, as derived from its objectives, are as under:

A. Safeguarding Assets:

One of the prime objectives of any audit is to ensure that the assets of the organisation are safeguarded. In the computerized environment, the assets to be safeguarded are hardware, software, data, and users. The yardstick to measure the importance of this objective is the expected loss that may be sustained by the organisation if the asset is destroyed, stolen, lying unutilized, service denied, or used for unauthorized purposes. The IS auditors should verify that the assets are put to effective use in a secured environment. To determine whether the assets of the organisation are duly safeguarded, the IS auditors should inspect, among others, the following areas:

Environmental Security: It is very important for the effectiveness of all other protective measures stipulated or installed at the sites. The server room houses the all-important hardware. Its location should be a strategic one and not easily accessible. The server room should be exclusively for the server itself and the other items, equipment, etc. should not be kept there.

Uninterrupted Power Supply: The uninterrupted power systems are meant for supplying conditioned and stabilized power to computer equipment at all times. It also provides stabilized power from battery storage when electricity fails. The UPS must function properly when electricity fails. The UPS should be maintained regularly.

Electrical Lines: Electrical cabling and wiring constitute the basic components. Faulty electrical cabling and wiring are responsible for operational failures. There should be separate and proper earthing for the dedicated electrical line.

Data Cabling: Information Technology experts estimate that 90 percent of the network problems are cable-related. Hence, all possibilities of routing cables, locations of cable closets, sites of Switch, Router installation, etc. should be explored before finalizing the plan. A detailed map of the cable layout including Switches, Routers is very important to guide the hardware service engineer in the event of a LAN cable fault. Further, electrical cable and data cable should not cross each other to avoid possible disturbance during data transfer.

Fire Protection: Fire alarm systems, smoke detectors, and fire extinguishers are very important to deal with the event of a fire breaking out. Fire extinguishers are commonly filled with water, carbon dioxide, or Halon. Little care is required while operating gas-based extinguishers because they replace oxygen and thereby, extinguish the fire. Water is effective, but it is dangerous to use in proximity to live equipment. Dry powder or foam-type extinguishers are not advisable because they leave deposits on the equipment.

Insurance: All critical computer equipment is required to be insured with a reputed insurance firm/s to secure the Information System resources/assets of the organisation.

Annual Maintenance Contract: Periodic maintenance of the computers, network, etc. is essential to ensure trouble-free operations of the equipment. For this purpose, it is required that the annual maintenance contract be awarded and renewed in time. At the same time, it is also essential that the maintenance staff is available on time. There should be a proper record of the activities carried out during maintenance.

Logical Security: It restricts access to the system if the user fails to identify himself/herself to the system correctly. Login name/user ID and password are controls for this security. It is exercised at the operating system level and the application system level. Logical security at the operating system level ensures access to the computer system when it is successfully powered on after its boot operation is completed. Logical security at the application system level gives access rights to specific application software depending on the responsibility and authority of the user. IS auditors should verify the effectiveness of the logical security in place by evaluating its controls. Secrecy and security of the user ID and password, different levels of access rights and their allocation to the users, creation of users, its records, users created for maintenance purpose and their termination on completion of the work, a user log in the status report, presence of dummy user ID in the system, etc. are some of the points which require consideration of the IS auditors.

B. Data Integrity:

Data is the most important resource in a computerized environment, which needs to be accurate, complete, consistent, up-to-date, and authentic. The IS auditors are concerned with the possibility of deviation from the standards. They are required to verify how well data integrity is maintained and find out any laxity therein.

The examination of the following points is very important in respect of data integrity:

Data Input Controls: The largest number of controls is available at the time of data entry in the system. Data Input Controls are error-prone because the activities involved in data entry are of a routine and monotonous nature. Data entry is also a major area for intentional fraudulent activity. It involves the addition, deletion, modification, or alteration of the input transactions or data. Hence, the IS auditors should minutely evaluate the effectiveness of the data input controls. The use of the scanner and inputs to the system through floppy should be monitored and controlled.

