CHAPTER 12

DIGITAL AUDITING AND ASSURANCE

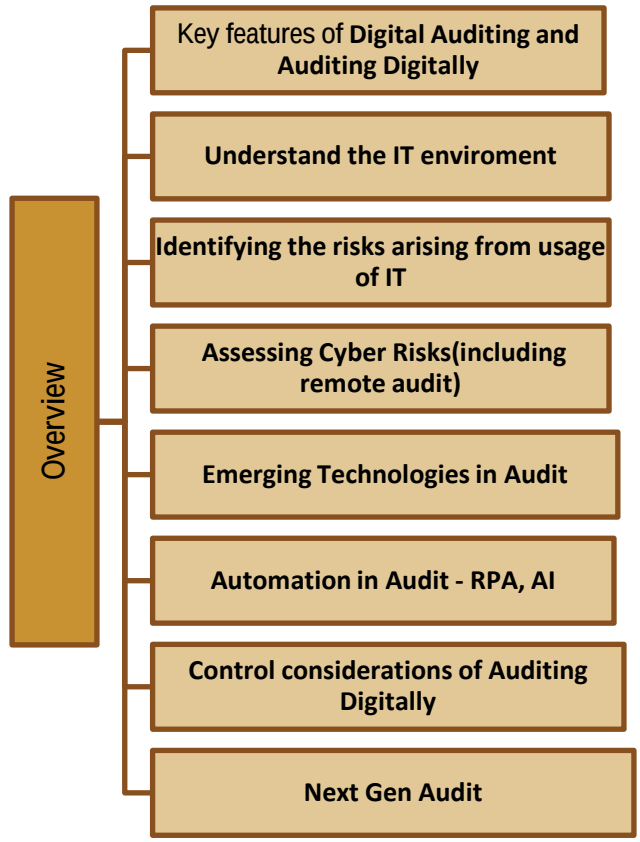
LEARNING OUTCOMES

After studying this chapter, you will be able to:

- Understand the key features of digital auditing and auditing digitally.
- Understand IT environment and its complexity.
- Know how to identify the IT dependencies impacting the audit.
- Gain the knowledge of how to identify IT related risks and controls that exists in an automated environment.
- Learn key considerations to assess the cyber risks and remote audit.
- Learn the control objectives that auditor should consider in performing IT audit.
- Know the types and tools available to perform digital audit.
- Learn the usage of data analytics in assessing and analysing the key data.

© The Institute of Chartered Accountants of India

CHAPTER OVERVIEW



CA M woke up on a leisurely Sunday morning to find a report in his favourite pink newspaper about ICAI and Indian Banks Association plans to develop a balance confirmation portal. The report further indicated that such a proposed common platform would ensure authenticated balance confirmations by auditors directly from banks. "Auditing digitally improves efficiency and quality of audits"- he thought. Wondering that besides ushering in an era of transparency, such initiatives are likely to enhance efficiency and reduce costs. What does auditing digitally precisely signify?

Auditing digitally is using the advancements in technology for conducting an effective and efficient audit. With a rapidly growing IT environment, adaptation of technology in auditing practices is imminent requirement. Use of data analytics, artificial intelligence and robotics

© The Institute of Chartered Accountants of India

process automation can go a long way in improving quality of audit. Data analytics involves analysing large sets of data to find actionable insights, trends and drawing of conclusions for informed decision making. Currently, audit approach is based upon sampling. This is undergoing transformation and process is likely to be accelerated in times to come.

Robotics Process Automation (RPA) involves use of programs to perform repetitive tasks. Such computer coded software is useful in many business processes like payroll generation, order processing, invoice processing and a host of other business functions involving repetitive tasks. RPA can help auditor in automating classification for risk assessment process with the help of bots. Bots can even be used to prepare report on automated controls configured on ERP!

He was also reading an article as to how disruptive blockchain technology could be as internet was in 90s and its impact on auditing profession. Blockchain as a technology takes the connectivity of the internet one step further. It offers users the internet of value. Blockchain is a shared immutable ledger and is replicated across several systems in almost real time. It is put together in encrypted blocks. It was further opined that Blockchain will do for transactions what the Internet did for information.

With emerging technologies like Blockchain and its combination with data analytics, big data and robotics, it is going to be possible to audit all of information. Since blockchain allows access to transaction history, it is going to revolutionize audit approach and work. The information stored on a blockchain is likely to be available to the auditor as soon as it is generated. How exciting outcomes of such a scenario could be? The dependency on the client to provide information may become redundant in coming future. Another important application of it is use of *"smart contracts"* which can be embedded in a blockchain to automate business processes. It is likely to lead to more emphasis on "tests of controls" than "tests on details".

His discerning mind was quickly realizing that with advancements in technology, cyber-attacks are also bound to grow. It is not an IT issue alone. It affects an entity's reputation and theft of sensitive information like intellectual property rights, personally identifiable information and disruptions in automated operations. Auditor should consider whether cyber risk represents a risk of material misstatement to the financial statement as part of the audit risk assessment activities. Focus should be on understanding the cyber risks affecting the entity and the actions being taken to address these risks.

© The Institute of Chartered Accountants of India

1. DIGITAL AUDIT

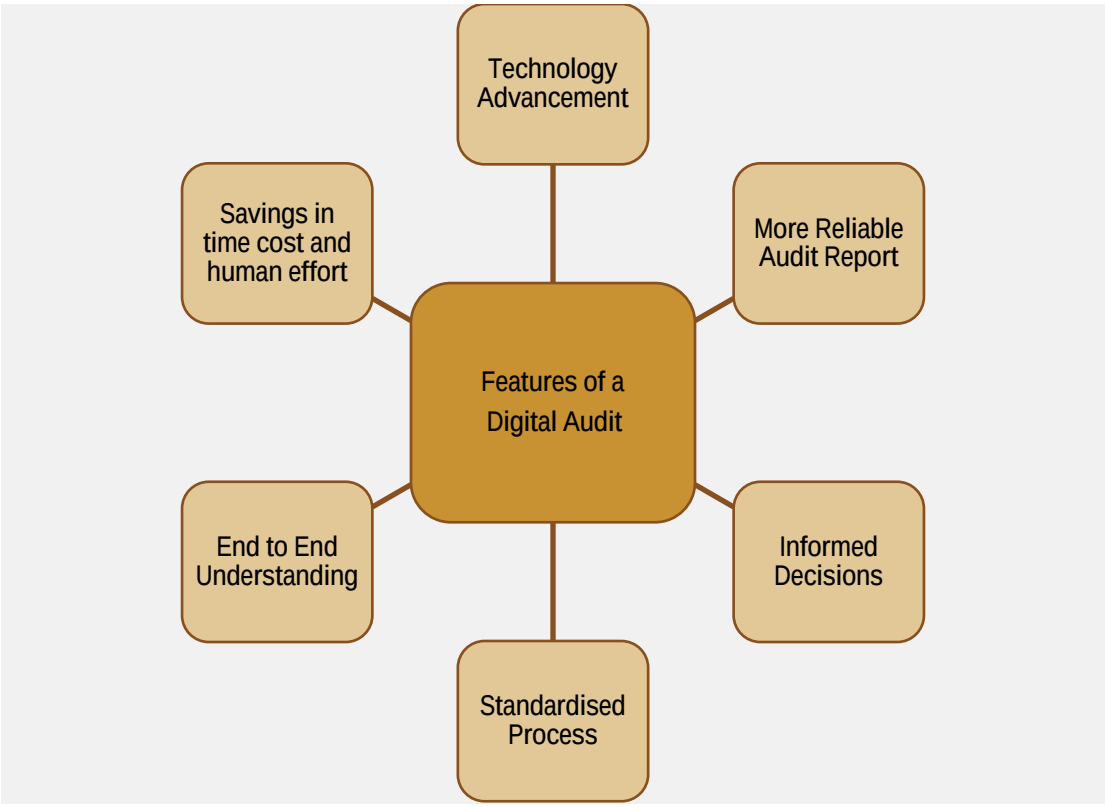
1.1 What is a Digital Audit?

Digital Audit is placing assurance on the effectiveness of the IT systems implemented in an organization. Technology is becoming an integral part of day-to-day business operations. It is essential that organizations review their technology-related controls to identify gaps and risks for continuous improvement and to ensure regulatory compliance. A strong controls and security position will allow organizations to build trust with their stakeholders.

1.2 Key Features of a Digital Audit

- Digital audit encourages the auditee to embrace the latest technological advancements and provides confidence to auditee to stay updated in a constantly evolving environment.
- A digital audit improves the quality of opinion. This consequently leads to a more reliable audit report
- Digital Audit leads to savings in time, cost and human effort which can be utilized towards more productive tasks. Many of today's digitally enabled processes can be orchestrated to operate autonomously 24x7, driving real-time transactions.
- Digital Audit allows to standardize processes and allow controls to be implemented to mitigate risk.
- The digital audit will help organization gain a more comprehensive overview of end-to-end processes and how technologies are utilized, controlled and optimized against standards set.
- The digital audit will help create a future for a digital strategy and paves way for adopting new technologies such as AI and Robotic, usage of analytics and automation.
- It can help auditee to make informed decisions.

© The Institute of Chartered Accountants of India



1.3 Advantages of Digital Audit

(i) Enhanced Effectiveness & Efficiency: Increased efficiency is one of the key benefits of digital audit. With the use of tools and automation techniques, auditee can standardize the processes and routine tasks can be automated like automating a reconciliation process that previously involved hours increase efficiency and saves time and costs.

(ii) Better Audit Quality: Technology can correctly evaluate massive volumes of data quickly. This can assist auditors in determining the areas that require more testing, lowering the chance that serious misstatements or other problems would go unnoticed.

(iii) 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.

(iv) Better Analytics: Improved analytics capabilities can aid management and auditors in seeing trends and patterns that may be challenging to spot manually. For instance, AI can examine a lot of financial data to spot possible fraud, which is hard for auditors to spot manually.

© The Institute of Chartered Accountants of India

(v) Improved Risk Assessment: Creating a number of automations to assist with the audit process and streamlined testing improves the risk assessment procedure. Management and auditors put their testing efforts on sites with a higher risk of material misstatement and make informed decisions.

1.4 Consideration and Challenges of Digital Audit:

Some considerations that organization should keep in mind while using digital techniques & automation:

Know what business benefits the organization wants to achieve with automation	Think people first and do not underestimate change is difficult	Target the right processes – this is a key for successful automation.
Automation is not a stand-alone solution and should be part of a broader digitalization strategy.	Ensure the process works and it is standardised before automating. Bots do not easily adapt to process change	Automation introduces new challenges for organization. Don't forget about governance and data security in the risk framework.

