DIGITAL AUDIT

[6 to 12 marks]

Q1. What is the concept of auditing Digitally? Its advantages & challenges?

A) Concept

i) Auditing Digitally is using advancements in technology for conducting an effective and efficient audit.

ii) With a rapidly growing IT environment it is essential to adapt technology in auditing practices.

iii) It is time to digitize the way an audit is delivered through automation and innovation.

B) Advantages [A B C D E]

(i) Improved **A**udit Quality:

The impact on Quality of audit is evident through automation and data analytics techniques we can do full population audit instead of sample based audit.

ii) **B**etter Transparency:

- With the technological advancement transparency has been increased.
- 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.

iii) Lower **C**osts:

- By automating processes that were previously done manually, technology can assist with the cost of auditing

iv) **D**ecreasing human dependency

- Technology helps in streamling the process of testing for auditors which decreases the errors which occurs from the judgement of different individuals.

v) Increased Efficiency:
Bcoz of automation tools, simple training & digital upskilling, the result may be increased efficiency and fewer errors.

c) Challanges
following are the challenges:
1) Reluctance to change,
2) Challenges with data security and governance,
3) Choosing the right tool and automating the right process
4) Ensuring Standardisation and correct configurations to avoid error and bias,
5) Evaluating business benefits the org. wants to achieve with automation.
5) Roadmap for digital strategy.

Q2. What are the Range of automated solution available ~~for audit~~.

following are the automated solution:

A) Macros & Scripts
Rules-based automation within a specific application.

b) Business Process Automation (BPA)
Reengineering existing business processes eg. workflows

c) Robotic Process Automation (RPA)
Automating labour-intensive, repetitive activities across multiple systems & interfaces

d) Intelligent Process Automation (IPA)
• Combining RPA with artificial intelligence technologies to identify patterns learn over time, & optimize workflows

Q3. What are the factors for auditors understanding the automated environments shall include?

[COPIA]:

1. **C**omponents of IT infrastructure for each application
2. **O**rganisation structure and governance.
3. **P**olicies, procedures and processes followed.
4. **I** — Extent of IT integration, use of service organizations. IT risks and controls
5. **A**pplications that are being used by the Co.

Example of how auditor can document the automated environment.

Application	Used for	Database	Operating System	Network	Server & Storage.
KOTS	Restaurant & Kitchen orders	MS-SQL	Windows 2016 Server	In-house developed	HP Server Internal HDD

Q4. What are the Key Areas for the auditor to understand the IT enviroment & its stages?

Following are the stages to understand IT environment.

- UNDERSTAND
- IDENTIFY
- ASSESS.

Following are the Key considerations [FISTA]

i) Understand the **F**low of Transaction:

The auditor should consider various aspects of the IT environment that are relevant to the flow of transaction & processing of info in the information system

Changes in the flow of txns, or info 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 txn's or info.

ii) **I**dentification of Manual & Automated controls.

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.

iii) Identification of **S**ignificant systems :

The auditor may identify the IT application & IT infrastructure which are related to significant class of txn., account balances & disclosures.

iv) Identification of the **T**echnologies used :

The auditor should understand the emerging technologies implemented, the role they play in entity info system and the risk arising from their use.

Some examples of emerging technologies are :

- Block chains including cryptocurrency businesses.
- Robotics
- Artificial Intelligence
- Internet of things
- Biometrics
- Drone.

v) **A**ssessing the complexity of the IT environment :

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.

Q5. What are the various risk to be considered while using IT environment? [LUCI-FE]

① **L**oss of data.

② **U**nauthorised access to data/direct data changes.

③ Unauthorized **C**hanges to systems or programs.

④ **I**naccurate processing of data, processing inaccurate data, or both.

⑤ **F**ailure to make necessary changes to systems or programs

⑥ **E**xcessive access / Privileged access (super users).

Q6. What are the IT dependencies impacting the Audit & name them?

① Identifying & documenting entities IT dependencies in a consistent & clear manner helps to:

(i) Identify the entity's reliance upon IT.

(ii) Understand how IT is integrated into the entity's business model.

(iii) Identify potential risks arising from the use of IT.

(iv) Identify related IT General Controls.

(v) Enables to design & develop an effective and efficient audit approach.

② IT dependencies are created when IT is used to initiate, authorise, record, process or report the txn. for inclusion in financial statement.

③ Following are the 5 types of IT dependencies. [SICAR]

(i) **Security**

Security including segregation of duty is enabled by the IT environment to determine the separation of roles and responsibilities that could allow an employee to perpetrate and conceal errors or frauds, or to process errors that go undetected.

ii) **Interfaces**

Interfaces are programmed logic that transfers data from one IT system to another.
eg, transfering data from payroll sub-ledgers to the general ledger.

iii) **Calculations**

Calculations are accounting procedures that are performed by an IT system instead of a person.
eg, the system will apply the "straight-line" depreciation formula to calculate depreciation of an asset.

iv) **Automated Controls**

These are designed into IT environment to enforce business rules.
eg, Purchase order approval via workflow or format checks. (eg. only on a particular date format is accepted.)

v) Reports:
System generated reports are the info generated by IT system. These are often used in execution of manual controls and business performance review.
[vendor master report, customer aging report]

④ Auditor should considers IT dependencies relevant to audit and evaluate the related risks.
Auditor should scope in ITGCs [Info technology general controls.]
to tests when there are IT dependencies identified in the system.

