Digital Auditing and Assurance

(Part-1) Auditing ____ Digitally _____

Concept of Auditing Digitally

- Auditing Digitally is using advancements in technology for conducting an effective and efficient audit. With a rapidly growing IT environment it is essential to adapt technology in auditing, practices.
- Auditing digitally involves conducting the audit through automation and innovation with the help of new technologies to capture data, automate procedures, analyse information and focus on the real risks of the client. (Thankyouu)

Expectations from an Auditor

- Audit teams need to involve the experts on different software applications and technologies.
- Having the right level of expertise of new technology (such as RPA, AI, blockchain technology) allows auditors to provide the highest quality of audit.
- More focus to be put on developing and using tools to automate and enhance existing processes, such as data analytics and collaboration and sharing tools, which help to drive quality in audits today.

Key Features or Advantages of Auditing Digitally

(i) **Improved Quality of Audits:** Through automation, data analytics techniques, auditor can easily move from sample auditing to full population of transactions being reviewed or re-performed.

(ii) **Decreasing human dependency:** Using technology minimizes the manual intervention which ultimately results in reducing the risk of manual errors.

(iii) **Increases Transparency:** New ERPs and tools have audit trail feature available to trace the transaction end to end.

(iv) **Automation and Ease:** Automating tasks like extracting data and sampling have improved the quality of audit and reduced the manual error.

(v) **Improved Efficiency:** What used to take weeks to learn and program, is now easily available to auditors after some simple training and digital upskilling which increases efficiency.

(vi) **Better risk assessment:** With usage of automation and technology in audit, auditor may focus on the real challenges and assess the potential risk precisely. It gives time to auditors to focus on the bigger picture rather than being involved with repetitive tasks.

Considerations in Auditing

(1) Identifying the problems to be solved

- Continuously evaluate the emerging technologies and latest tools to see what can benefit the audit.

- Think about what would make the audit easier.

(2) Identifying the technology that help can auditor

- There are a number of tools available and many vendors and start-ups using data acquisition, manipulation and visualization tools.
- Consider how comfortably these solutions will integrate into auditor current processes and flag any potential implementation issues early on.

(3) How to upskill team members

Technology is only as good as the people using it. Training and development are critical to ensure teams understand how and why they are using the technology. Reluctance to change is obvious, however continuous training help them to get better.

(4) Range of automated solutions

There is a range of automation solutions, from low to high sophistication, which helps to standardize the repeatable tasks and optimize the efforts resulting in doing better.

(Part-2) Digital ____ Audit _____

Digital Audit

Placing **assurance** on effectiveness of IT systems implemented in an organization (Auditee)

Key Features of a Digital Audit (Client ke perspective se socho)

- Digital audit encourages auditee to use the latest **technological advancements**.
- It can help auditee to make **informed decisions**.
- Digital audit improves quality of opinion and leads to a more **reliable audit report**.
- Digital audit will help create a **future for a digital strategy** & paves way for adopting new technologies such as AI and Robotic, usage of analytics and automation.
- Digital Audit allows to **standardize processes**.
- Digital audit helps organization in more comprehensive overview of **end-to-end processes**.
- Digital Audit leads to **savings in time, cost and human effort** which can be utilized towards more productive tasks.

Advantages of Digital Audit

(i) **Better Audit Quality:** Technology can correctly evaluate massive volumes of data quickly. This can assist auditors in determining the areas that require more testing.

(ii) **Better Analytics:** Improved analytics capabilities help management and auditors in seeing trends and patterns that may be challenging to spot manually.

(iii) **Improved Risk Assessment:** Management and auditors put their testing efforts in areas with a higher risk of material misstatement and make informed decisions.

(iv) **Enhanced Effectiveness & Efficiency:** With use of tools & automation techniques, processes can be standardized and routine tasks can be automated e.g. automating a reconciliation process increase efficiency and saves time & costs.

(v) **Lower Costs:** By automating processes that were previously done manually, technology can assist with the cost of auditing. This may shorten the time needed to complete an audit, which may lower the audit's overall cost.

Challenges of Digital Audit

- Reluctance to change.
- Challenges with data security and governance.
- Choosing the right tool and automating the right process.
- Ensuring standardisation and correct configurations to avoid error and bias.
- Evaluating business benefits the organization wants to achieve with automation and
- Roadmap for digital strategy.

Consideration Of Digital Audit

Auditor is required to obtain an understanding of management's implementation of new Audit technologies and perform procedures to understand changes to company's business, including any changes to IT environment. Areas of focus could include understanding the following:

- New activities or changes to existing processes due to new technology (e.g., new revenue streams, changes in the roles and responsibilities of entity personnel, automation of manual tasks etc.).
- Changes in the way the entity's systems are developed and maintained and whether these changes introduce new risks and require new controls to respond to those risks.
- Impact of new technology as to how the organization obtains and uses relevant, quality information to support functioning of internal control

Understand the IT Environment

Understanding of Automated Environment

As required by SA 315, auditor is required to obtain understanding of entity & its environment. In an automated environment, auditor is required to obtain an understating of the following:

- Applications being used by the entity;
- IT infrastructure components for each of the application;
- Organisation structure and governance;
- Policies, procedures and processes followed;
- Extent of IT Integration, use of service organisation;
- IT risks and controls.