Data Processing Controls: The application system processes the data online on a day-to-day basis. The IS auditors are concerned about the Data Processing Controls. They should examine that only designated/authorized officers perform the start-of-day operation. The day-end process should be completed with the generation of the prescribed reports. It is also required that proper record is maintained in respect of the corrections made in the database under authentication.

Patch Program: It uses the file structure of the existing database files and is capable of effecting changes in a data file. It bypasses the proper menu access controls provided by the application software system and does not leave an audit trail. It can add, modify, alter and delete the data. The behaviour of the approved programs is known and certified, but it is uncertain in the case of such patch programs. They usually bypass all the safeguards available to the system programs. They conveniently flout all norms to achieve results at any cost. Therefore, the IS auditors should verify that only approved programs are loaded in the system and the application programs are identical with the list of the approved programs in respect of file name, file size, date, and time of compilation. It is also necessary that a record be maintained regarding the patch programs used indicating the reasons under authentication.

Purging of Data Files: It is pruning of the data files of the identified past period for which it is no more necessary to store the data in the current system. Before undertaking the purging activity, it is necessary to take a backup of the full data directory. The purging of the static data or master particulars is never taken. The IS auditors should examine that the purged data backup media is stacked in chronological order for easy tracing and also is in safe custody. A manual record of purging activity should also be maintained. Access to the purged data should be restricted and controlled to ensure the integrity of the purged data.

Data Backup: Data backup is an essential aspect of all computer operations. Some commonly used computer media include hard disks, floppy disks, tape cartridges, CD-ROMs, DVD ROMs, etc. Off-site back-ups are taken

on floppies or tape cartridges, while on-site back-up is taken on hard disks. Back-up is one of the measures of business continuity planning and is also required for archiving old records. The backups must be taken regularly. One set of backups requires to be stored off-site. The backups have to be tested periodically by restoring the data therefrom. The backup media have to be verified periodically for readability. Backup media should be properly labelled and numbered. This is a very important area and requires proper attention.

Restoration of Data: It is defined as downloading of data afresh from magnetic media, in case of a crash of the system, irrecoverable corruption, or loss of data, for going back online. Backup is taken at a particular point of time like the beginning of day operations, end of day operations, etc. Thus, the restoration of data is dependent on the magnetic media and the data stored thereon. Restoration of the data is required in the event of major corruption of data. In the event of a virus attack or destruction of a server or the computer site, the only option is to fall back upon the restoration option. Restoration of data helps to obtain a position of data as of a particular date, to establish whether any data tampering has taken place. It assists in conducting system audits as of the previous date and generates ledgers of previous years. Transactions of the purged period can also be retrieved.

C. Business Continuity Planning:

Disruption of operations can occur because of two types of problems. First, some minor problems like power failure, UPS failure, server failure, inability to read/restore backups, cable fault, etc. can disrupt the operations. The second type of disruption can occur on account of natural calamities like fire, flood, building collapse, or man-made calamities like a bomb blast, radiation, virus attack, induced data loss, etc. Business Continuity Plan is prepared to recover from such kinds of interruptions. It relates to a higher level of failure. It is all about anticipating any disastrous event and planning adequately for the business to live through it. The IS auditors should verify the existence and operability of the Business Continuity Plan. They should also examine the awareness of the staff regarding the execution of the plan in a genuine emergency and comment upon its effectiveness. Business Continuity Plan should be documented and tested at regular intervals to assess its effectiveness.

BCP is required to satisfy short, medium, and long-term recovery. In the short term, the essential systems and services are restored. Medium-term plans are for recovering the organisation's systems and services temporarily. Long-term plans are for a total recovery of the processing environment.

There are three methods of recovery namely cold, warm and hot backup sites. A cold site is where a computer room is provided in which equipment can be installed when needed. A warm site is a computer room filled with all the required equipment, but onto which all the software and applications must be loaded when it is needed. A hot site is one where the original installation is duplicated and ready to use when a disaster occurs.

BCP should outline the responsibilities for all the recovery processes, procedures for reproducing the computer media, location of the backup media, priorities for recovery, sources of replacement hardware and software, and alternative data communication facilities.