As auditors will obtain an understanding of management's implementation and oversight of new technologies, they also will perform procedures to understand the changes to the company's business, including any changes to the information technology environment. Areas of focus could include understanding of 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, changes in staffing levels that affect an entity's internal control environment)
- 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
- The impact the new technology as how the organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

© The Institute of Chartered Accountants of India

2. AUDITING DIGITALLY

2.1 What is the 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.

Using Sampling Tools for selection of a sample size from a population based on materiality or using Bot for analysis of statutory payments compliance as part of an audit assignment.

It is time to digitize the way an audit is delivered through automation and innovation. There are new technologies to help *capture* data, *automate* procedures, *analyse* information and *focus* on the real risks of the client. The opportunity is in understanding how technology can help and then applying it to the auditing challenges.

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. Investment in digitally upskilling the people is the real secret to quality technology audit. Investment in technology across the profession has largely been focused 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. While this will remain core to the role of technology in the audit, there are many opportunities where more advanced technologies such as AI and drones could have an even bigger impact. Such technologies may also play a role in evolving the scope of the audit (e.g., in using data analytics and machine learning to help identify fraud).

A manager on a weekly basis performs a manual control to review if vendor master additions and changes in the system are done post appropriate approvals.

This control can be tested and reperformed by the auditor using RPA technology – BOTs can login into the system and generate the report and write the output to an Excel file. Based on the population the BOT will select the samples of changes to be tested. Further BOT will pull the correct file with approved changes from SharePoint. Then it will perform the testing wherein it will populate the details of approvals (date, approved by) and identify if changes made without approvals. Lastly BOT will summarise the results for all the selected samples in an excel file.

© The Institute of Chartered Accountants of India

The auditor will then review the final results file to check if there are any exceptions (changes made without approvals) noted in the selected samples.

Due to the usage of BOT manual intervention has been reduced, more accurate results are populated, it results in saving auditors time as well and exceptions highlighted can be readily reviewed.

2.2 Key Features or Advantages of Auditing Digitally:

Following are key features or advantages of Auditing Digitally:

(i) Improved Quality of Audits: The impact on quality is evident, through automation, data analytics techniques we can easily move from sample auditing to full population of transactions being reviewed or re-performed. This ultimately free up time for audit teams to analyses the information and better understand the business they audit. Technology requires an element of upfront investment, and it can be challenging to implement with regards to resources and people, but the value once it is up and running is undeniable.

(ii) Decreasing human dependency: Using technology minimizes the manual intervention which ultimately results in reducing the risk of manual errors. Technology helps in streamlining the process of testing for auditors which decreases the errors which occur from the judgement of different individuals.

(iii) Increases Transparency: With the technological advancement transparency has been increased. New ERPs and tools have audit trail feature available to trace the transaction end to end. It helps the management or auditors to review the details like the date on which any change is made, who made the change, what has been changed, all such details are captured and can be used while performing audit.

(iv) Automation and Ease: Automating tasks like recording work in repositories, extracting data and sampling have improved the quality of audit and reduced the manual error. Using dashboards (e.g., Power BI) for reporting helps in understanding the position and helps the auditor to form his opinion.

(v) Improved Efficiency: What used to take weeks to learn and programme using deep experts, is now easily available to auditors after some simple training and digital upskilling. The result may be increased efficiency and fewer errors, but the benefits are wider reaching and personal. This also results in improved retention of talent and confidence.

© The Institute of Chartered Accountants of India

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. Dashboards, visual presentations and other tools helps in understanding where the risk lies and what all areas need more attention.

2.3 Considerations in Auditing Digitally

While all industry sectors are affected by the emergence of new technologies it is important to remember that the auditor's needs are unique. There are few questions it is important to ask and answer – at all stages of tech journey:

2.3.1 What problems are you trying to solve?

Continuously evaluate the emerging technologies and latest tools to see what can benefit the audit. Think about what would make your audit easier or better and how you will measure return on your investment.

2.3.2 Which technology can help you?

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 your current processes and flag any potential implementation issues early on.

2.3.3 How will you upskill your people to make best use of the technology available?

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.

2.3.4 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. Some of the techinques are using robotics and automation for data gathering activities, use of data analytics for planning and budgetting and reporting by dashboards.

© The Institute of Chartered Accountants of India

Macros and Scripts	Business Process Automation (BPA)	Robotic Process Automation (RPA)	Intelligent Process Automation (IPA)
Rules-based automation within a specific application	Reengineering existing business processes e.g. workflows	Automating labour-intensive, repetitive activities across multiple systems and interfaces	• Combining RPA with artificial intelligence technologies to identify patterns, learn over time, and optimize workflows

3. UNDERSTAND THE IT ENVIRONMENT

- Understanding the ways in which the entity relies upon IT and how the IT environment is set up to support the business. This allows the auditor to better understand where risks might arise from the entity's use of IT (required as per SA 315).
- Understanding how IT is used by the entity helps in identifying controls over the entity's IT processes.
- Assessing the complexity of the IT environment helps the teams consider whether to involve IT specialists or experts in the planning and/or execution of the audit, including initial consideration of whether to include specialists in the complexity assessment.

The auditor's understanding of the automated environment should include the following:

- The applications that are being used by the company.
- Details of the IT infrastructure components for each of the application.
- The organization structure and governance.
- The policies, procedures and processes followed.
- Extent of IT integration, use of service organizations.
- IT risks and controls.

© The Institute of Chartered Accountants of India

The illustration below is an example of how an 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

3.1 Key Areas for an Auditor to Understand IT Environment

Key Areas for an Auditor to Understand IT Environment are as follows:

1. Understand the flow of transaction: The auditor's understanding of the IT environment may focus on identifying and understanding the nature and number of the specific IT applications and other aspects of the IT environment that are relevant to the flows of transactions and processing of information in the information system. Changes in the flow of transactions, or information within the information system may result from program changes to IT applications, or direct changes to data in databases involved in processing or storing those transactions or information.

2. Identification of Significant Systems: The auditor may identify the IT applications and supporting IT infrastructure concurrently with the auditor's understanding of how information relating to significant classes of transactions, account balances and disclosures flows into, through and out the entity's information system.

3. Identification of Manual and Automated Controls: An entity's system of internal control contains manual elements and automated elements (i.e., manual and automated controls and other resources used in the entity's system of internal control). An entity's mix of manual and automated elements varies with the nature and complexity of the entity's use of IT. The characteristics of manual or automated elements are relevant to the auditor's identification and assessment of the risks of material misstatement.

© The Institute of Chartered Accountants of India

4. **Identification of the technologies used:** The need to understand the emerging technologies implemented and the role they play in the entity's information processing or other financial reporting activities and consider whether there are risks arising from their use.

   Given the potential complexities of these technologies, there is an increased likelihood that the engagement team may decide to engage specialists and/or auditor's experts to help understand whether and how their use impacts the entity's financial reporting processes and may give rise to risks from the use of IT.

   Some examples of emerging technologies are:

   - Blockchain, including cryptocurrency businesses (e.g., token issuers, custodial services, exchanges, miners, investors)
   - Robotics
   - Artificial Intelligence
   - Internet of Things
   - Biometrics
   - Drone

5. **Assessing the complexity of the IT environment:** Not all applications of the IT environment have the same level of complexity. The level of complexity for individual characteristics differs across applications. Complexity is based on the following factors – automation used in the organization, entity's reliance on system generated reports, customization in IT applications, business model of the entity, any significant changes done during the year and implementation of emerging technologies.

   After considering the above factors for each application the over complexity is assessed of the IT environment.

4. IDENTIFYING THE RISKS ARISING FROM USAGE OF IT

4.1 How to identify the IT Risks?

In identifying the risks arising from the use of IT, the auditor may consider the nature of the identified IT application.

Applicable risks arising from the use of IT may also be identified related to cybersecurity.

© The Institute of Chartered Accountants of India

It is more likely that there will be more risks arising from the use of IT when the 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.

4.2 Risks arising from use of IT

- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database.
- The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties. Unauthorized changes to data in master files.
- Unauthorized changes to IT applications or other aspects of the IT environment.
- Failure to make necessary update IT applications or other aspects of the IT environment.
- Inappropriate manual intervention.
- Data loss or data corruption is a major risk which arises from use of IT. If appropriate cybersecurity controls and protocols not followed it may lead to loss of sensitive data, hackers might encrypt your system or illegally break into your system. Risk of fraud can arise if users alter the information or there is a case of physical security breach or theft of sensitive information.
- There is a risk of system downtime which is caused by hardware failures, faulty configurations, cyberattacks or power outage. It means the IT systems will not be operational or will be unavailable/offline which may hamper the business.
- Since companies uses more than one IT systems to support their business system integration (means integrating one or more systems) and system compatibility comes in place. However, system integration and compatibility have some risks. In case of system failure in one system may also lead to widespread failure in integrated systems. Or if the integration between two systems is not appropriate the end result would be incorrect. System compatibility means sharing compatible hardware, software and operating system while performing the integration. Compatibility risks arises if different versions of same software are used, if the patches are not upgraded which may lead to bugs.

© The Institute of Chartered Accountants of India

- With advancement in usage of IT the risk of regulatory compliances increases. Any change in the law, order, guidelines or agreements will impact the business, its related costs, investments etc. A FMCG sector will be subject to different regulatory requirements than a financial company, however both businesses will need to manage their respective compliance risks.

Performance Issues arises with the way requests are processed in the IT systems. Heavy data load, network usage impacts the application performance and its responsiveness. To overcome the performance issues of IT systems, resources or hardware can be added to an existing nodes, which is known as scaling. However, scaling can be expensive therefore an informed decision should be made in case of adding a hardware or changing the architecture.

4.3 Know how to identify the IT dependencies impacting the Audit

4.3.1 Why is it important to identify IT dependencies?

Identifying and documenting the entity's IT dependencies in a consistent, clear manner helps to identify the entity's reliance upon IT, understand how IT is integrated into the entity's business model, identify potential risks arising from the use of IT, identify related IT General Controls and enables us to develop an effective and efficient audit approach.

4.3.2 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 financial statements.

There are five types of IT dependencies as described below:

Type	Description
Automated Controls	Automated controls are designed into the IT environment to enforce business rules. For example, Purchase order approval via workflow or 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) when a transaction is entered.
Reports	System generated reports are information generated by IT systems. These reports are often used in an entity's execution of a manual control, including business performance reviews, or may be the source of entity information used by us when selecting items for testing, performing substantive tests of details or performing a substantive analytical procedure. E.g. (Vendor master report, customer ageing report)

© The Institute of Chartered Accountants of India

Calculations	Calculations are accounting procedures that are performed by an IT system instead of a person. For example, the system will apply the 'straight-line' depreciation formula to calculate depreciation of an asset (i.e., cost of the asset, less the residual value of the asset at the end of its useful life divided by the useful life of the asset) or the system will calculate the value of the amount invoiced to a customer by multiplying the item price times the quantity shipped.
Security	Security including segregation of duties is enabled by the IT environment to restrict access to information and to determine the separation of roles and responsibilities that could allow an employee to perpetrate and conceal errors or fraud, or to process errors that go undetected.
Interfaces	Interfaces are programmed logic that transfer data from one IT system to another. For example, an interface may be programmed to transfer data from a payroll sub-ledger to the general ledger.