Stages involved in understanding the IT Environment

1. Understand
2. Identify
3. Assess

Documenting the understanding

Auditor is required to document understanding of automated environment. Example given below illustrates how auditor can document details of an automated environment:

Application	Used for	Database	Operating System	Network	Server and Storage
SAP ECC/ HANA	Integrated application software	Oracle 19c	HP-UX LAN	WAN	HP Server and NAS
REVS	Front Desk, Guest Reservations	MS-SQL Server 2018	Windows 2016 Server	In-house developed	HP Server Internal HDD
KOTS	Restaurant and Kitchen Orders	MS-SQL Server 2018	Windows 2016 Server	In-house developed	HP Server Internal HDD
BILLSYS	Billing	Oracle 12c	Windows 2016 Server	Packaged Software	HP Server Internal HDD

Key Areas for an Auditor to Understand IT Environment

(1) Understand flow of transaction

Focus on identifying and understanding nature and number of specific IT applications and other aspects of IT environment that are relevant to flows of transactions and processing of information in information system.

(2) Identification of Significant Systems

Identify the IT applications and supporting IT infrastructure concurrently with understanding of how information relating to significant classes of transactions, account balances and disclosures flows into, through and out entity's information system.

(3) Identification of Manual and Automated Controls

- Entity's system of internal control contains manual & automated elements. An entity's mix of manual and automated elements varies with the nature & complexity of entity's use of IT.
- Characteristics of manual or automated elements are relevant to auditor's identification and assessment of the RMM.

(4) Identification of technologies used

- Understand emerging technologies implemented and the role they play in entity's information processing or other financial reporting activities and consider whether there are risks arising from their use.
- There is increased likelihood that ET may decide to engage experts to help understand whether and how the use of emerging technologies impacts the entity's financial reporting processes and may give rise to risks from the use of IT.

Examples of emerging technologies

(i) Blockchain, including cryptocurrency businesses (e.g., token issuers, custodial services, exchanges, miners, investors)

(ii) Robotics

(iii) Artificial Intelligence

(iv) Internet of Things

(v) Biometrics

(vi) Drone

Assessing complexity of IT environment

Level of complexity differs across applications. Complexity is based on the following factors:

(i) automation used in the organization, entity's reliance on system generated reports,

(ii) customization in IT applications,

(iii) business model of the entity,

(iv) any significant changes done during the year and

(v) implementation of emerging technologies.

Identifying the Risks arising from usage of IT

How to identify IT Risks

- In identifying risks arising from use of IT, auditor may consider nature of identified IT application.
- Applicable risks arising from the use of IT may also be identified related to cyber security.
- It is more likely that there will be more risks arising from use of IT when volume or complexity of automated application controls is higher, and management is placing greater reliance on those controls for effective processing of transactions or the effective maintenance of the integrity of underlying information.

Risks arising from use of IT

(i) Unauthorized access to data that may result in destruction of data or improper changes to data, including recording of unauthorized or non-existent transactions, or inaccurate recording of transactions.

(ii) Possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.

(iii) Unauthorized changes to data in master files.

(iv) Unauthorized changes to IT applications or other aspects of the IT environment.

(v) Failure to make necessary update IT applications or other aspects of the IT environment.

(vi) Inappropriate manual intervention.

(vii) Data loss or data corruption.

(viii) Risk of system downtime caused by hardware failures, faulty configurations, cyberattacks or power outage.

(ix) Risks associated with system integration and compatibility.

(x) Risk of regulatory compliances. Any change in the law, order, guidelines or agreements will impact the business, its related costs, investments etc.

IT dependencies

(1) Importance of Identification of IT Dependencies

(i) To identify the entity's reliance upon IT,

(ii) To understand how IT is integrated into the entity's business model

(iii) To identify potential risks arising from the use of IT,

(iv) To identify related IT General Controls and

(v) To enable an effective and efficient audit approach.

(2) How IT dependencies arise

IT Dependencies are created when IT is used to initiate, authorize, record, process, or report transactions or other financial data for inclusion in F.S.

(3) Types of IT dependencies

(i) Automated Controls

Automated controls are designed in IT environment to enforce business rules. For example: Purchase order approval through -

- Format checks (e.g., only a particular date format is accepted),
- Existence checks (e.g., Duplicate customer number cannot exist), and/or
- Reasonableness checks (e.g., maximum payment amount)

(ii) Reports

System generated reports (e.g. Customer Ageing Report) are used for execution of manual control, including business performance reviews, or may be the source of entity information used by auditor while selecting items for testing, performing substantive tests of details or a substantive analytical procedure.

