Guidance Note on IS Audit – The Institute of Cost Accountants of India (Module - 5 : DISSA Course)

Arijit Chakraborty

March 19 , 2022

Audit Kit

- IT risks include Information Technology Risks at the organizational level, information technology risks at the general control level, and information technology risks at the business process level.
- The Continuous Integration of IT and Business is putting more and more Chie Information Officers (CIOs) under unprecedented pressure. On the one hand, any disturbances in IT may have an impact on IT-Dependent Businesses, which makes CIOs must pay extra attention to any potential risks of IT.
- In terms of responding to IT Risks, **Importance of IT Audits includes 2 levels**:
- The First is to Prevent Risks: IT Audits can help companies identify and prevent risks in the IT systems that support the business, and can also help companies audit IT systems avoid possible risks from external compliance.
- The Second is to Co-operate with the CIO to effectively manage the risks found in the audit and make risk prevention better. IT Auditing first appeared in the FINANCIAL INDUSTRY with deeper IT Applications, and then gradually expanded to other industries.

Guidance Note

- The Goal of IT Audit is to Assist the organization's Information Technology managers to effectively fulfil their responsibilities to achieve the Organization's Information Technology Management Goals.
- The Organization's Information Technology Management Objectives are to ensure that the Organization's Information Technology strategy fully reflects:

✓ *the Organization's Business Strategic Objectives,*

✓ *Improve the Reliability, Stability, Security, and Data Processing Integrity and Accuracy of the Information System on which the Organization Depends, and*

✓ *Improve the Effectiveness and Efficiency of the Information System Operation ensure that the Operation of the Information System Complies with the relevant requirements of Laws, Regulations, and Compliance*.

Approach

- **Guidelines with regard to IS audit Information Systems Audit Policy**
- The IS auditor shall prepare the procedure including the information on how to meet the Standards while performing the IS auditing work. However, the procedure shall not set the requirements for IS auditing.
- IS auditing should be performed by personnel with the required expertise and skills such as Certified Information Systems Auditor, Certified Information Systems, Security Professionals
- Major areas, which will require to be IS audited, are broadly as under:

✓ Safeguarding of Assets.

✓ Data Integrity.

✓ System Effectiveness.

✓ System Efficiency.

✓ Organization and Administration.

- **Safeguarding of Assets**: The IS auditors will require to concentrate on the following areas to ensure that the Information Systems Assets of the organization are safeguarded:

✓ Environmental Security.

✓ Uninterrupted Power Supply.

✓ Electrical Lines.

✓ Data Cables & Networking Products.

✓ Fire Protection.

✓ Insurance of Assets.

✓ Annual Maintenance Contract.

✓ Logical Security & Access Control - Operating System Level.

✓ Logical Security & Access Control – Application System Level.

- **Environmental Security**:
- **Checking**: Central Server Level. The IS auditors should verify whether:
- There is separate room for the server.

✓ Server room has adequate space for operational requirements.

✓ Server room is away from the basement, water / drainage systems.

✓ Server room can be locked and the key being under the custody of the authorized persons (System Administrator) only. Any failed attempts or system tampering as also unscheduled movement in restricted areas, glass breakage or the opening of doors will require to be logged and immediately reported to the Control Staff at the site.

✓ Server is not in close proximity to the UPS room.

✓ Access to server room is restricted to authorized persons and activities in the server room are monitored.

✓ Air-conditioning system provides adequate cooling.

✓ Storage devices to keep stationary and other such items are not kept inside the server room.

- ✓ Smoking, eating and drinking are prohibited in the server room to prevent spillage of food or liquid into sensitive computer equipment.
- ✓ Briefcases, handbags and other packages are restricted from the server room, tape library and other sensitive computer area to prevent unauthorized removal of data held on removable media as also to prevent entry of unacceptable material into the area.
- ✓ Server room is neat and clean to ensure dust free environment.
- ✓ Scanners are kept in safe custody and access is restricted.

Uninterrupted Power Supply:

- **Checking**: Central Server Level and Branch / Department Level. In addition to the availability of the Generator facility at the site, the IS auditor should verify whether:

- ❑ There is a separate enclosure and locking arrangement for the UPS.
- ❑ Maintenance agency provides battery service regularly.
- ❑ There is a regular contract for maintenance of the UPS and the preventive maintenance is carried as per the contract.
- ❑ The record of the tests undertaken is maintained to verify the satisfactory functioning of the UPS.
- ❑ UPS cabin has adequate ventilation to take care of acid fumes emitted by the Lead Acid batteries.
- ❑ Capacity of the UPS system is sufficient to take care of the electricity load required for computers installed.
- ❑ UPS is free of the electricity load relating to the tube-lights, fans, water coolers etc.
- ❑ UPS functions properly when electricity fails.