4.3.3 Understanding and responding to risks arising from IT dependencies

When auditors identify IT dependencies that are relevant to the entity's flow of transactions and processing of financial information, they need to understand how management responds to the associated risks that may arise from them.

Management may implement information technology general controls (ITGCs) to address risks related to IT dependencies.

The illustration below is an overview of the Control Objectives and controls for each area of General IT Controls:

Access Security Objective: To ensure that access to programs and data is authenticated and authorized to meet financial reporting objectives	• Access requests to the 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.
Program Change Objective To ensure modified systems continue to meet financial reporting objectives	• Change Management policy and procedures are maintained. • Development, testing and 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 mainatined between developer and implementor.
Data Centre and network operations Objective To ensure production systems are appropriately backed up to meet financial reporting objectives	• Policies and procedures for data back and recovery is maintained. • Data is appropriately backed up and recoverable • Restoration testing is perfomed • Monitoring and complaince of service level agreements. • Batch job scheduled are monitored for failures and access is restricted.

© The Institute of Chartered Accountants of India

IT dependencies may also affect the design of the entity's controls and how they are implemented.

Therefore, auditors consider IT dependencies relevant to audit and evaluate the related risks. Auditor should scope in ITGCs to tests when there are IT dependencies identified in the system. If the controls around IT environment are not implemented or operating effectively it will result in not relying on ITGCs which means the IT dependencies could not be relied upon.

5. ASSESSING CYBER RISKS (INCLUDING REMOTE AUDIT)

5.1 What is Cyber Risk:

A cyber-attack is an attempt to gain unauthorized access to a computing system or network with the intent to cause damage, steal, expose, alter, disable, or destroy data.

Regulators across the globe have placed the topic of cyber risk management under increasing scrutiny, requiring financial institutions to assess the maturity of their cybersecurity program, manage cyber risks, and enhance resiliency against cyber-attacks. Most common types of cyber-attacks are:

- Malware : Malware or malicious software is any program or code that is created with the intent to do harm to a computer, network or server. Malware is the most common type of cyberattack, its subsets are ransomware, fileless Malware trojans, viruses etc.

Type	Description
Ransomware	In a ransomware attack, an adversary encrypts a victim's data and offers to provide a decryption key in exchange for a payment. Ransomware attacks are usually launched through malicious links delivered via phishing emails, but unpatched vulnerabilities and policy misconfigurations are used as well.
Fileless Malware	Fileless malware is a type of malicious activity that uses native, legitimate tools built into a system to execute a cyber-attack. Unlike traditional malware, fileless malware does not require an attacker to install any code on a target's system, making it hard to detect.
Trojan	A trojan is malware that appears to be legitimate software disguised as native operating system programs or harmless files like free downloads. Trojans are installed through social engineering techniques such as phishing or bait websites.
Mobile Malware	Mobile malware is any type of malware designed to target mobile devices. Mobile malware is delivered through malicious downloads, operating system vulnerabilities, phishing, smishing, and the use of unsecured Wi-Fi.

© The Institute of Chartered Accountants of India

- Denial-of-Service (DoS) Attacks : A Denial-of-Service (DoS) attack is a malicious, targeted attack that floods a network with false requests in order to disrupt business operations. In a DoS attack, users are unable to perform routine and necessary tasks, such as accessing email, websites, online accounts or other resources that are operated by a compromised computer or network. While most DoS attacks do not result in lost data and are typically resolved without paying a ransom, they cost the organization time, money and other resources in order to restore critical business operations.

- Phishing: Phishing is a type of 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.

Type	Description
Spear Phishing	Spear-phishing is a type of phishing attack that targets specific individuals or organizations typically through malicious emails. The goal of spear phishing is to steal sensitive information such as login credentials or infect the targets' device with malware.
Whaling	A whaling attack is a type of social engineering attack specifically targeting senior or C-level executive employees with the purpose of stealing money or information or gaining access to the person's computer in order to execute further cyberattacks.
Smishing	Smishing is a type of fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.
Vishing	Vishing, a 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.

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

Type	Description
Domain Spoofing	Domain spoofing is a form of phishing where an attacker impersonates a known business or person with fake website or email domain to fool people into the trusting them. Typically, the

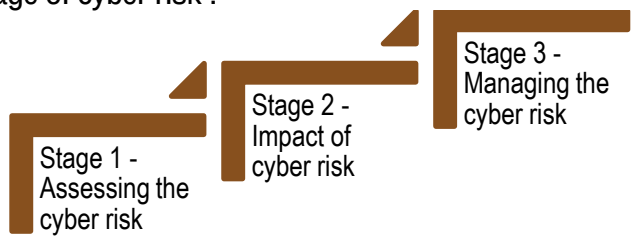
© The Institute of Chartered Accountants of India

	domain appears to be legitimate at first glance, but a closer look will reveal subtle differences.
Email Spoofing	Email spoofing is a type of cyberattack that targets the 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.

- Identity-Based Attacks : When a 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.
- Insider Threats : When current or former employees that pose danger to an organization because they have 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.
- DNS Tunneling : DNS Tunneling is a type of cyberattack that leverages domain name system (DNS) queries and responses to bypass traditional security measures and transmit data and code within the network. This tunnel gives the 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.
- IoT-Based Attacks: An IoT attack is any 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

5.2 Stages of Cyber Risks:

Following are 3 Stage of cyber risk :



1. Stage 1 - Assessing the cyber risk: No organization is completely immune to a cyber risk. Different clients will have different levels of risks, even with the same industry. Every organization should consider at least the common threats-

© The Institute of Chartered Accountants of India

- Ransomware disabling their organization (including their plants and manufacturing facilities)
- Common criminals using email phishing and hacks for fraud and theft.
- Insiders committing malicious activities or accidental activities resulting in unintended discourse of information theft and frauds.

2. Stage 2 - Impact of cyber risk: Cyber-attack can impact one, two or more types of risks. The impact of the attack would vary from organization to organization and most importantly from an attack to attack. Some of the indicative areas can be –

- 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
- Intellectual property theft which may not only take the competitive advantage, but we may also result in any impairment/impediment 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:

- Gain a holistic understanding of the cyber risks, threats facing their organization and other financial institutions
- Assess existing IT and cybersecurity program and capabilities against the relevant regulatory requirements
- Align cybersecurity and IT transformation initiatives with strategic objectives and critical risks
- Understand accepted risks & documented compensating controls

© The Institute of Chartered Accountants of India

5.3 Cyber Security Framework

Cybersecurity framework includes how management is identifying the risk, protecting and safeguarding its assets (including electronic assets) from the risk. Management preparedness to detect the attacks, anomalies and responsiveness to the adverse event.

5.3.1 Identify the risk:

Auditor has to determine whether the entity's risk assessment process considers cybersecurity risks.

Entity should conduct a periodic risk assessment & develop a management strategy which identifies cybersecurity risks around IT system failure affecting the entity's primary business or potential loss of data or inability to access data as required, Risk of unauthorized access to the IT network.

The entity should maintain and periodically reviews an inventory of their information assets- i.e., Asset Management (e.g., intellectual property, patents, copyrighted material, trade secrets and other intangibles).

The entity should classify and prioritize protection of their information assets based on sensitivity and business value and periodically reviews the systems connected to the network on which digital assets reside.

From the governance perspective management should review how cybersecurity risks affect internal controls over financial reporting. In case of adverse attack how management is going to assess the impact on the recoverability of financial data and impact on revenue recognition.

Management needs to identify if any established a risk-based cybersecurity program can be leveraged e.g. (NIST, ISO etc.)

To determine overall responsibility for cybersecurity in the business environment entity should establish roles and responsibilities over cybersecurity (CISO, CIO). Further the risk assessment should be discussed with those charged with governance (e.g., the Audit Committee or Board of Directors).

5.3.2 Protect the risk

Obtained an understanding of the entity's processes for safeguarding of assets subject to cybersecurity. Entity monitors whether there has been unauthorized access to electronic assets and any related impact on financial reporting.

© The Institute of Chartered Accountants of India

Formal training should be conducted to make the teams aware of the risk associated with cyber-attacks. Entity should implement effective controls for data security. Entity should have a process & procedures in place for identifying material digital/electronic assets on the balance sheet subject to cybersecurity risk (e.g., intellectual property, patents, copyrighted material, trade secrets) and prioritizing their protection based on criticality.

5.3.3 Detect The risk

Entity should have controls and procedures that enable it to identify cybersecurity risks and incidents and to assess and analyse their impact on the entity's business, evaluate the significance associated with such risks and incidents, and consider timely disclosures.

Review entity's processes to monitor and detect security breaches or incidents. If management has implemented anti-virus in the system to secure it from anomalies or if firewall logs are being continuously monitored to detect any repetitive attacks. A monitoring process should be established to review how many such events have been denied by the firewall. Monitoring process should also include if any upgrades or updates are required to safeguard the systems from vulnerabilities.

5.3.4 Respond to the risk

In case of material cybersecurity or data breach has been identified management should capture the details of nature of incident and how the incident or data breach was identified. Entity should have a response planning in place to capture the details of nature of incident and the same needs to be communicated with those who are ultimately responsible for this framework and with those charge with governance.

The security incident response plan helps in analysing the impact and severity of the attack and helps the organisation in taking the appropriate actions. Management should assess Litigation costs, Regulatory investigation costs and Remediation costs as a part of mitigation process and improvement management should assess the future action plans that needs to be taken to safeguard the organisation from such attacks.