(iii) Calculations

Accounting procedures performed by IT system instead of a person. For example, calculation of depreciation, charging interest in delayed payments, etc.

(iv) Security

Security including segregation of duties is enabled by IT environment to restrict access to information.

(v) Interfaces

Programmed logic that transfer data from one IT system to another. For example, an interface may be programmed to transfer data from a payroll subledger to the general ledger.

Understanding & responding to risks arising from IT dependencies

Auditors need to understand how management responds to the associated risks that may arise from IT Dependencies. Management may implement General IT Controls to address risks related to IT dependencies. General IT Controls maintain the integrity of information and security of data and commonly include controls over the following:

(i) Access security.
(ii) Program change.
(iii) Data center and network operations.

Control Objectives and Controls for each area of General IT Controls

(1) Objectives & Activities of Access Security

Objective: To ensure that access to programs and data is authenticated and authorized to meet financial reporting objectives.

Activities:

- Access requests to application are properly reviewed and authorized by management
- Access of terminated user is removed on a timely basis.
- Access rights to applications are periodically monitored for appropriateness.
- Transactions of administrative and sensitive generic IDs are monitored.
- Security policies are procedures are maintained.
- Access to operating system and database is restricted.

(2) Objectives & Activities of Program Change

Objective: To ensure that modified systems continue to meet financial reporting objectives.

Activities:

- Change Management policy and procedures are maintained.
- Development, testing & production environments are segregated for changes to application configurations.
- Changes are adequately tracked and recorded.
- Changes to application configurations are adequately tested and approved before being migrated into production.
- Emergency changes are approved.
- Segregation of duties is maintained between developer and implementor.

(3) Objectives & Activities of Data Center & Network & operations

Objective: To ensure that production systems are processed to meet financial reporting objectives.

Activities:

- Policies and procedures for data back and recovery is maintained.
- Data is appropriately backed up and recoverable.
- Restoration testing is performed.
- Monitoring and compliance of service level agreements.
- Batch job scheduled are monitored for failures and access is restricted.

Assessing Cyber Risks

Cyber Risk

- Risk of damage, steal, expose, alter, disable or destroy of data due to Cyber Attack is known as Cyber Risk.
- Cyber-attack is an attempt to gain unauthorized access to a computing system or network with intent to cause damage, steal, expose, alter, disable, or destroy data.

Types of Cyber Risk

(1) Malware

Any program that is created with the intent to do harm to a computer, network or server. Its subsets are:

(i) **Ransomware:** An adversary encrypts a victim's data and offers to provide a decryption key in exchange for a payment.

(ii) **Fileless Malware:** A malicious activity that uses native, legitimate tools built into a system to execute a cyber-attack. Fileless malware does not require to install any code on a target's system, making it hard to detect.

(iii) **Trojan:** A malware that appears to be legitimate software disguised as native operating system programs or harmless files like free downloads.

(iv) **Mobile Malware:** Malware designed to target mobile devices. Mobile malware is delivered through malicious downloads, operating system vulnerabilities and use of unsecured Wi-Fi.

(2) Denial-of-Service (DoS) Attacks

- Targeted attack that floods a network with false requests in order to disrupt business operations. Users are unable to perform routine & necessary tasks, such as accessing email, websites or other resources that are operated by a compromised computer or network.
- While most DoS attacks do not result in lost data & are typically resolves without paying a ransom, they cost the organization time, money and other resources in order to restore critical business operations.

(3) Phishing

Cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information, such as passwords or account numbers or to download a malicious file that will install viruses on their computer or phone. Its subsets are:

(i) **Spear Phishing:** Phishing attack that targets specific individuals typically through malicious emails to steal sensitive information such as login credentials or infect the targets' device with malware.

(ii) **Whaling:** Social engineering attack specifically targeting senior or C level executive employees to steal money or information or gaining access to person's computer in order to execute further cyberattacks.

(iii) **SMiShing:** Social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information. Or sending money to cybercriminals.

(iv) **Vishing:** Voice phishing attack, is the fraudulent use of phone calls and voice messages pretending to be from a reputable organization to convince individuals to reveal private information such as bank details and passwords.

(4) Spoofing

A technique through which a cybercriminal disguises themselves as a known or trusted source. In so doing, adversary is able to engage with the target and access their systems or devices with ultimate goal of stealing information. Extorting money or installing malware or other harmful software on the device. Its subsets are:

(i) **Domain Spoofing:** Attacker impersonates a known business or person with fake website or email domain to fool people into the trusting them. Typically, the domain appears to be legitimate at first glance, but a closer look will reveal subtle differences.