Output Reports: One of the basic principles in the computerized environment is known as GIGO i.e., 'Garbage in Garbage out. This means that, if the input to the system is garbage (or meaningless), the output will also be garbage. Reports and printouts are generated in the computerized environment to ensure the correctness of the inputs and processing. Reports are also important to ensure that the application system programs serve the needs of the organisation. Any lacunae or bugs in the application software can be located by checking the reports and printouts. The importance of checking the reports can never be overemphasized. The IS auditors should scrutinize output reports on a sample basis to identify the trend, the quality of follow-up, and the control exercised by the management. The audit trail report should generate the user ID of the data entry operator and the authorized official

for any addition, change, modification, and deletion of transactions effected in the database. It should provide evidence/information of unauthorized access outside the application menu. The IS auditors should verify whether the audit trail reports are generated and checked by the designated officials. Exceptional transaction report is also very important to report.

Version Control: Data integrity is very much dependent on the version of the software running in the system. An authorized version of the software can lead to accurate processing. Non-standard programs are a potential threat to integrity. A complete listing of the programs loaded in the system should be available on record for verification. The IS auditors should verify that licensed copies of the operating system and the application system software are used for computerized operations.

Virus Protection: A computer virus is a program that is self-replicating and can corrupt or destroy data irretrievably. It resembles biological viruses in behaviour. It may have a dormancy period and get activated on a certain date. It is potentially disastrous. Anti-virus software is available and is capable of countering against known viruses, malicious programs. Anti-virus software is updated by the manufacturers regularly to counter against the new viruses coming up. It is necessary to keep the anti-virus software updated at all times. All extraneous floppies and other media should be checked/scanned for viruses before use.

D. System Effectiveness:

It is expected that the Information system should improve the overall quality of work including accuracy and time consumed in performing the tasks. Further, it should be user-friendly. The IS auditors should judge how effective the system is in accomplishing the goals with which computerization was introduced.

E. System Efficiency:

The IS auditors should examine whether every computer asset is used to its maximum operational capacity.

F. Organisation and Administration:

Efficiency in computerized operations is dependent on the efficiency of the personnel using the computer resources. Computer personnel should do their work completely, timely, accurately and that too, with minimum resources. They should deliver more output quantitatively and qualitatively. Proper placement of the computer personnel based on their aptitude, skill, knowledge, and experience is very important. Computer personnel should be used effectively and efficiently with proper security for the organisation to reap maximum advantages.

Segregation of duties, the job description for each level, proper training to the staff, dual control aspect in performing important operations, a designated system administrator with the suitable back-up arrangement, etc., are important points to be considered. Records of work assigned to the staff, rotation, training imparted, login name given, etc. are to be checked/verified by the IS auditors.

To Sum Up:

Information Security Audit is an evaluation process that assesses an organisation's established security practices. It is a process that determines the effectiveness of the defense systems established against any threats.

The Information Security Audit typically includes vulnerability scans, penetration testing, network assessments, and much more that help determine vulnerabilities and security loopholes in the IT systems. The audit is a combination of administrative, physical hardware, software application, and network assessment. This way, the evaluation process can help a company/organisation gain an understanding of its current security posture.

Solved Cases

Case Study: 1

Practical 'IS Audit' Case Study for Verification of 'Know Your Customer (KYC)' in Core Banking System (CBS) of Banks.

The objective of this Case Study is to Test KYC Norms on 'Savings Bank Account' from Customer Master Data in Core Banking **Solutions (CBS) of Banks.**

To Test this objective, the auditor has to issue a 'Data Request' to IT Department in the following format:

- **Data Required:** Savings Bank Account Customer Master Information in CBS.
- **Period:** Period of Audit Coverage.
- **Fields of Reference:** Branch ID, Customer ID, Account ID, First Holder & Joint Holder/s Name, Address, PAN Number, Mobile Number, Residence Number, Office Number, Mode of Operation, and Clear Balance.
- **Format of Data:** Text Form.