Electrical lines:

- **Checking**: Central Server Level and Branch / Department Level. The IS auditors should verify whether:

✓ Power supply to computer equipment is through UPS system only.

✓ The electrical wiring looks concealed and is not hanging from ceiling or nodes.

✓ The circuit breaker switches exist in locked condition only.

Data Cables:

- ✓ **Checking**: Central Server Level and Branch / Department Level. The IS auditors should verify whether:
- ✓ A map of the cable layout is kept in a secure place with proper authority. This is helpful in timely and fast repairs of LAN cable faults.
- ✓ Cabling is properly identified and recorded as fiber optic, co-axial, unshielded twisted pair (UTP) or Shielded Twisted Pair (STP).
- ✓ Electrical cable and data cable do not cross each other to avoid possible disturbance during data transfer within the network.

- **Fire Protection**:
- **Checking**: Central Server Level and Branch / Department Level. The IS auditors should verify whether:

✓ Fire alarm system is installed.

✓ Smoke detectors are provided in the server room and in the other areas of computer installations.

✓ Smoke detectors are tested on a regular basis to ensure that they work.

✓ Gas type (Carbon dioxide, Halon etc.) fire extinguishers are installed at strategic places like server room, UPS room and near the nodes and printers.

✓ Dry powder or foam type extinguishers should not be used as they tend to leave deposits.

✓ Staff knows how to use the fire extinguishers.

✓ Fire extinguishers are regularly refilled / maintained.

✓ An evacuation plan is documented and rehearsed at regular intervals for taking immediate action in the case of the outbreak of fire

- **Insurance**:
- **Checking**: Central Server Level. The IS auditors should verify whether:

✓ All the computer equipment's are covered under the appropriate electronic equipment insurance policy with a reputed insurance firm.

✓ A record of the original policy is maintained with the detailed list of the equipment covered under the policy.

✓ Information regarding shifting of computer equipment to or from or within the department / office is conveyed to the insurance firm.

✓ Adequacy of the insurance cover should be verified as per the policy of the organization.

- **Annual Maintenance Contract**:
- **Checking**: Central Server Level and Branch / Department Level. The IS auditors should verify whether:

✓ Stamped agreements for maintenance contract are executed and available.

✓ Activities carried out during maintenance have been reported in the registers and duly authenticated.

✓ Contract renewal rates are maintained in the register.

✓ Access for maintenance purpose is granted only on verifying the identity of the service person.

✓ The maintenance staff support is available in time.

Logical Security & Access Control – Operating System

- **Checking**: Central Server Level, Dept. of Information Technology Level and Branch / Department Level. The IS auditors should verify whether:

✓ Access to the systems is only through password protected user IDs.

✓ Operating System (OS) allots unique user identity (ID) for all users.

✓ OS provides for different levels of access rights to volumes, directories and files.

✓ OS prompts for change of the user password after the lapse of specified periods.

✓ OS ensures secrecy and security of the user passwords & access rights granted to a user.

✓ Unrestricted access to the systems is provided only to the System Administrator.

✓ Administration level access is restricted to authorized and limited persons.

✓ All the security features available in the OS are enabled / taken advantage of as far as possible for ensuring better security.

- ✓ Administration access should not be available to the officials who are under notice period, retiring shortly, under disciplinary action etc.
- ✓ OS provides for loading of virus prevention software and is implemented.
- ✓ Record is maintained and authenticated regarding the installation of the Operating System, it's up-gradation, re-installation and maintenance.
- ✓ A register is maintained in respect of all the OS level users, giving the details such as the date of creation, suspension, cancellation, access rights granted, purpose of creation etc.
- ✓ Users created for audit / maintenance purpose are disabled immediately after work is over.
- ✓ The department reviews the number of the OS level users periodically.