(ii) **Email Spoofing:** Cyberattack that targets businesses by using emails with forged sender addresses. Because the recipient trusts the alleged sender, they are more likely to open the email and interact with its contents, such as a malicious link or attachment.

(5) Identity-based Attacks

Valid user's credentials have been compromised and an adversary is pretend to be that user. For e.g., people often use the same user ID and password across multiple accounts. Therefore, possessing the credentials for one account may be able to grant access to other, unrelated account.

(6) Insider Threats

It occurs when a current or former employee is having direct access to the company network, sensitive data, and intellectual property (IP), as well as knowledge of business processes, company policies or other information that would help carry out such an attack.

(7) Domain Name System (DNS) Tunneling

- Cyberattack that leverages DNS queries & responses to bypass traditional security measures and transmit data and code within the network.
- This tunnel gives hacker a route to unleash malware and/or to extract data. IP or other sensitive information by encoding it bit by bit in a series of DNS responses.

(8) loT-Based Attacks

Cyberattack that targets an Internet of Things (IoT) device or network. Once compromised, the hacker can assume control of the device, steal data, or join a group of infected devices.

Stages of Cyber Risks

(1) Stage 1

Assessing the Cyber Risk

(i) Every organization should consider certain common threats like:

(ii) Ransomware disabling their organization (including their plants and manufacturing facilities).

(iii) Common criminals using email phishing and hacks for fraud and theft.

(iv) Insiders committing malicious activities resulting in unintended discourse of information theft and frauds.

(2) Stage 2

Impact of Cyber Risk

Impact of attack vary from organization to organization and most importantly from an attack to attack. Some of the indicative areas are:

- Regulatory costs.
- Business interruptions causing an operational challenge for an organization.
- Data loss, reputational loss and litigation.
- Ransomware – more common these days where entire systems are encrypted.
- IP theft which may not only take the competitive advantage, but may also result in any impairment charge because of the loss of IP.
- Incident response cost which could be for investigations & remediations.
- Breach of Privacy, if personal data of a consumer is hacked it could have a significant impact on the organization.
- Fines and penalties

(3) Stage 3

Managing the Cyber Risk

A strategic approach to cyber risk management can help an organization to:

(i) Gain a holistic understanding of cyber risks, threats facing their organization & other financial institutions.

(ii) Assess existing IT and cybersecurity program and capabilities against the relevant regulatory requirements.

(iii) Align cybersecurity & IT transformation initiatives with strategic objectives and critical risks.

(iv) Understand accepted risks & documented compensating controls.

Cyber Security Framework

It includes how management is identifying the risk, protecting and safeguarding its assets from the risk, management preparedness to detect the attacks, anomalies and responsiveness to the adverse event.

Risk Management Process

(1) Step 1: Identify the Risk

(i) **Risk Assessment & Management Strategy:** Entity should conduct a periodic risk assessment & develop a management strategy which identifies cybersecurity risks around IT system.

(ii) **Asset Management:** Entity should maintain and periodically reviews an inventory of their information assets (e.g., intellectual property, patents, copyrighted material, trade secrets and other intangibles).

(iii) **Governance:** Management should review how cybersecurity risks affect internal controls over financial reporting.

(iv) **Business Environment:** To determine overall responsibility for cybersecurity, entity should establish roles & responsibilities over cybersecurity (CISO, CIO).

(2) Step-2: Protect the Risk

(i) **Unauthorised Access:** Entity should monitor whether there has been unauthorized access to electronic assets and any related impact on financial reporting.

(ii) **Training:** Formal training should be conducted to make the teams aware of the risk associated with cyberattacks.

(iii) **Data Security:** Entity should implement effective controls for data security.

(3) Step-3: Detect the Risk

Entity should have controls and procedures that enable it to -

- identify cybersecurity risks and incidents
- to assess & analyse impact of such risks & incidents on entity's business,
- evaluate the significance associated with such risks and incidents, and
- consider timely disclosures.

(4) Step 4: Respond to the Risk

(i) **Response Planning:** Entity should have a response planning in place to capture the details of nature of incident.

(ii) **Communication:** Response Plan needs to be communicated with those who are ultimately responsible for this framework and with TCWG.

(iii) **Mitigation Process:** Management should assess Litigation costs Regulatory investigation costs and Remediation costs as a part of mitigation process.

(5) Step 5: Recover from Risk

(i) **Recovery Plan:** Once impact evaluated & communicated with regulators, recovery plan needs to be implemented to overcome the impact.

(ii) **Improvements:** Necessary improvements like patch upgrades, better controls, improved technology in terms of firewall, anti-virus, tools etc. needs to be implemented to safeguard the entity.

Control considerations for Cyber Risks

(1) Controls around vendor setup and modifications

- Who is responsible for making changes to vendor master data? Is the process centralized or decentralized?
- Are other communication channels, such as email, used to request changes to vendor master data? (If yes, consider if multi-factor authentication is enabled for email).
- What systems and technologies are used to initiate, authorize and process requests related to changes to vendor master data?
- Are authentication protocols defined to verify modifications to vendor master data (e.g., call back procedures, multi-factor authentication)?