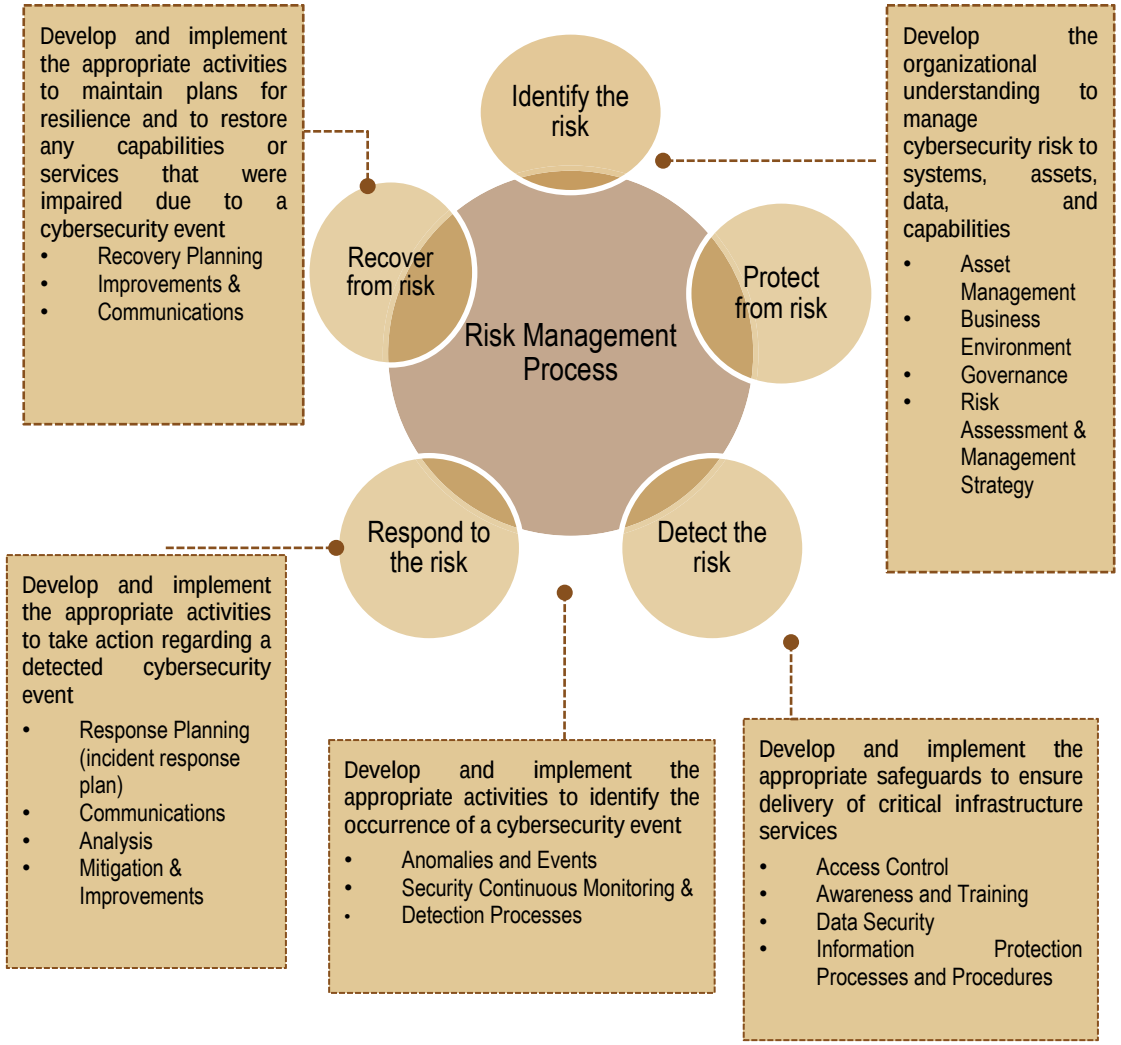
5.3.5 Recover from risk

Entity should undertake appropriate actions to recover from the attack and make sure the business is up and running.

Once the impact evaluated and communicated with the regulators the recovery plan needs to be implemented to overcome the impact. Necessary improvements – like patch upgrades, better

© The Institute of Chartered Accountants of India

controls, improved technology in terms of firewall, anti-virus, tools etc needs to be implemented to safeguard the entity.



TEST YOUR UNDERSTANDING 1

Sukanya, a CA final student, is of the view that cyber risks are issues of IT and result only in information loss to an entity. She also feels that many cyber-attacks are not directly targeted at financial systems and do not pose risk of material misstatements to financial statements of an entity. Is her view proper?

© The Institute of Chartered Accountants of India

Case study

What has happened:

The CEO of a hotel realized their business had become the victim of wire fraud when the accounts payable executive began to receive insufficient fund notifications for regularly recurring bills.

A review of the accounting records exposed a serious problem. Upon investigating it was noted that the CEO had clicked on a link in an email that he thought was from the trusted source. However, it wasn't and when he clicked the link and entered his credentials, the cyber criminals captured the CEO's login information, giving them full access to intimate business and personal details.

Type of Attack: Social engineering, phishing attack.

A phishing attack is a form of social engineering by which cyber criminals attempt to trick individuals by creating and sending fake emails that appear to be from an authentic source, such as a business or colleague. The email might ask you to confirm personal account information such as a password or prompt you to open a malicious attachment that infects your computer with malware.

Result: The hotel's cash reserves were depleted. The fraudulent transfers amounted to more than ₹1 million. The hotel also contacted a cybersecurity firm to help them mitigate the risk of a repeat attack.

Impact: The business lost ₹1 million, and the funds were not recovered. Further there was loss of business reputation too.

Lessons Learned:

- Train the staff about the dangers of clicking on unsolicited email links and attachments, and the need to stay alert for warning signs of fraudulent emails. Engage in regular email security training.
- Implement stringent wire transfer protocols and include a secondary form of validation (Multi Factor Authentication)
- Have a cyber incident response plan ready to implement.

5.4 Control considerations for Cyber Risks:

Apart from having the cyber security policies, procedures, framework and regular assessment in place, management should have a strong and updated internal controls to ensure they are covered from cyber risks:

© The Institute of Chartered Accountants of India

1) Controls around vendor setup and modifications:

Certain cyber schemes exist in which changes to bank account or other critical vendor information are requested through email phishing scams by individuals purporting to be authorized vendor personnel.

Entities have inappropriately dispersed funds to these individuals and therefore inappropriately reduced the liability owed to the actual vendor, resulting in an impact to the financial statements (i.e., loss of cash and related expense)

– 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:

Wire transfers or electronic funds transfers, similar to vendor changes noted above, cyber schemes pertaining to fraudulent requests for wire transfers are made relating to business transactions and vendor payments, as well as fraudulent requests appearing to come from financial institutions requesting disbursement from customer asset accounts.

– Are personnel responsible for wire transfers educated on the 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 0 wire transfers?

3) Controls around patch management:

Cyber and ransomware attacks exploit known security vulnerabilities resulting in the manipulation or the destruction of data. Exploitations of known security vulnerabilities are often caused by unapplied patches or upgrades.

© The Institute of Chartered Accountants of India

– 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 by external vendors (e.g., Microsoft for Windows patches)?

5.5 Remote Audit

Remote audit or virtual audit is when the auditor uses the online or electronic means to conduct the audit. It could be partially or completely virtual, auditor engages using technology to obtain the audit evidence or to perform documentation review with the participation of the auditee.

Audit planning and scoping is crucial in every audit. This includes a discussion of the scope and schedule, and the ways to conduct audit. The COVID-19 pandemic has changed the entire business landscape and processes have been adjusted to this new situation, where remote audit is appreciated by clients as well.

Considerations for remote audit:

Auditors must develop tailored strategies to ensure the remote audit meets the requirements and deliver results equivalent to traditional onsite audits.

Feasibility and Planning

- Planning should involve 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 is determining what technology may be used, if auditors and auditees have competencies and that resources are available.
- The execution phases of a remote audit involve video/tele conferencing with auditees. The documentation for audit evidence should be transferred through a document sharing platform.

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. The information, once reviewed and 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, which may require additional agreements from both sides (e.g., there will be no recording of sound and images, or authorizations to using people's images). Auditors should not take screenshots of auditees

© The Institute of Chartered Accountants of India

as audit evidence. 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). VPN is a service which creates safe and encrypted online connection. It prevents unauthorized users to enter into network and allows the users to perform work remotely.

Risk assessment

- The communication from auditor as well as auditees need to clear and consistent, and this becomes crucial during remote audit. The risks for achieving the audit objectives are identified, assessed and managed. The assessment if remote audit would be sufficient to achieve the audit objectives should be done and documented for each audit involving all members of the audit team and the audited organization representative.

Advantages and Disadvantages of remote audit:

ADVANTAGES	DISADVANTAGES
Cost and time effective: No travel time and travel costs involved.	Due to network issues, interviews and meetings can be interrupted.
Comfort and flexibility to the audit team as they would be working from home environment,	Limited or no ability to visualize facility culture of the organization, and the body language of the auditees. Time zone issues could also affect the efficiency of remote audit session
Time required to gather evidence can spread over several weeks, instead of concentrated into a small period that takes personnel from their daily activities.	The opportunity to present doctored documents and to omit relevant information is increased. This may call for additional planning, some additional/different audit procedures, Security and confidentiality violation.
Auditor can get first-hand evidence directly from the IT system as direct access may be provided.	Remote access to sensitive IT systems may not be allowed. Security aspects related to remote access and privacy needs to be assessed
Widens the selection of auditors from global network of experts.	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.

Remote auditing plays a vital part, and provide assurance when unprecedented circumstances, like COVID. It provides an opportunity for organisations and auditors to leverage communication technology tools. In addition, management perception about remote audits is changing as it provides

© The Institute of Chartered Accountants of India

flexibility in terms of time ensuring that day-to-day business activities are not impacted, along with the reductions in cost.

Auditor should also consider while performing audit using remote means, if access to system and network is provided post appropriate approvals both to employees who are working remotely and to auditors who are auditing remotely and if data is transferred through encrypted means to maintain data privacy. Management should maintain and review the list of people who are working remotely and make sure they access the system and network through VPN (Virtual Private Network) only and such accesses should be approved. Further once the employee leaves the organisation or audit is completed such VPN access should be terminated timely. Auditors can test such controls while performing remote audit.

6. EMERGING TECHNOLOGIES IN AUDIT

Emerging technologies are altering the financial reporting environment substantially, and this change is accelerating. Some examples of emerging technologies are – Data analytics (CAATs (ACL, Alteryx, Power BI, CaseWare), artificial intelligence (AI), robotic process automation, and blockchain. These are changing the way business gets done, and auditors are leading by transforming their own processes.

As the use of emerging technologies in the financial reporting process increases, it becomes important for auditor and the client to upskill on the emerging technologies. Some important considerations for auditors are to assess the impact of emerging technologies on business and evaluate whether management is properly assessing the impact of emerging technologies on internal control over financial reporting.

Data Analytic Techniques

Generating and preparing meaningful information from raw system data using processes, tools, and techniques is known as Data Analytics. Audit analytics or audit data analytics involves analyzing large sets of data to find actionable insights, trends, draw conclusions and for informed decision making. The use of audit analytics enables greater efficiencies and more accurate findings from the review process.

As a result, businesses will be able to create strategies based on verifiable data and professional assumptions and auditors can improve the audit quality. It allows auditors to more effectively audit the large amounts of data held and processed in IT systems in larger clients.