Logical Security & Access Control – Application System

- **Checking**: Dept. of Information Technology Level and Branch / Department Level. The IS auditors should verify whether:

- ❑ System provides for unique user IDs and password for all users.
- ❑ System provides for different levels of access.
- ❑ System prompts for change of user password after lapse of specified period.
- ❑ System ensures secrecy and security of the user passwords and the access rights granted to users.
- ❑ Unrestricted access to the entire application system menus is provided only to a Super User.
- ❑ Super User access in application level is not given to staff who is under notice period, retiring shortly, under disciplinary action etc.
- ❑ The application system user list is periodically reviewed.

Data Integrity:

- **Checking**: Central Server Level and Dept. of Information Technology Level. The IS auditor will require to address, among others, the following areas under IS auditing:
- Data Input Controls.
- Data Processing Controls.
- Patch Programs.
- Purging of Data Files.
- Backup of data.
- Restoration of Data.
- Output Reports.
- Virus Protection.

- **Back up of Data**: The IS auditors should verify whether:

✓ All the floppies / CDs / tapes, purchased, pertaining to the OS software, application software and utility programs, drivers etc. are recorded in a register and properly stored.

✓ Hardware, software, operating system, printer manuals are properly labelled and maintained.

✓ Latest user manuals of the application software and other end-user packages running on the system are available for guidance.

✓ Daily / weekly / monthly and quarterly back-up of data is taken without fail and is available (as per requirement).

✓ Backup tapes are properly labeled and numbered.

✓ Proper storage procedures and facilities are in place for backup copies.

- **Virus Protection**: The IS auditors should verify whether:

❑ Anti-virus software is loaded in the system.

❑ Anti-virus software is regularly updated to cover software updates against the latest viruses.

❑ All extraneous floppies are checked for virus including the floppies carried by the IS auditors.

- **Cyber Security**:

- ❑ Verify the Cyber Security Policy of the Bank with reference to the framework and strategy to check cyber threats depending on the level of complexity of business and acceptable levels of risks and the measures to address / reduce the said risks.
- ❑ Verify if the IT architecture / framework - network, server, database and application, end user systems, etc., takes care of security measures at all times.
- ❑ Review of the security measures by the Board or IT sub-committee of the Board periodically.
- ❑ Verify if the BCP / DR arrangements / policy in place includes procedures to be followed in case of cyber risks.
- ❑ Verify the detective and corrective measures / steps in place to address various types of cyber threats in services offered by the Bank – NEFT / RTGS / IMPS / SWIFT / debit cards, etc.

- **Inventory Management of Business IT Assets**
- Financial Institutions should maintain an up-to-date business IT Asset Inventory Register containing the following fields, as a minimum:
- Details of the IT Asset (viz., hardware / software / network devices, key personnel, services, etc.).
- Details of systems where customer data are stored.
- Associated business applications, if any.
- Criticality of the IT asset (For example, High / Medium / Low).
- Classify data / information based on sensitivity criteria of the information

- **Secure Configuration**
- The firewall configurations should be set to the highest security level and evaluation of critical device (such as firewall, network switches, security devices, etc.) configurations should be done periodically.
- Systems such as Network, application, database and servers should be used dedicatedly for the purpose for which they have been set up.
- **Anti-virus and Patch Management**
- Put in place systems and processes to identify, track, manage and monitor the status of patches to servers, operating system and application software running at the systems used by the Financial Institution officials (end-users).
- Implement and update antivirus protection for all servers and applicable end points preferably through a centralized system

- **Secure Mail and Messaging Systems**
- Implement secure mail and messaging systems, including those used by Financial Institution's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.
- Document and implement email server specific controls.
- **Removable Media**
- As a default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorized for defined use and duration of use.
- Secure the usage of removable media on workstations / PCs / Laptops, etc. and secure erasure / deletion of data on such media after use.
- Get the removable media scanned for malware / anti-virus prior to providing read / write access.

- **Customer Education and Awareness**
- Improve and maintain customer awareness and education with regard to cyber security risks.
- Educate the customers on keeping their card, PIN etc. secure and not to share with any third party.
- **Backup and Restoration**
- Take periodic back up of the important data and store this data 'off line' (i.e., transferring important files to a storage device that can be detached from a computer / system after copying all the files).
- **Vendor / Outsourcing Risk Management**
- All the outsourcing service level agreements (SLAs) signed with the vendors must clearly mention the responsibility of the Financial Institution and vendor in case of any failure of services.
- The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints.
- Vendors' service level agreements shall be periodically reviewed for performance in security controls