(2) Controls around electronic transfer of funds

- Are personnel responsible for wire transfers educated on relevant threats and information related to common phishing scams associated with fraudulent requests for wire transfers?
- Are authentication protocols defined to verify wire transfer requests (e.g., call back procedures, dual-authentication procedures)?
- What systems and technologies are used to facilitate the request/initiation, authorization and release of wire transfers?

(3) Controls around patch management

- Does the entity have a patch management program?
- Does the entity run periodic vulnerability scans to identify missing/unapplied patches?
- How is the entity notified of patches external vendors (e.g., Microsoft for Windows patches)?

Remote Audit Meaning / Virtual Audit

(1) Meaning

- Using online or electronic means to conduct the audit. It may be partially or completely virtual.
- Auditor uses technology to obtain audit evidence or to perform documentation review with the participation of the auditee.

(2) Considerations

(i) Feasibility and Planning

- Planning involves agreeing on audit timelines, meeting platform (Zoom calls/ Microsoft Teams/Google Meet) to be used for audit sessions, data exchange mechanisms, any access authorization requests.
- Ensure feasibility of use of technology, if auditors & auditees have competencies and resources are available.
- Execution phases involve video/tele conferencing with auditees.

- Documentation for audit evidence should be transferred through a document sharing platform.

(ii) Confidentiality, Security and Data Protection

- To ensure data security and confidentiality, access to document sharing platform should be sufficiently restricted and secured by encrypting the data that is sent across the network.
- Information, once reviewed & documented by auditor, is removed from the platform, and stored according to applicable archiving standards and data protection requirements.
- Auditors should take into consideration legislation and regulations.
- Any screenshots of documents or records or other kind of evidence should be previously authorized by the audited organization.
- In case of accessing the auditee's IT system, auditor should use VPN (Virtual private network).

(iii) Risk assessment

- Risks for achieving audit objectives are identified, assessed and managed.
- Assessment whether remote audit would be sufficient to achieve audit objectives should be done & documented.

(3) Advantages of Remote Audit

- Cost and time effective: No travel time and travel costs involved.
- Comfort and flexibility to audit team.
- Time required to gather evidence can spread over several weeks, instead of concentrated into a small period.
- Auditor can get first-hand evidence directly from the IT system.
- Widens the selection of auditors from global network of experts.

(4) Disadvantages of Remote Audit

- Due to network issues, interviews and meetings can be interrupted.
- Limited or no ability to visualize facility culture of the organization, and the body language of the auditees.
- Opportunity to present doctored documents and to omit relevant information is increased.
- Remote access to sensitive IT systems may not be allowed.
- Cultural challenges for the auditor. Lack of knowledge for local laws and regulations could impact audit.
- Audit procedures like physical verification of assets and stock taking cannot be performed.

Emerging Technologies in Audit

Data Analytic Techniques

(1) Meaning and Concept

- Generating and preparing meaningful information from raw system data using processes, tools, and techniques is known as Data Analytics
- It involves analyzing large sets of data to find actionable insights, trends, draw conclusions and for informed decision making,
- Use of audit analytics enables greater efficiencies and more accurate findings from the review process.
- It allows auditors to audit more effectively, large amounts of data held and processed in IT systems.

NOTE

Data analytics methods used in an audit are known as Computer Assisted Auditing Techniques or CAATs.

It involves use of multiple data analytical tool that help auditor to deep dive into the problem statement & hence increase audit quality.

(2) Benefits

Audit analytics helps:

(i) To discover and analyze patterns.
(ii) Identifying anomalies.
(iii) Extract other useful information in data

Tools used as Part of CAATs

(1) Audit Command Language (ACL)

- ACL Analytics is a data extraction and analysis software used for fraud detection and prevention and risk management.
- It samples large data sets to find irregularities or patterns in transactions that could indicate control weaknesses or fraud.
- ACL (Audit Command Language) is used to analyse and check complete data sets to perform Trial Balance reconciliations during the Audits. In such case scenarios, entity provided the GL dump & system Trial Balance.

(2) Alteryx

- Alteryx is used to consolidate financial or operational data to assess controls.
- **Example:** Alteryx used for logistics organization to recompute revenue entries recorded by system to match with the financials that showcased expected revenue turnover.

  Due to Alteryx's processing speed and ease to implement functions, auditors could perform re-computation for all the transactions entry and noted that revenue was being

understated as expected revenue was more than actual calculated. This was due to the fact that addendum between logistic company and client was not revised in the system and old versions of rates were used to compute the revenue. Alteryx helped in analysing and recomputing the huge data set and to focus on actual risk.