IT Department in turn ran a SQL Query on the production database and generated a text file dump, which was saved by IT in a secure folder with special access to the Audit Team only.

The Audit team has to import the text file, using the Text Report import option within the Generalised Audit Software (GAS).

Post import, the Auditor has to use the Duplicate Key test within the GAS to identify fictitious accounts opened with similar PAN Numbers, Mobile Numbers Address Office Numbers, or Residence Numbers but different Customer IDs.

The Auditor has to identify where account opening details like PAN Number, Mobile Number, etc. were similar for different Customer IDs. These cases have been taken up for further checking with the account opening forms from the respective Branch to ascertain the validity of the accounts opened.

Additionally, the Auditor has to employ a SOUNDEX (**Soundex** is a phonetic algorithm for indexing names by sound, as pronounced in English) Test on the Customer Name Field. The SOUNDEX Test generates a unique alpha-numeric code in a new computed field. This code depends on the mnemonic of the Name rather than the spelling. For example. Two Customer Accounts with the names Prasanna Iyer and P AIyer will have the same SOUNDEX Code. After arriving at this code, duplicate tests can be run on the code rather than the Name. The advantage here is that the Duplicate on Code will generate similar-sounding names (Essence of De-Dup Tests Globally), whereas a pure Duplicate will perform an exact match.

The Auditor has to perform De-Dup Tests to Identify Customers who have multiple Savings Bank Accounts within the same Branch of the Bank, which is a potential Red Flag.

The above is the IS Audit Procedure to identify the KYC-which is an important aspect while opening Customer Accounts by the Commercial Banks.

The same procedure is to be adopted by the IS Auditor to verify the various Electronic Products of the Banking, but the Characteristics / Objectives / Fields may be different from One Bank Product to another Bank Product.

Case Study: 2

Vodafone Intelligent Solutions (VOIS), formerly known as Vodafone Shared Services Ltd, is a Vodafone Group partnership whose mission is to create a world-class digital experience to connect and inspire people to build a better tomorrow. Founded in 2009, Vodafone Shared Services Ltd provides voice support for IT shared services, network shared services, financial and HR shared services along with BI & Analytics, digital experience, and automation to Vodafone Group, local markets, and companies across the globe.

For Vodafone, maintaining strict cybersecurity measures is an integral part of delivering an exceptional digital experience to its customers. Cybersecurity is built into all systems, processes, and applications, to proactively defend against the prolific and increasingly sophisticated cyber threats facing organisations today.

Challenges:

As a partner to Vodafone UK Customer Care, VOIS India is required to maintain resilient adherence to PCI DSS compliance at all times, since Vodafone UK Customer Care has to deal with various customers of the UK Mobility with an obligation to protect their data. These companies typically store significant amounts of personally identifiable information (PII), including names, addresses, and financial details belonging to their customers. Given the nature and range of information, the impact of a cyberattack can be both serious and far-reaching.

As part of Vodafone's PCI DSS requirements, Gururaj Kannarpadi, General Manager of IT at Vodafone, was tasked with evaluating potential vendors for a cost-effective File Integrity Monitoring (FIM) and Change Control solution to help them safeguard sensitive customer credit card data is stored within their environment as well as meeting the strict compliance requirements laid out by the PCI-DSS.

Gururaj explained, "I began my evaluation by running a POC with a company who I originally believed to be the leader in this space. After 2 months and resources spent running the POC, their solution was not picking up suspicious changes within our environment, or collecting much data at all, to be frank, so we had to cut our losses and move on to explore other possible solutions."

Solution:

After searching for vendors in the FIM and Change Control space, Gururaj quickly learned of NNT Solutions (No-Name Technologies Inc.) and discovered early on that its Change Tracker Gen7 R2 solution was not only the most feature-rich, but that it was also the most competitively priced solution on the market combined with vastly superior proactive pre-sales and technical support.

Gururaj noted that "Once I requested a demonstration of NNT's solution I was immediately surprised to see just how quickly and responsive their team was. Overall, the excellent pre-sales experience with NNT set the tone for how I would be treated if I was a customer and compared to the alternative provider we were originally speaking to - the difference was night and day."