- **Human Resources**:
- Recruitment Policy and Procedures for Staff.
- Formal Organization Chart and defined job description prepared and reviewed regularly.
- Proper Segregation of Duties maintained and reviewed regularly.
- Prevention of unauthorized access of Former Employees.
- Close Supervision of Staff in sensitive position.
- People on Notice period moved in non-sensitive role.
- Dismissed Staff to be removed from premises with immediate effect
- **IT Financial Control**:
- Comprehensive Outsourcing Policy.
- Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security lapse in the Vendor Contract.
- Periodic review of Financial and Operational Condition of service provider with emphasis to Performance Standards, Confidentiality and Security, Business Continuity Preparedness.
- Contract clauses for Vendor to allow RBI or Personnel authorized by RBI access relevant Information / Records within reasonable frame of time.

- **Inventory and Information / Data Classification**: Effective control requires a detailed inventory of information assets. Such a list is the first step in classifying the assets and determining the level of protection to be provided to each asset.
- The inventory record of each information asset should, at the least, include:
- A clear and distinct identification of the asset.
- Its relative value to the organization.
- Its location.
- Its security / risk classification.
- Its asset group (where the asset forms part of a larger information system).
- Its owner.
- Its designated custodian.

- **Security Measures Against Malware**:
- Malicious software is an integral and a dangerous aspect of internet-based threats which target end-users and organizations through modes like web browsing, email attachments, mobile devices, and other vectors. Malicious code may tamper with a system's contents, and capture sensitive data. It can also spread to other systems. Modern malware aims to avoid signature-based and behavioral detection, and may disable anti-virus tools running on the targeted system. Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against these threats by attempting to detect malware and block their execution
- Typical controls to protect against malicious code use layered combinations of technology, policies and procedures and training. The controls are of the preventive and detective / corrective in nature. Controls are applied at the host, network, and user levels:

RPA Definition

Robotic Process Automation (RPA) = innovative solution **for fully automatic handling of business processes** with high volume & repetitive nature

- **RPA = integrated in existing IT infrastructure**
- Software robot = access to diverse applications with ID / password.
- Robot can gather information / change data.
- **Result -** Automation of business processes

Objectives of RPA

- Key objectives of implementing RPA -
- Ÿ Improve customer experience
- Ÿ Improve accuracy
- Ÿ Manage controls
- Ÿ Higher efficiency
- Ÿ Reduction of monotonous work
- Ÿ Cost saving
- Ÿ Skill upgradation of personnel

RPA Use Cases- Finance

- ► Operational accounting (billing & collections, AP, AR
- ► General accounting (allocations & adjustments, journal entry
- ► Processing, reconciliations, intercompany transactions & close)
- ► Financial & external reporting
- ► Planning, budgeting & forecasting
- ► Treasury processes

RPA -Tax

- Analyse account changes & evaluate potential tax impact
- Populate tax returns with financial data
- Automated import of financial tax workbook into tax return forms (using tax return software)
- Complete non-financial tax return line items & information fields
- Execute work-flow processes for tax returns & initiate electronic estimated payments
- Submit tax returns & related payments.
- **Contracts :**
- RPA = leverage Natural Language Processing (NLP),
- schedule invoices by NPL
- can load & identify functional information from fee schedules of contracts & invoices

Capabilities of RPA

- RPA bots can use OS applications like a human user.
- Bots = capable of copying most user actions:
- ***Launching and using various applications including***

1. Opening emails & attachments
2. Logging into applications
3. Moving files & folders

- ***Integrating with enterprise tools by***

1. Connecting to system APIs
2. Reading & writing to databases

- ***Augmenting data by***
- Scraping data from web including social media

RPA= Potential benefits

- **Efficiency and quality**
- Human errors = eliminated.
- enhances compliances/ auditability & results in higher staff satisfaction.
- Capacity increase by robotics virtual workforce & organisations can refocus on staff for better services.
- **Productivity boost**
- Average handling time is reduced.
- Monitoring is performed round the clock.
- It results in development of new competencies.

Technology : Set up RPA Bots

- **Setting up Instructions**
- Developer gives detailed instructions to robots to perform & interact with Robot Controller Library.
- **Robot Controller**
- Core RPA Software = used to give jobs to robots & monitor their activities
- **Robots**
- machine or desktop or virtual system - interacts directly with Robot Controller & Business Applications.
- **Business Users**
- review work of robots & resolves any exception , escalates, if required for resolution.