(3) Power BI

- Power Bi is a business intelligence (BI) platform that provides nontechnical business users with tools for aggregating, analyzing, visualizing and sharing data.
- From audit perspective, such visualization tools can be used to find the outliers in the population.
- **Example:** Auditors were required to analyse the trends of sales during the year. With use of Power BI, sales data provided by the client was further converted into dashboard to analyse the trends and patterns as per the market standards.

(4) CaseWare

- CaseWare is a data analysis software & provide tools that helps in conducting audit and assurance engagements quickly, accurately and consistently.
- It shares analytical insights which help in taking better informed decisions.
- Used by accounting firms, governments and corporations worldwide, this trusted platform integrates everything, an auditor need to conduct assurance and reporting engagements.

(a) Examples of Tests that can be performed with CAATs

1. **Identify exceptions:** Identify exceptional transactions based on set criteria. For example, cash transactions above 10,000.
2. **Identify errors:** Identify data, which is inconsistent or erroneous. For e.g.: account number which is not numeric.
3. **Verify calculations:** Re-perform various computations in audit software to confirm the results from application software confirm with the audit software. For e.g.: TDS rate applied as per criteria.
4. **Existence of records:** Identify fields, which have null values. For example: invoices which do not have vendor name.
5. **Data completeness:** Identify whether all fields have valid data. For example: null values in any key field such as date, invoice number or value or name.
6. **Data consistency:** Identify data, which are not consistent with the regular format. For example: invoices which are not in the required sequence.
7. **Duplicate payments:** Establish relationship between two or more tables as required. For example, duplicate payment for same invoice.
8. **Accounts exceeding authorized limit:** Identify data beyond specified limit. For example, transactions entered by user beyond their authorized limit or payment to vendor beyond amount due or overdraft allowed beyond limit.

Automated Tools in Audit

Internet of Things (IoT)

(1) Concept

(i) Connecting any device (cell phones, coffee makers, washing machines, and so on) to the internet. Key components of IoT are data collection, analytics, connectivity, people and process.

(ii) IoT not only changes business model, but also affects strategic objectives of the organization.

(iii) Researchers uses loT devices to gather data about customer preferences and behavior, though that can have serious implications for privacy and security.

(iv) **Examples:** Connected Cars, connected manufacturing equipment's, smart home security.

(2) Audit Implications

- Auditors not being able to rely only on manual controls. Auditor need to scope new systems into the audit.
- Audit firms need to train & upskill auditors to evaluate the design & operating effectiveness of automated controls.
- Consumer-facing tools that connect to business environments in new ways can impact the flow of transactions & introduce new risks for management and auditors to consider.
- Auditors need to consider volume of the transactions, processes and controls related to it.

(3) Common Risk

(i) Device hijacking;
(ii) Data siphoning;
(iii) Denial of Service (DoS) attacks;
(iv) Data breaches; and
(v) Device theft.

Artificial Intelligence (AI)

(1) Concept

- AI refers to a system that can think and learn. Al systems utilize data analysis & algorithms to make decisions based on predictive methods. Complex algorithms are developed to propose decisions based on a pattern or behavior learned over time.
- **Examples:** Self-driving cars, manufacturing robots, smart assistants, marketing chatbots, virtual travel booking agent.

AI to predict when to book the lowest prices for flights, hotels, car and vacation home rentals. Using historical flight and hotel data, Al will also recommend to user whether booking has reached its lowest price point or if the user should hold out a bit longer for the price to drop.

(2) Audit Implications

(i) **Logical Flow of Process:** Auditor must focus on the logical flow of processes. Auditors should confirm their understanding of how the use of AI affects the entity's flows of transactions, including the generation of reports or analytics used by management.

(ii) **Assessing Effectiveness of Algorithms:** Auditors should assess effectiveness of algorithms & whether their output is appropriately reviewed and approved.

(iii) **AI Functionality:** Auditors need to consider cybersecurity and search for possible bugs and vulnerabilities that can be exploited to impact AI functionality.

(iv) **Decision Making process:** Auditors also should consider whether the AI is making decisions or being utilized by management as part of the decision-making process.

(3) Common Risk

(i) **Security:** More data the system uses, from more sources; more entry points and connections are formed and greater the potential risks.

(ii) **Inappropriate configuration:** AI may also be used to diagnose medical conditions. If it is badly configured or malfunctions, it could harm people before the problem is spotted.

(iii) **Data Privacy:** Data used and shared should have necessary explicit consent from data providers.

Blockchain

(1) Concept

- Blockchain is based on a decentralized & distributed ledger that is secured through encryption.
- Each transaction is validated by the blockchain participants, creating a block of information that is replicated & distributed to all participants. All blocks are sequenced so that any modification or deletion of a block disqualifies the information.
- Despite resistance, the benefits associated with blockchain technology are being recognized across a variety of other industries.
- **Examples:** Bitcoin, Cryptocurrency transfer application – Blockchain in money transfer, Blockchain smart contracts.