© The Institute of Chartered Accountants of India

Audit analytics helps:

- To discover and analyze patterns
- Identifying anomalies
- Extract other useful information in data

The data analytics methods used in an audit are known as Computer Assisted Auditing Techniques or CAATs. It involves use of multiple data analytical tool or visualization tools that can help the auditor to deep dive into the problem statement and hence increase the audit quality. This also minimizes the scope of missing out on key attributes that might be of a higher risk to the organization and its respective business.

Auditor performing audit analytics can make use of various applications and tools that help them to analyse large data sets and obtain insights that help them to make the quality of the audit better. Some of the popular tools used across the industry as part of CAATs are listed below:

1. ACL - Audit Command Language (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, the entity provided the General Ledger dump and system Trial Balance. Using ACL, the completeness of the data can be ensured as the data set exceeded beyond the capacity of the excel and basic functions like record count, sum, pivoting can be performed within ACL where excel could not perform such actions.

2. Alteryx - Alteryx is used to consolidate financial or operational data to assess controls. A fully transparent audit trail of every action is performed in Alteryx in form of a workflow which makes it easier for the user to learn as no prior knowledge of coding or scripting is required. Alteryx can also be leveraged to automate analytics and perform Machine Learning to search for patterns indicative of fraud or irregularities speed up your processes like accounting close, tax filings, regulatory reporting, forecast creation etc. It can also be used to automate set procedures that are performed periodically like reconciliations, consolidations, marketing workflows, system integrations, continuous audits etc.

   Alteryx used for logistics organization to recompute the revenue entries recorded by the system to match with the financials that showcased the expected revenue turnover. Due to Alteryx's processing speed and ease to

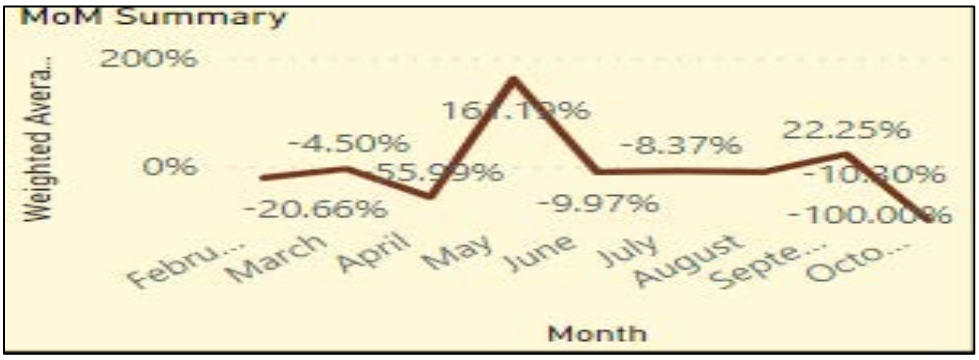
© The Institute of Chartered Accountants of India

implement functions, auditors could perform re-computation for all the transactions entry and noted that the revenue was being understated as the expected revenue was more than the actual calculated. This was due the fact that the addendum between the logistic company and the 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, it can also be used for reporting purpose (audit reports) in an interactive dashboard to the higher management.

Power BI dashboard used for checking the outliers of the apparel company. Auditors were required to analyse the trends of the sales during the year. By the use of Power BI, the sales data provided by the client was further converted into dashboard to analyse the trends and patterns as per the market standards.

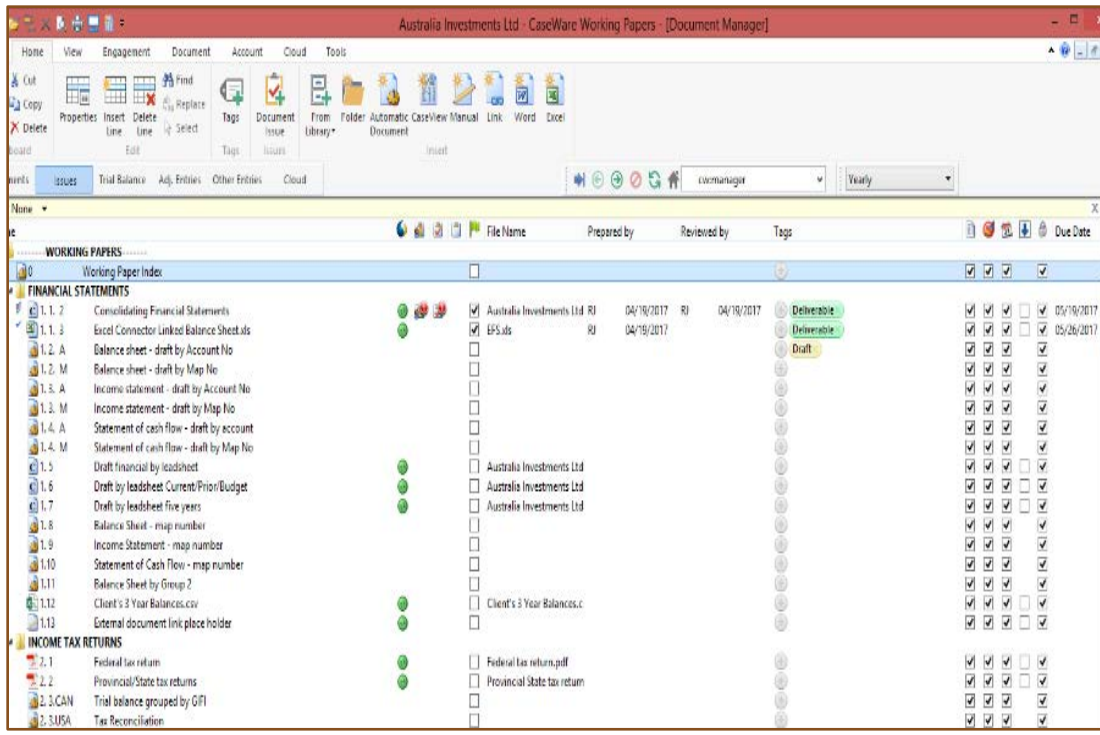
In analysis performed on untimely sales, it was noted that sales transactions were performed during non-business hours. Illustrative charts below which were utilized as part of the analysis by the auditors.



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. It helps in streamlining processes and eliminating the routine tasks. Used by accounting firms, governments and corporations worldwide, this trusted platform integrates everything you need to conduct assurance and reporting engagements.

© The Institute of Chartered Accountants of India

CaseWare provides the solutions to build accounting software which turns any document, including financial statements into cost effective client ready report. It automatically links to client data and securely communicate with the client in real time. Regardless of location, all authorized users have access to the same documents. Consistency of data is ensured. Refer screenshot below to illustrate audit, review and compilation process maintained on-screen.



TEST YOUR UNDERSTANDING 2

CA Y is planning to use CAATs extensively in audit of a company-be it for compliance tests or substantive tests. Can you list out examples of few situations (in brief) of tests performed by him using CAATs?

7. AUTOMATED TOOLS IN AUDIT

Enterprises are adopting emerging technologies at a rapid pace to create synergies and harness the latest technologies.

© The Institute of Chartered Accountants of India

Robotic process automation (RPA), blockchain, machine learning, Internet of Things (IOT) and artificial intelligence (AI) are some prime examples of automation.

Automation and use of technology often requiring auditors to understand and perform procedures on a larger group of systems that produce information relevant to the production of financial statements.

Based on managements and auditors' independent risk assessment procedures, the audit's scope may need to include peripheral systems, as well as testing general IT and application controls relative to those systems due to the increased use of technology that is relevant to financial reporting.

7.1 Internet of Things

IoT is the concept of connecting any device (cell phones, coffee makers, washing machines, and so on) to the internet. Key components of IoT are data collection, analytics, connectivity, and people and process. IoT not only changes the business model, but also affects the strategic objectives of the organization. The risk profile of the entity changes with exposure to new laws and regulations.

Connected Cars, connected manufacturing equipment's, smart home security, (The options for home security from doorbell cameras or outdoor cameras - users can view video feeds when they are away from home) or Data from machines can be used to predict whether equipment will break down, giving manufacturers advance warning to prevent long stretches of downtime. Or a refrigerator placing an order with a grocery store whenever the supply of eggs falls below a certain number. Or smart oven works by scanning QR or bar codes and connecting to Wi-Fi, which it then uses to determine the best temperature and time to cook the food to avoid undercooking or burning. Researchers uses IoT devices to gather data about customer preferences and behavior, though that can have serious implications for privacy and security.

Audit Implications

A shift to connected devices and systems may result in auditors not being able to rely only on manual controls. Instead, auditors may need to scope new systems into their audit. Audit firms may need to train and upskill auditors to evaluate the design and operating effectiveness of automated controls.

Consumer-facing tools that connect to business environments in new ways can impact the flow of transactions and introduce new risks for management and auditors to consider. Consider payment processing tools that allow users to pay via credit card at a retail location through a mobile device.

© The Institute of Chartered Accountants of India

This could create a new path for incoming payments that may rely, in part, on a new service provider supplying and routing information correctly. Auditors would need to consider the volume of those transactions and the processes and controls related to it.

Common risks of IoT:

The key risks associated with IoT, including, device hijacking, data siphoning, denial of service attacks, data breaches and device theft.

7.2 AI (Artificial intelligence)

Artificial intelligence (AI) refers to a system or a machine that can think and learn. AI systems utilize data analysis and algorithms to make decisions based on predictive methods. Complex algorithms are developed to propose decisions based on a pattern or behavior learned over time.

Self-driving cars, manufacturing robots, smart assistants, marketing chatbots, virtual travel booking agent. The self-deploying robots can determine how much vacuuming there is to do based on a room's size, uses AI to scan room size, identify obstacles and remember the most efficient routes for cleaning.

Siri to help find your Air Pods or told Amazon Alexa to turn off the lights, quick commands to open a phone camera or start a particular playlist, AI to predict when to book the lowest prices for flights, hotels, car and vacation home rentals. Using historical flight and hotel data, AI will also recommend to the user whether the booking has reached its lowest price point or if the user should hold out a bit longer for the price to drop.

Auditor Implications

Given the invisible nature of algorithms, audits must focus on the logical flow of processes. A review of AI should ascertain whether unintended bias has been added to the algorithms. Auditors should assess the effectiveness of algorithms and whether their output is appropriately reviewed and approved. Because AI is built on software modules, auditors must also consider cybersecurity and search for possible bugs and vulnerabilities that can be exploited to impact AI functionality. 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. Auditors also should consider whether the AI is making decisions—or being utilized by management as part of the decision-making process.