Like most organisations, VOIS was looking for a reliable FIM solution that could help spot malicious changes, but not be inundated with overwhelming change noise. Fortunately for VOIS, NNT's Closed-Loop Intelligent Change

Control Technology captures and identifies reoccurring change patterns and automatically identifies them as either harmless or potentially harmful, as well as highlighting changes that were not part of a pre-approved change request. NNT puts the 'Integrity' back into FIM.

Gururaj claims, "From the start of my journey with NNT, the sales and technical support teams were nothing but helpful and committed to finding us a solution to our PCI compliance needs. Not to mention that we purchased Change Tracker at a fraction of the cost of their competitors. There's no comparing Change Tracker to anything else – Change Tracker is undoubtedly the clear winner in the FIM and Change Control market."

Results:

Working with NNT has allowed Vodafone to address their mandatory PCI DSS requirements by adopting an integrity monitoring and change control solution that assures their customers that their data is being properly tracked for any changes that may be harmful.

Gururaj claimed, "To anyone looking for vendors in this space, I would blindly close your eyes and go with NNT. Don't even bother with the demo - just go for it. I've done the research and have seen first-hand the kind of results you can expect to see."

With Change Tracker, Vodafone is now able to achieve continuous PCI compliance and streamline the audit process by removing the need for internal staff to spend countless hours collecting evidence to present to external auditors.

Exercise

A. Theoretical Questions

Multiple Choice Questions

1. Control in the design of an information system is used to _____ .

   (a) Inspect the system and check that it is built as per specifications.

   (b) Protect data from accidental or intentional loss.

   (c) Ensure that the system processes data as it was designed to and that the results are reliable.

   (d) Ensure the privacy of data processed by it.

2. Controls are necessary for information systems as _____ .

   (i) Massive amounts of data are processed and human errors are expected in data entry.

   (ii) Accidental errors can lead to loss of money and credibility in a system.

   (iii) To protect the system from virus attack.

   (iv) Data may be lost due to disk crashes.

   (a) (i) and (ii)

   (b) (i) and (iii)

   (c) (i) and (iv)

   (d) (ii) and (iii)

3. The major objectives of control are _____ .

   (i) Guard against frauds in data entry/processing.

   (ii) Check clerical handling of data before it enters a computer.

   (iii) To provide a method to trace the steps and find where an error has occurred.

   (iv) Automatically correct errors in data entry/processing.

   (a) (i), (ii), and (iv)

   (b) (i), (ii), (iii), and (iv)

   (c) (i), (ii), and (iii)

   (d) (i) and (iii)

4. A two-way check is used to _____ .

   (i) Check program correctness.

   (ii) Find data entry errors.

   (iii) Find multiplication errors.

   (iv) Find an arithmetic error in processing.

   (a) (i) and (ii)

   (b) (ii) and (iii)

   (c) (ii) and (iv)

   (d) (i) and (iv)

5. A check-point procedure _____ .

   (a) Checks program correctness at certain points.

   (b) Divides a program into smaller parts.

   (c) Breaks programs into portions at the end of each of which a check point program is executed.

   (d) Finds points in a program where it is convenient to check it.

6. Audit in the design of information system is used to _____ .

   (a) Inspect the system and check that it is built as per specifications.

   (b) Protect data from accidental or intentional loss.

   (c) Ensure that the system processes data as it was designed to and that the results are reliable.

   (d) Ensure the privacy of data processed by it.

7. By auditing around the computer, we mean _____ .

   (a) The inputs and the corresponding outputs are compared and checked for correctness.

   (b) The programs and procedures are checked for correctness.

   (c) Special synthetic data is input and outputs checked for correctness.

   (d) Programs are written to check the functioning of the computer.

8. An audit trail is established in a system to _____ .

   (a) Detect errors in a system.

   (b) Enable auditing of a system.

   (c) Localize the source of an error in a system.

   (d) Trail a program.

9. In auditing with a computer _____ .

   (a) Auditing programs are designed and used to check a system.