(2) Audit Implications

(i) **Governance and Security:** Auditors should consider appropriate governance & security around the transactions. Although blockchain's core security premise rests on cryptography, there are risk factors associated with it.

(ii) **Insecure API, data confidentiality and Privacy:** As blockchain interacts with systems & business partners, concerns related to insecure application programming interfaces (APIS), data confidentiality & privacy cannot be ignored. Weak blockchain API are something auditors cannot overlook.

(iii) **Data privacy laws and regulations:** Auditors must be able to determine whether data put on blockchain will expose enterprise to liability for noncompliance with applicable laws and regulations.

(3) Common Risk

(i) **Inability to reverse transactions:** Inability to reverse transactions and to access data without the required keys make the system secure, but also mean that organisations need specific protocols and management processes to ensure that they are not locked out and have clear contingency plans.

(ii) **Security Concerns:** Operating through network nodes could also expose the organisation to cyber-attacks and data hacks, so security issues are important.

(iii) **Regulatory landscape:** Regulatory landscape is still evolving for blockchain, so audit teams should check that compliance managers are following developments constantly and adapting processes accordingly.

NFT (Non-Fungible Token)

(i) Meaning

- NFT means something is unique and cannot be replaced. Unlike physical money and cryptocurrencies are fungible (means they can be traded or exchanged for one another) NFTs are non-fungible tokens.
- NFTS contains digital signature which make them unique. NFTs are digital assets, e.g., photos, videos, artwork, sports collectibles etc.
- NFTs are tokens used to represent ownership of unique items. NFTs allow their creators to tokenize things like art, collectibles, or even real estate. They are secured by the blockchain and can only have one official owner at a time. No one can change the record of ownership or copy/paste a new NFT into existence.

(ii) Key Features of NFT

- **Digital Asset:** NFT is a digital asset that represents Internet collectibles like art, music, and games with an authentic certificate created by blockchain technology that underlies Cryptocurrency.
- **Unique:** It cannot be forged or otherwise manipulated.
- **Exchange:** NFT exchanges take place with cryptocurrencies such as Bitcoin on specialist sites.

(iii) Challenges of NFT

NFTS has its **own** challenges like ownership and copyright concerns, security risks, market is not that wide, online frauds etc.

(iv) Audit Considerations

Includes comprehensive code review for verifying the safety of a token, valid contract, data privacy and potential cyber threat.

Robotic Process Automation (RPA)

(1) Concept

- Automation of repetitive processes performed by users.
- It is a software technology that emulate humans' actions interacting with digital systems and software.
- **Key Contributors to RPA:** Process efficiency, customer experience and control effectiveness.
- RPA software bots can interact with any application or system the same way people do, except that RPA bots can operate around clock, nonstop, much faster & with 100% reliability and precision.

(2) Audit Implications

(i) **Understanding of the processes:** To understand RPA processes, which include data extraction, aggregation, sanitization and cleansing. Unless auditors understand these processes, they will not be in a position to initiate an audit.

(ii) **Review of Source Code:** A comprehensive assurance process might demand review of the source code.

(iii) **Understanding of tools:** To perform substantive testing, auditors must have an understanding of the tools used to develop & maintain RPA. This will be helpful when auditors review logs, configuration controls, privileged access controls and the like.

(iv) General IT controls are applicable as always.

(3) Common Risk

(i) **Operational and execution risks:** Robots are deployed without proper operating model. Buying the wrong tool, making wrong assumptions, taking shortcuts, and jeopardizing security and compliance.

(ii) **Change management risks:** Not following the change management implementation lifecycle, improper & incomplete testing (not covering all scenarios) leads to inaccurate results.

(iii) **RPA Strategy Risk:** Setting wrong expectations and unrealistic business goals creates an environment of uncertainty.

(4) RPA to check IND AS, IFCoFR and Standards on Auditing

To ensure accurate financial reporting, effective internal controls, and reliable audit procedures, following elements to be incorporated in audit practices:

- IND AS (Para-wise details: Para reference, Accounting policy, Relevant data to be captured, Relevant calculation to be made, Presentation in F.S.)

- IFCoFR,
- Audit procedures as per Standards on auditing

Example (Ind-AS 16: PPE)

Para Ref.	6
Accounting policy	Define PPE as tangible assets that are held for use in production or supply of goods or services, for rental to others, or for administrative purposes; and are expected to be used during more than one period.
Relevant data to be captured	Identify PPE items & their cost components.
Relevant calculation to be made	Apply recognition criteria & measurement principles.
Presentation in F.S.	Disclose PPE items & their carrying amounts, depreciation methods and rates, useful lives, impairment losses, etc.
IFCoFR	Establish internal controls over identification, recognition, measurement, depreciation, impairment and disclosure of PPE.
Audit procedures as per SAs	Verify existence, ownership, valuation and disclosure of PPE by inspection, confirmation, vouching, analytical procedures, etc.