© The Institute of Chartered Accountants of India

If management shifts its focus on oversight by relying on AI, auditors should understand what shift occurred, how new risks might be addressed, and whether existing risks may not be getting the same level of attention. Understanding these changes could drive changes in the audit approach.

Common risks for AI

AI comes with list of risks. Security is one of the key risks – the more data the system uses, from more sources, the more entry points and connections are formed and the greater the potential risks. 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. Data privacy - The data used and shared should have the necessary explicit consent from data providers.

7.3 Blockchain

Blockchain is based on a decentralized and distributed ledger that is secured through encryption. Each transaction is validated by the blockchain participants, creating a block of information that is replicated and 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.

Bitcoin, cryptocurrency transfer application - Blockchain in money transfer, blockchain smart contracts.

Audit Implications

Auditors should consider the appropriate governance and security transactions around the transactions. Although blockchain's core security premise rests on cryptography, there are risk factors associated with it. As blockchain interacts with legacy systems and business partners, concerns related to insecure application programming interfaces (APIs), data confidentiality and privacy cannot be ignored.

Weak blockchain application development protocols are something auditors cannot overlook. Similarly, data privacy laws and regulations may be area of concern as data are communicated across geographic boundaries. Auditors must be able to determine whether the data put on blockchain will expose the enterprise to liability for noncompliance with applicable laws and regulations.

© The Institute of Chartered Accountants of India

Common risks for blockchain technology

The strengths of blockchain can also be its weaknesses. The 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. Operating through network nodes could also expose the organisation to cyber-attacks and data hacks, so security issues are important. Auditors should also ensure that the organisation has the necessary data management processes and complies with regulations. The regulatory landscape is still evolving for blockchain, so audit teams should check that compliance managers are following developments constantly and adapting processes accordingly.

7.3.1 NFT (Non-Fungible Token)

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 the 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.

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.

Challenges of NFT –

NFTs has its own challenges like ownership and copyright concerns, security risks, market is not that wide, online frauds etc. NFT audit considerations includes comprehensive code review for verifying the safety of a token, valid contract, data privacy and potential cyber threat.

© The Institute of Chartered Accountants of India

Case Study

XY Bank, headquartered in New York, offers a broad range of financial services including asset management, commercial banking, investment banking, and treasury and securities services.

The Five Indian banks in partnership with XY bank, provide a comprehensive range of banking services and products encompassing retail banking, corporate banking, international banking, and other financial services. All these banks have been significant contributors to the digitalization of banking services in India.

Under the pilot programme, the Indian banks will open on-chain Nostro accounts with XY Bank branch in Gift City. The blockchain-based system is expected to facilitate instant, 24×7 settlement between the accounts held at the US bank. Essentially, it will create a private intra-correspondent banking network, redefining the traditional banking hours and enabling seamless money transfer.

Following are the illustrative steps for performing audit of above said block chain:

(a) Obtain a comprehensive understanding of the blockchain-based pilot program, including its objectives, scope, and key processes involved.

(b) Review the partnership agreements, contracts, and legal documentation governing the relationship between the Indian banks and XY Bank.

(c) Identify the specific blockchain technology used, its functionalities, and the underlying smart contracts.

(d) Assess Internal Controls:

Review policies and procedures related to the on-chain Nostro accounts, settlement processes, and money transfer mechanisms.

Assess the governance framework, risk management practices, and compliance procedures established by the Indian banks and XY Bank.

(e) Review Security Measures:

Assess encryption methods, cryptographic key management, and secure transmission protocols used for data protection.

Review measures taken to prevent unauthorized access, cyber threats, and potential vulnerabilities in the blockchain network.

(f) Test Transaction Validity and Accuracy:

© The Institute of Chartered Accountants of India

Validate that transactions are recorded and settled accurately on the blockchain, ensuring adherence to relevant regulations and contractual obligations.

Perform reconciliations between on-chain Nostro accounts and the corresponding accounts held at XY Bank to confirm the accuracy of balances and transactions.

(g) Evaluate Compliance and Regulatory Requirements:

Review documentation and procedures related to customer due diligence, transaction monitoring, and reporting obligations.

Ensure that the pilot program adheres to industry-specific standards and best practices.

(h) Assess Business Continuity and Disaster Recovery:

Evaluate the adequacy of backup and recovery procedures, redundancy measures, and failover mechanisms to ensure uninterrupted operations.

Test the effectiveness of these plans by conducting simulations or examining historical incidents and response procedures.

(i) Report Findings and Recommendations:

Provide recommendations for improving internal controls, security measures, compliance procedures, and overall efficiency and effectiveness of the pilot program.

Communicate the audit results to the relevant stakeholders, highlighting areas of concern and suggesting remedial actions.

7.4 Robotic Process Automation

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

Case Study

A large passenger carrier is having an AI bot for passenger ticket booking with following processes:

User Interaction: The bot interacts with passengers through various channels such as a website, mobile app, or messaging platforms. Passengers can initiate a conversation with the bot by providing their travel details, preferences, and other required information.

© The Institute of Chartered Accountants of India

Natural Language Processing (NLP): The bot utilizes natural language processing techniques to understand and interpret the passenger's queries and requests. It can process text or voice inputs and extract relevant information to facilitate ticket booking.

Query Handling: The bot responds to passenger queries related to ticket availability, fares, train schedules, seat preferences, and other relevant information. It can provide real-time updates and answers to common passenger questions.

Booking Process: Upon receiving a booking request, the bot collects the necessary details from the passenger, including travel dates, destinations, class preferences, and passenger information. It validates the inputs, checks seat availability, and calculates fares based on the carrier's pricing structure.

Integration with Booking Systems: The bot interfaces with the carrier's booking systems to check seat availability, reserve seats, and process payment transactions. It securely communicates with the backend systems to initiate the booking process.

Payment Processing: The bot facilitates secure payment transactions, allowing passengers to provide payment details and complete the booking. It may integrate with various payment gateways or services to process credit card payments, net banking, or other payment methods.

Confirmation and Ticket Generation: Once the booking is successfully processed, the bot generates a booking confirmation along with a unique ticket number. It provides the passenger with the necessary information, including the ticket details, train information, and any other relevant instructions.

Ancillary Services: The bot may offer additional services such as seat upgrades, meal selection, travel insurance, or other ancillary offerings. It can provide information and assist passengers in availing these services during the booking process.

Post-Booking Support: The bot can assist passengers with post-booking support, including itinerary changes, cancellations, or ticket modifications. It handles these requests, checks the carrier's policies, and processes the necessary changes as per the passenger's requirements.

Integration with Customer Support: The bot may be integrated with customer support systems to escalate complex queries or issues to human agents when necessary. It can provide a seamless transition from automated assistance to human interaction, ensuring a high level of customer service.

Following are the illustrative steps to audit ticket booking bot system:

- Identify the objectives and goals of auditing the IRCTC ticket booking bot.

© The Institute of Chartered Accountants of India

- Determine the scope of the audit, including the specific aspects of the bot's functionality and operations to be evaluated.
- Review relevant regulatory and compliance standards applicable to the ticket booking process, such as data protection and privacy regulations, payment card industry standards, and any specific industry guidelines.
- Identify and assess potential risks associated with the ticket booking bot, such as unauthorized access to customer data, system failures, or inaccurate booking information.
- Develop a comprehensive set of audit procedures to assess the effectiveness, efficiency, and compliance of the ticket booking bot. This may include:
- Reviewing the system architecture, design, and documentation.
- Evaluating the security measures in place, including authentication, access controls, and encryption.
- Testing the bot's functionality by simulating booking scenarios and verifying the accuracy of the results.
- Assessing the performance of the bot, such as response times and scalability.
- Analyzing logs and audit trails to detect any unusual or suspicious activities.
- Examining the data handling processes, ensuring proper encryption, storage, and protection of customer data.
- Verifying compliance with relevant regulations, policies, and procedures.
- Conducting penetration testing or vulnerability assessments to identify potential weaknesses in the bot's security.
- Decide on the appropriate sampling methodology to evaluate the bot's performance and compliance. This may involve selecting a representative sample of booking transactions or data for analysis.
- Conduct the audit based on the defined procedures, following best practices and professional audit standards.
- Document your findings, including any issues or areas of improvement identified during the audit.
- Compile the audit findings into a comprehensive report, detailing the audit objectives, scope, procedures performed, and results.

© The Institute of Chartered Accountants of India

- Provide recommendations for addressing any identified weaknesses, risks, or non-compliance issues.
- Present the report to relevant stakeholders, such as management, IT teams, and compliance officers.
- Track the implementation of recommended actions and ensure appropriate measures are taken to address any identified weaknesses.
- Periodically review and monitor the bot's performance, security, and compliance to ensure ongoing effectiveness.

Audit Implications:

It is of utmost importance for auditors 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.

A comprehensive assurance process might demand review of the source code. To perform substantive testing, auditors must have an understanding of the tools used to develop and maintain RPA. This will be helpful when auditors review logs, configuration controls, privileged access controls and the like. General IT controls are applicable as always.

Common Risks of RPA:

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. Assigning proper responsibilities, training and clearly stating about changing roles also can help you reduce operational risk to a great extent.

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

RPA Strategy Risk: Setting wrong expectations, improper KPIs, and unrealistic business goals creates an environment of uncertainty. Management should discuss, and analyse the complete working characteristics, potential, and limitations of RPA before drafting a robotic process automation.

RPA to check IND AS, IFCoFR and Standards on Auditing.

Incorporating Standards on Auditing, IFCoFR, IND AS (para-wise details of | Para reference | Accounting policy | Relevant data to be captured | Relevant calculation to be made | Presentation in financial statements | IFCoFR | Audit procedures as per Standards on auditing |) in audit practices

© The Institute of Chartered Accountants of India

ensures accurate financial reporting, effective internal controls, and reliable audit procedures. Leveraging RPA in conjunction with these frameworks can significantly enhance audit efficiency, accuracy, and compliance. RPA developers and auditors should collaborate to align RPA workflows with relevant standards and guidelines, ultimately improving the effectiveness of audits and enhancing client assurance given below:

Columnar Presentation of IND AS 16 - Property, Plant & Equipment with IFCoFR and Audit Procedures						
Para ref.	Accounting policy	Relevant data to be captured	Relevant calculation to be made	Presentation in financial statements	IFCoFR	Audit procedures as per Standards on auditing
6	Define PPE as tangible assets that are held for use in the 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.	Identify PPE items and their cost components.	Apply recognition criteria and measurement principles.	Disclose PPE items and their carrying amounts, depreciation methods and rates, useful lives, impairment losses, etc.	Establish internal controls over the identification, recognition, measurement, depreciation, impairment, and disclosure of PPE.	Verify the existence, ownership, valuation, and disclosure of PPE by inspection, confirmation, vouching, analytical procedures, etc.
7	Recognize an item of PPE as an asset if it is probable that future economic benefits associated with the item will flow to the entity; and the cost of the item can be measured reliably.	Assess the probability and reliability of future economic benefits and cost of PPE items.	Apply cost model or revaluation model for subsequent measurement of PPE items.	Disclose the basis of recognition and measurement of PPE items.	Establish internal controls over the assessment of probability and reliability of future economic benefits and cost of PPE items.	Verify the recognition criteria and measurement basis of PPE items by inspection, confirmation, vouching, analytical procedures, etc.