   (b) The hardware of the computer is thoroughly checked for malfunctions.

   (c) System software is thoroughly checked to ensure error-free operations.

   (d) Auditors check the system with a computer.

10. By information system testing we mean _____ .

   (a) Testing an information system correctly.

   (b) Determining whether a system is performing as per specifications.

   (c) Determining whether a system is performing optimally.

   (d) Ensuring proper function of a system.

11. Parallel runs are used _____ .

   (a) During regular operation of an information system.

   (b) When a system is initially implemented.

   (c) Whenever errors are found in a computerized system.

   (d) Whenever management insists.

12. To protect a system from viruses one should _____ .

   (i) Not allow unauthorized use of floppy disks.

   (ii) Scan viruses in files received via a network or floppies.

   (iii) Isolate a system from networks.

   (iv) Install a roll-back recovery program in the system.

(a) (i) and (iii)

(b) (i) and (ii)

(c) (ii) and (iv)

(d) (i), (iii), (iv)

13. A firewall is used in a system connected to a wide area network to _____ .

(a) Prevent the spread of fire in the network.

(b) Prevent unauthorized access by hackers.

(c) To scan for viruses in files.

(d) To extinguish fire spreading via network cables.

14. Security in the design of information systems is used to _____ .

(a) Inspect the system and check that it is built as per the specifications.

(b) Protect data and programs from accidental or intentional loss.

(c) Ensure that the system processes data as it was designed to and that the results are reliable.

(d) Ensure the privacy of data processed by it.

15. It is necessary to protect the information system from the following:

(i) Natural disasters like fire, floods, etc.

(ii) Disgruntled employees.

(iii) Poorly trained employees.

(iv) Hackers.

(v) Industrial spies.

(vi) Data entry operators.

(a) (ii), (iii), (iv), (v)

(b) (i), (ii), (iii), (iv), (v)

(c) (i), (iv), (v)

(d) (i), (ii), (iii), (iv), (v), (vi)

Short Essay Type Questions

1. What is an RFC?
2. What types of processes can you add to deployment plans to help security?
3. What are some ways that companies can lose data?
4. In evaluating the use of a biometric system in an environment that has high-security requirements, what is an item that is important to consider?
5. Describe a honeypot.
6. When an auditor evaluates an IT system, what user features should be evaluated?
7. Auditors are used to review security controls and policies. What are the pitfalls of inadequate control implementation and policy definitions?
8. What is the purpose of network encryption?
9. Name two types of backup methods used for remote backup sites.
10. What is sociability testing?
11. Discuss the nature and significance and scope of the systems audit. Also mentions various steps involved in conducting an information system audit.
12. Discuss system audits of computerized secretarial functions.
13. Write short notes on:
    (a) Norms and procedures for computerization
    (b) Computer control and security
    (c) Testing of computer system
    (d) Objectives of Information Systems Auditing
14. Discuss the Foundations of Information Systems Auditing.
15. What do you mean by operation control? Describe in details.
16. What do you mean by test pack? State the use of the test pack in IS Audit.
17. What is the meaning of documentation standards? Explain its importance.
18. State the relationship between Systems audit and various management functions.

Answer:

Multiple Choice Questions

1.	(c)	Ensure that the system processes data as it was designed to and that the results are reliable.
2.	(a)	(i) and (ii)
3.	(c)	(i), (ii), and (iii)
4.	(c)	(ii) and (iv)
5.	(c)	Breaks programs into portions at the end of each of which a check point program is executed.
6.	(a)	Inspect the system and check that it is built as per specifications.
7.	(a)	The inputs and the corresponding outputs are compared and checked for correctness.
8.	(c)	Localize the source of an error in a system.
9.	(a)	Auditing programs are designed and used to check a system.
10.	(b)	Determining whether a system is performing as per specifications.
11.	(b)	When a system is initially implemented.
12.	(b)	(i) and (ii)
13.	(b)	Prevent unauthorized access by hackers.
14.	(b)	Protect data and programs from accidental or intentional loss.
15.	(d)	(i), (ii), (iii), (iv), (v), (vi)