Control Considerations or Objectives of Auditing Digitally

Control Considerations to be Focused

(i) **Holistic understanding of changes:** Auditors should gain a holistic understanding of changes in industry and IT environment to effectively evaluate management's process for initiating, processing, and recording transactions and then design appropriate auditing procedures.

(ii) **Considerations of Risks:** Auditors should consider risks resulting from implementation of new technologies & how they differ from those that arise from traditional systems.

(iii) **Digital Upskilling:** Auditors should consider whether digital upskilling or specialists are necessary to determine the impact of new technologies and to assist in the risk assessment & understanding of design, implementation & operating effectiveness of controls.

Technology Risks where Auditor should test the appropriate controls

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.

- Unauthorized access to data that might result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions or inaccurate recording of transactions.
- Possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties, thereby leading to insufficient segregation of duties.
- Unauthorized or erroneous changes to data in master files.
- Unauthorized changes to systems or programs.
- Failure to make necessary or appropriate changes to systems or programs.
- Inappropriate manual intervention.
- Potential loss of data or inability to access data as required.
- Risks introduced when using third-party service providers.
- Cybersecurity risks.

Key Steps for auditors in a Changing IT Environment

- Maintain sufficient professional skepticism when reviewing management's risk assessment for new systems.
- Understand the direct and indirect effects of new technology and determine how its use by the entity impacts the auditor's overall risk assessment.
- Understand how technologies impact the flow of transactions, assess the completeness of the in-scope ICFR systems, and design a sufficient and appropriate audit response.
- Assess appropriateness of management processes to select, develop, operate & maintain controls related to organization's technology based on the extent technology is used.

Next Generation Audit

(a) Shift of Focus

Next Generation Audit is human-led, tech-powered and data-driven. It is based on combining emerging technologies to redefine how audits are performed.

Next Generation Audit aims to the following:

From	to
Sampling Populations	Full Population Analysis
Multiple datasets	One data set
Disconnected tools	Integrated ecosystem services
Manual Risk Assessments	Dynamic, data-driven risk assessment
Separated communication	Embedded Communications
Repetitive Tasks	High Value Work and Capacity for Growth
Manual Work	Automation
Ad hoc Insights	Insights from a broader audit

Technology forming part of Next Generation Audit

(1) Drone Technology

- Drones have great load capacity for carrying sensors & cameras, thus they can photograph and physically examine count of large quantities of fixed assets and inventory.
- Drone captured audit information can be combined with various alternative sources of information such as QR code readers, manual counts etc. to consolidate audit information & enhance execution speed while ensuring correctness and completeness of data.

(2) Augmented Reality

It allows users to view the real-world environment with augmented (added) elements, generated by digital devices. **Example:** Pokémon Go, a game for mobile devices in which players chase imaginary digital creatures (visible on their mobile phones) around physical locations.

(3) Virtual Reality (VR)

- VR goes a step forward and replaces the real world entirely with a simulated environment, created through digitally generated images, sounds, and even touch and smell.
- Using special equipment, such as a custom headset, the user can explore a simulated world or simulate experiences such as flying or skydiving.

(4) Metaverse

- Metaverse is emerging 3-D digital space that uses virtual reality, augmented reality, and other advanced internet technology to allow people to have lifelike personal and business experiences online.
- It represents a convergence of digital technology to combine and extend the reach and use of Cryptocurrency, Artificial Intelligence (AI), Augmented Reality (AR) and Virtual Reality (VR).

Potential application of the metaverse in the financial domain

(i) **Virtual Banking and Transactions:** A forward-thinking financial institution, establishes a presence in the metaverse to offer virtual banking services. Users can create virtual bank accounts, access personalized financial dashboards, and perform transactions using virtual currencies.

(ii) **Digital Asset Management:** A digital asset management company, recognizes the growing popularity of virtual assets in the metaverse. They launch a virtual asset trading platform within the metaverse, allowing users to buy, sell, and trade NFTS and other digital assets.

(iii) **Virtual Financial Education and Training:** A Financial Learning Academy aims to enhance financial literacy using the metaverse. They create a virtual classroom environment where participants can attend interactive financial education sessions.

(iv) **Virtual Meetings and Conferences:** For a leading industry even an organisation hosts a virtual conference within metaverse. Participants from around the world can access the conference through their virtual avatars.

(v) **Data Visualization and Analytics**: A company utilizes the metaverse to offer advanced data visualization and analytics tools to financial professionals. Their virtual analytics platform allows users to visualize complex financial data in interactive and immersive 3D environments.

(b) Common Risks Associated

- Public safety;
- Cybersecurity;
- Data Privacy;
- Data protection;
- Lack of standards;
- Technical challenges; and
- Concerns over taxation, jurisdiction, and customer protection.