© The Institute of Chartered Accountants of India

8	Measure the cost of an item of PPE as the cash price equivalent at the recognition date. If payment is deferred beyond normal credit terms, measure the cost at the present value of all future payments.	Identify the cash price equivalent and the present value of deferred payments for PPE items.	Calculate the present value of deferred payments using an appropriate discount rate.	Disclose the cash price equivalent and the present value of deferred payments for PPE items.	Establish internal controls over the identification and calculation of cash price equivalent and present value of deferred payments for PPE items.	Verify the cash price equivalent and present value of deferred payments for PPE items by inspection, confirmation, vouching, analytical procedures, etc.
9	Include in the cost of an item of PPE any costs directly attributable to bringing the asset to the location and condition necessary for it to be capable of operating in the manner intended by management. Exclude any costs that are not directly attributable to bringing the asset to that location and condition.	Identify the directly attributable costs and the non-attributable costs for PPE items.	Allocate the directly attributable costs to PPE items based on a rational and consistent basis. Exclude any non-attributable costs from PPE items.	Disclose the directly attributable costs and the non-attributable costs for PPE items.	Establish internal controls over the identification and allocation of directly attributable costs and non-attributable costs for PPE items.	Verify the directly attributable costs and non-attributable costs for PPE items by inspection, confirmation, vouching, analytical procedures, etc.

© The Institute of Chartered Accountants of India

10	Include in the cost of an item of PPE any borrowing costs that are directly attributable to the acquisition, construction or production of a qualifying asset as part of the cost of that asset in accordance with Ind AS 23 Borrowing Costs. A qualifying asset is an asset that necessarily takes a substantial period of time to get ready for its intended use or sale.	Identify the borrowing costs and the qualifying assets for PPE items.	Allocate the borrowing costs to qualifying assets based on a rational and consistent basis.	Disclose the borrowing costs and the qualifying assets for PPE items.	Establish internal controls over the identification and allocation of borrowing costs and qualifying assets for PPE items.	Verify the borrowing costs and qualifying assets for PPE items by inspection, confirmation, vouching, analytical procedures, etc.
11	Exclude from the cost of an item of PPE any trade discounts and rebates	Identify the trade discounts and rebates for PPE items.	Deduct the trade discounts and rebates from the cost of PPE items.	Disclose the trade discounts and rebates for PPE items.	Establish internal controls over the identification and deduction of trade discounts and rebates for PPE items.	Verify the trade discounts and rebates for PPE items by inspection, confirmation, vouching, analytical procedures, etc.
15	Recognize the cost of a self-constructed asset as the cost of an item of PPE.	Identify the self-constructed assets and their cost components.	Apply the same principles as for an acquired asset.	Disclose the self-constructed assets and their costs.	Establish internal controls over the identification and measurement of self-	Verify the self-constructed assets and their costs by inspection, confirmation, vouching,

© The Institute of Chartered Accountants of India

					constructed assets.	analytical procedures, etc.
31	Review the residual value, useful life and depreciation method of an asset at least at each financial year-end and, if expectations differ from previous estimates, account for the change as a change in an accounting estimate in accordance with Ind AS 8 Accounting Policies, Changes in Accounting Estimates and Errors.	Identify the residual value, useful life and depreciation method of PPE items.	Assess whether there is any indication of change in expectations from previous estimates.	Adjust the depreciation charge accordingly and disclose the nature and effect of the change in estimate.	Establish internal controls over the review and adjustment of residual value, useful life and depreciation method of PPE items.	Verify the residual value, useful life and depreciation method of PPE items by inspection, confirmation, vouching, analytical procedures, etc.
41	Recognize the cost of replacing part of an item of PPE as an asset if it is probable that the future economic benefits embodied within the part will flow to the entity; and the cost of the item can be measured reliably. Derecognize the carrying	Identify the replacement parts and their costs for PPE items.	Assess the probability and reliability of future economic benefits and cost of replacement parts.	Allocate the cost of replacement parts to PPE items and remove the carrying amount of replaced parts. Disclose the replacement parts and their costs for PPE items.	Establish internal controls over the recognition and measurement of replacement parts for PPE items.	Verify the replacement parts and their costs for PPE items by inspection, confirmation, vouching, analytical procedures, etc.

© The Institute of Chartered Accountants of India

	amount of the replaced part.					
57	Derecognize an item of PPE on disposal or when no future economic benefits are expected from its use or disposal. Gain or loss arising from derecognition is included in profit or loss when the item is derecognized.	Identify the disposed or retired PPE items and their carrying amounts.	Calculate the gain or loss on derecognition as the difference between net disposal proceeds and carrying amount.	Recognize the gain or loss on derecognition in profit or loss. Disclose the disposed or retired PPE items and their gain or loss on derecognition.	Establish internal controls over the identification and calculation of gain or loss on derecognition of PPE items.	Verify the disposed or retired PPE items and their gain or loss on derecognition by inspection, confirmation, vouching, analytical procedures, etc.

8. CONTROL CONSIDERATIONS OR OBJECTIVES OF AUDITING DIGITALLY

Emerging technologies can bring great benefits, but they also come with a varied set of substantial risks.

The strength of the auditing profession is the assessment of risks and controls. As they address the challenge of assessing technology risk, auditors can and should focus on the following control considerations:

1. Auditors should gain a holistic understanding of changes in the industry and the information technology environment to effectively evaluate management's process for initiating, processing, and recording transactions and then design appropriate auditing procedures.

2. Auditors, as appropriate, should consider risks resulting from the implementation of new technologies and how those risks may differ from those that arise from more traditional, legacy systems.

3. Auditors should consider whether digital upskilling or specialists are necessary to determine the impact of new technologies and to assist in the risk assessment and

© The Institute of Chartered Accountants of India

understanding of the design, implementation, and operating effectiveness of controls. E.g., cybersecurity control experts, IT specialists in the team etc.

Some examples of technology risks where auditors should test the appropriate controls for relying on the digital systems

- 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 (specific risks might arise when multiple users access a common database)
- The possibility of information technology 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

8.1 Key Steps for Auditors in a Changing Technology Environment

As auditors obtain an understanding of the impact of technology on a company's business, its systems of internal control, and its financial reporting, some important reminders include the following:

- 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.

© The Institute of Chartered Accountants of India

- Understand how the technologies impact the flow of transactions, assess the completeness of the in-scope ICFR systems, and design a sufficient and appropriate audit response.
- Assess the appropriateness of management's processes to select, develop, operate, and maintain controls related to the organization's technology based on the extent the technology is used.

TEST YOUR UNDERSTANDING 3

A company is planning to use Robotics process automation (RPA) to streamline its hiring process. Earlier, the company used to hire from campuses of various management institutes leading to high recruitment costs, inefficient hire yield and resultant lack of diversity. How RPA can be used to automate the hiring process? List out tentative few such steps. What could be likely benefits of using RPA in hiring process?

9. NEXT GENERATION AUDIT

The 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 communication
Repetitive tasks	High value work and capacity for growth
Manual work	Automation
Ad hoc insights	Insights from a broader audit

We live in an era of fast technological progress, with new digital devices, applications, and tools being developed almost on a daily basis. 3D printing, augmented reality (AR) and virtual reality (VR), biotechnology, auditing through drones (also known as an 'Unmanned Aerial Vehicle' (UAV)and

© The Institute of Chartered Accountants of India

quantum technology are some of the most rapidly advancing areas, with many implications for society.

Drone Technology: Using drone technology in the remote locations for stock counts. Drones have great payload capacity for carrying sensors and cameras, thus they can photograph and physically examine the 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, handheld bar scanners, manual counts etc. to optimise quality of deliverables, consolidate audit information and enhance the execution speed while ensuring correctness and completeness of data.

Drone Technology: Using drone technology in the remote locations for stock counts. Drones have great payload capacity for carrying sensors and cameras, thus they can photograph and physically examine the 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, handheld bar scanners, manual counts etc. to optimise quality of deliverables, consolidate audit information and enhance the execution speed while ensuring correctness and completeness of data.

Augmented reality: The technology allows users to view the real-world environment with augmented (added) elements, generated by digital devices.

One famous example was Pokémon Go, a game for mobile devices in which players chase imaginary digital creatures (visible on their mobile phones) around physical locations.

Virtual reality: 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.

Examples of augmented and virtual reality? In architecture and engineering businesses, AR and VR allow architects to see their building plans come to life before being built. In the business sector, these technologies allow products to be previewed or customised, thus improving productivity and offering new marketing possibilities.

In the health sector, AR can provide surgeons with additional information when operating on a patient, such as heartbeat and blood pressure monitoring and virtual x-rays. Vision Pro is essentially

© The Institute of Chartered Accountants of India

an augmented-reality (AR) headset that "seamlessly" blends the real and digital worlds. The device can switch between augmented and full virtual reality (VR) using a dial.

Metaverse: The metaverse is the 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)

The internet offers many experiences today, but tomorrow's Metaverse will feel more interconnected than ever before. We are heading towards mature landscape of virtual spaces with transferable identities and assets enabled by blockchains (NFTs) that are interoperable or interchangeable. It further includes highly automated systems, immersive interfaces, hyperconnected networks and digital reflections.

Some considerations for future –

- Beyond cryptocurrencies, coins, and exchanges, players in the Metaverse will need to consider how to build digital monetary systems and apply economic principles to things like digital land.
- Governance models will become ever more difficult to balance openness and user contribution with strategic direction and innovation.
- Identity in the digital world has historically been different based on the platform utilized. The practical challenge of identity will also have to be considered in the Metaverse (e.g., KYC)
- Synchronicity is the ability for aspects of the Metaverse to be multiplayer, simultaneous, and real-time. This includes transactions and actions happening in the Metaverse and are dependent on the infrastructure of digital economies, networking and computing power required to operate a digital world.

Case scenarios to illustrate the potential application of the metaverse in the financial domain:

- 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. Customers can seamlessly transfer funds, make virtual purchases, and engage in virtual commerce, all within the immersive environment of the metaverse. XYZ Bank leverages the metaverse to provide a convenient and interactive banking experience, attracting tech-savvy customers who value digital innovation.

© The Institute of Chartered Accountants of India

- 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. Investors can diversify their portfolios, participate in virtual auctions, and even showcase their virtual art collections in virtual galleries. Crypto Investments Ltd. leverages the metaverse's decentralized and secure infrastructure to facilitate transparent and efficient transactions of virtual assets.
- 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. Students can engage in simulated investment activities, learn about budgeting and financial planning, and gain hands-on experience through virtual trading simulations. Financial Learning Academy leverages the immersive nature of the metaverse to provide an engaging and practical financial education platform, preparing individuals for real-world financial challenges.
- Virtual Meetings and Conferences: For a leading industry even an organisation hosts a virtual conference within the metaverse. Participants from around the world can access the conference through their virtual avatars. They can attend keynote speeches, panel discussions, and networking events in virtual conference halls. Attendees can interact with industry experts, explore virtual exhibition booths, and establish valuable connections in the financial sector. Global Finance Summit leverages the metaverse to create a global and inclusive conference experience, fostering collaboration and knowledge sharing.
- 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. Users can explore data trends, conduct simulations, and analyze financial performance through intuitive interfaces within the metaverse. Analytics Solutions Inc. leverages the metaverse's immersive capabilities to enhance data-driven decision-making, enabling financial professionals to gain deeper insights into market trends and make informed investment decisions.

Common Risks associated:

Beyond their potential, these technologies also come with challenges such as public safety, cybersecurity, data privacy, data protection, lack of standards and technical challenges. Since they often track movements and data, massive amounts of data are generated about the whereabouts of users. It also raises questions about taxation, jurisdiction, and customer protection. Regulators and

© The Institute of Chartered Accountants of India

auditors have to think of the controls around privacy, data security, governance to make it more regulated.

10. CONCLUSION

Emerging technologies bring opportunities to organizations, but they also expose the enterprise to new risk. Auditors are expected to identify the right balance between cost and benefit of internal controls for mitigating these risk factors. This includes understanding how technology integrates with business, how it is governed, which activities are automated and how they are controlled, what the business impacts are as a result of this automation, and how negative impacts are controlled and monitored. Though auditors are not expected to be experts in every technology, they should be able to identify the risk inherent with these technologies. This includes understanding the technology architecture, the internal control framework embedded in the technology and its integration with business.

Integrated Case Scenario:

Consider the following five situations: -

[A] Safe Health Insurance Limited is a company working in field of health insurance sector. It is now using a claim management system where incoming claims can be immediately identified on the website itself. A form is issued to the customer who signs it. The details are verified by the system against data present in it. Such a system has allowed faster processing of claims, error-free data validation and increased customer satisfaction.

[B] During the course of audit of a company, it is noticed that a cyber attack took place on the data in which files were encrypted and computers got locked. The hacker then demanded a booty for decryption of files which was to be paid in bitcoins.

[C] CA X, auditor of a company, is looking into cyber security risks of the company. He is making inquiries regarding processes and controls relating to privileged account access, patch management program, vendor risk management program. He has also performed external network penetration testing.

[D] "Verificatory" is an entity which can stamp e-mails or any files. It simplifies certifying of e-mails by just e-mailing to them to an e-mail specifically created for each customer. Many law firms can use this service to certify documents. The information is secured by networks of thousands of computers distributed across the globe. It uses cryptographic algorithms. The information can be verified from anywhere in the world. Its hashing and time stamping is of significant evidentiary value.

© The Institute of Chartered Accountants of India

[E] CA X is planning for audit of an entity. The timelines are agreed in a meeting with key management person on an electronic meeting platform. The entity also agrees to provide data electronically. Video-conference meetings are to be held from time to time with the client.

Keeping in view above situations, answer the following questions: -

1 In respect of situation regarding working of insurance company in health insurance sector, which of following technologies has likely been used?

(a) Internet of things

(b) Data analytics

(c) Robotic process automation

(d) Power BI

2. Which type of cyber attack is referred to situation described in para [B]?

(a) Ransomware

(b) Trojan

(c) Denial of service attacks

(d) Fileless Malware

3. In situation described at [C] above, which is not part of risk assessment procedures to assess cyber security risks?

(a) Making inquiries regarding processes and controls relating to privileged account access

(b) Making inquiries regarding processes and controls relating to patch management program

(c) Making inquiries regarding processes and controls relating to vendor risk management program

(d) Performing external network penetration testing

4. The kind of services being provided by an entity described at [D] above, are example of use of: -

(a) Blockchain technology

(b) Internet of things

© The Institute of Chartered Accountants of India

(c) Ethical hacking

(d) Cyber attestation

5. Which of following is false in an audit described at para [E]?

(a) The opportunity to present doctored documents and to omit relevant information is decreased.

(b) Remote access to sensitive IT systems may not be allowed.

(c) It provides comfort and flexibility to the audit team as they would be working from their office/home environment.

(d) Time zone issues could also affect the efficiency of audits.

Key Takeaways

- A digital audit improves the quality of opinion. This consequently leads to a more reliable audit report. It leads to savings in time, cost and human effort which can be utilized towards more productive tasks.
- Auditing digitally is using the 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.
- It is necessary for an auditor to understand key areas of automated environment. Such key areas include understanding flow of transaction, identification of significant systems, identification of manual and automated controls and identification of technologies used.
- It is also imperative upon an auditor to identify the risks arising from the use of IT. The auditor may consider the nature of the identified IT application.
- Applicable risks arising from the use of IT may also be identified related to cybersecurity. It is more likely that there will be more risks arising from the use of IT when the 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.
- Cyber risks have to considered like a business risk. It is necessary for an auditor to understand cyber risk strategy of an entity. It should include gaining some knowledge about cybersecurity framework of an entity.

© The Institute of Chartered Accountants of India

- Cybersecurity framework includes how management is identifying the risk, protecting and safeguarding its assets (including electronic assets) from the risk, management preparedness to detect the attacks, anomalies and responsiveness to the adverse event.
- Apart from having the cyber security policies, procedures, framework and regular assessment in place, management should have a strong and updated internal controls to ensure they are covered from cyber risks. Such controls could include controls over vendor setup, electronic fund transfer and patch management etc.
- Emerging technologies in business are also transforming auditing landscape. Data analytics, artificial intelligence (AI), robotic process automation, and blockchain are some of such technologies.
- Auditing digitally also has to assess technology risk considerations like relying upon programs which are inaccurately processing the data, issue of technological personnel gaining access privileges beyond those necessary to perform their duties, inability to access data as required, cybersecurity risks etc.

TEST YOUR KNOWLEDGE

Theoretical Questions

1. *Briefly describe the advantages and challenges of Auditing digitally.*
2. *What are the stages involved in understanding the IT environment and what key considerations auditor should consider?*
3. *Auditor should scope in ITGCs to tests when there are IT dependencies identified in the system. Briefly describe the types of IT dependencies.*
4. *What does cyber risk explain it with some examples.*
5. *Briefly describe the cyber security Framework.*
6. *What are the advantages and disadvantages of remote audit?*
7. *In an automated environment, the data stored and processed in systems can be used to get various insights into the way business operates. This data can be useful for preparation of management information system (MIS) reports and electronic dashboards that give a high-level snapshot of business performance. In view of above you are required to briefly discuss the meaning of data analytics and example of such data analytics techniques.*

© The Institute of Chartered Accountants of India

8. *Enterprises are adopting emerging technologies at a rapid pace to create synergies and harness the latest technologies. Give 3 examples of automated tools used as a part of emerging technologies along with the risk and audit considerations associated with these tools.*

9. *Emerging technologies can bring great benefits, but they also come with a varied set of substantial risks. Give some examples of technology risks of digital system and the control considerations to consider while assessing technology risk.*

10. *Give example of emerging technologies available for Next Generation Audit along with the risks associated with it.*

Answers to Test Your Understanding Questions

1. The cyber risks are not an issue of IT alone. Rather, it is a business risk and has an effect on whole business organization. It affects entity's reputation and can lead to many other consequences which are listed below: -
   - 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
   - Intellectual property theft which may not only take the competitive advantage, but we may also result in any impairment/impediment 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

   It may happen that many cyber attacks are not directly targeted at financial systems. However, the access gained by the attackers may provide them the ability to:

   - Manipulate or modify financial records
   - Modify key automated business rules
   - Modify automated controls relied upon by the management.

   Further, auditor should consider whether cyber risk (like other business risks) represents a risk of material misstatement to the financial statement as part of the audit risk assessment activities. Focus should be on understanding the cyber risks affecting the entity and the actions being taken to address these risks.

© The Institute of Chartered Accountants of India

2. (i) *Identify exceptions:* Identify exceptional transactions based on set criteria. For example, cash transactions above ₹ 10,000.

   (ii) *Identify errors:* Identify data, which is inconsistent or erroneous. For e.g.: account number which is not numeric.

   (iii) *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.

   (iv) *Existence of records*: Identify fields, which have null values. For example: invoices which do not have vendor name.

   (v) *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.

   (vi) *Data consistency:* Identify data, which are not consistent with the regular format. For example: invoices which are not in the required sequence.

   (vii) *Duplicate payments:* Establish relationship between two or more tables as required. For example, duplicate payment for same invoice.

   (viii) *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.

3. RPA can be used to streamline hiring process in a company. The tentative steps could include: -

   - Place advertisements on social media/career advice sites.
   - Link redirects candidate to a career site.
   - Career site pulls information of candidate.
   - An algorithm scans applicants for desired and suitable roles.
   - Selected candidates may be asked to play online games to assess their skills.
   - A certain percentage of those applicants are called for a video interview using an interview software.

The automated hiring process will reduce full time effort involvement, provide with a wider assessment range, reduce the impact of recruiter biases, increase the efficiency of mapping of interested candidates, reduce recruiting costs, increase hire yield, reduce time to hire, increase diversity.

© The Institute of Chartered Accountants of India

Answers to Integrated Case Scenario:

1. (c)
2. (a)
3. (d)
4. (a)
5. (a)

Hints /Answers to Theoretical Questions:

1. Advantages – Improved efficiency, better quality, lower costs, improved risk assessment.

   Challenges – 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 the roadmap for digital strategy.

   For details refer Para 2.

2. The stages involved in understanding of IT environment are: Understand – Identify – Assess.

   Key considerations - Understand the flow of transaction, Identification of Significant Systems, Identification of Manual and Automated Controls, Identification of the technologies used and. Assessing the complexity of the IT environment.

   For details refer Para 3.

3. For details refer para 4.
4. For details refer para 5.1.
5. For details refer para 5.3.
6. For details refer para 5.5
7. For details refer para 6
8. For details refer para 7
9. For details refer para 8
10. For details refer para 9

© The Institute of Chartered Accountants of India

NOTES

© The Institute of Chartered Accountants of India

NOTES

© The Institute of Chartered Accountants of India