Q7. What is CYBER RISK?

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

B) TYPES
i) Malware: Malware or malicious S/w is any program or code that is created with intent to do harm to a computer, N/w or server.
It is a most common type of cyber attack.

Following are the types:

RANSOMWARE

In this, an adversary encrypts a victim's data and offers to provide a decryption key in exchange for a payment.

It is done by a phishing emails.

FILELESS MALWARE

It is a type of malicious activity that uses native, legitimate tools built into a system to execute a cyber-attack.

TROJAN

It is installed via social-engineering techniques such as phishing (or) bait websites.

It is a malware that appears to be legitimate S/W disguised as native operating system programs (or) harmless files like free downloads.

MOBILE MALWARE

It is a type of malware designed to target mobile devices via use of unsecured Wifi.

ii) Denial-of-Services (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.

While most DoS attacks do not result in lost data and are typically resolved w/o paying a ransom, they cost the organisation time, money and other resources in order to restore critical business operations.

iii) Phishing

It is a type of cyber attack that uses email, phone, social media, SMS to entice a victim to share sensitive info.

following are the types:

(a) Spear Phishing

It is a type of phishing attack that targets specific individuals or organisations typically through malicious emails.

(b) 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 info or gaining access to the person's computer in order to execute further cyberattacks.

(c) Smishing

It is a type of fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal info.

(d) Vishing

Vishing, a voice phishing attack, is the fraudulent use of phone calls and voice messages pretending to be from reputable org. to convince individuals to reveal private info. such as bank details and passwords.

iv) Spoofing

It is a technique through which a cyber criminal disguises themselves as a known or trusted source.

following are the types:

DOMAIN SPOOFING

It 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.

EMAIL SPOOFING

It is a type of cyberattack that targets the businesses by using emails with forged sender addresses.

v) Identity Based Attacks

When a valid user's credentials have been compromised and an adversary is pretend to be that user.

for eg. if a person uses same id & password for multiple accounts, the cyber criminal may have access to other accounts of the users.

vi) Insider Threats

If a current or former employee pose a danger to an org. because they have access to company's n/w, sensitive data, and intellectual property that would help to carryout such an attack.

vii) DNS Tunneling:

It 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 install a malware or extract sensitive info by encoding it in a series of DNS responses.

viii) 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

Q8. What are stages of Cyber Risk?

[AIM]

Stage 1 - Assessing the cyber risk:

No org. is immune to a cyber risk.

Following are the common threats to an org:-

- Ransomware disabling their org.
- Common criminals using email phishing & hacks for fraud and theft.
- Insiders committing malicious activities or accidental activities

Imp

Stage 2: Impact of cyber risk

The impact of cyber risk can vary from org. to org. Some of the indicative areas are: [FIR BIRD]

1. **F**ines and penalties
2. **I**ncident response cost which could be for investigations & remediations.
3. **R**egulatory costs.
4. **B**reach of Privacy.
5. **I**ntellectual 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.
6. **R**ansomware - more common these days where entire systems are encrypted.
7. **D**ata loss, reputational loss and litigation.

Stage 3: Managing the cyber risk

following are the steps to manage the risk:

1. Gain a holistic understanding of cyber risk, threats facing their org. and other financial institution.
2. Assess the existing cybersecurity program and capabilities against the regulatory requirements

③ Align cybersecurity and IT transformation initiatives with strategic objectives.

④ Understand accepted risks & documented compensating controls.

Q10. Explain cybersecurity framework?

It includes how mgt. identifies the risk, protect & safeguard its assets from the risk and mgt. preparedness to detect the attacks and responsiveness to the adverse events.

Following are the steps:

① Identify the risk [covid symptoms]

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

Entity should conduct a periodic risk assessment & develop a mgt. strategy which identifies cybersecurity risks around IT system failure affecting the entity's primary business or potential loss of data.

② Protect the risk (isolation)

Obtained an understanding of the entity's process 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.

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.

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.

⑤ Recover from risk

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

Q11. What are the control consideration around vendor setup and modification

following are controls:

1. Controls around vendor setup and modifications:

- Who is responsible for making changes to vendor masters data? Is the process centralized or decentralized?

- Are other communication channels, such as email, used to request changes to vendor masters 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 masters data?

- Are authentication protocols defined to verify modifications to vendor masters data (eg. call back procedures, multi-factor authentication)?

Q12. What are the controls around electronic transfer of funds.

following are the controls:

- Are personnel responsible for wire transfers educated on the relevant threats and info related to common phishing scams associated with fraudulent

requests for wire transfers?

- Are authentication protocols defined to verify wire transfer requests (eg. call back procedures, dual-authentication procedures)?

→ What systems and technologies are used to facilitate the request/initiation, authorization and release of wire transfers?

Q13. What are the controls around patch mgt?

following are the controls:

- 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 (eg. microsoft for windows patches)

Q14. Explain Remote Audit? its advantage & Disadvantage?

① Remote Audit or Virtual Audit is when the auditor uses the online or electronic means to conduct the audit.

② It could be partially or completely virtual.

③ The auditor uses technology to obtain the audit evidence or to perform documentation review with the participation of the auditee

④

Advantages	Disadvantages
i) Cost and time effective: No travel time and travel costs involved.	i) Due to network issues, interviews and meetings can be interrupted.
ii) Comfort and flexibility to the audit team as they would be working from home environment.	ii) Time zone issues could also effect the efficiency of remote audit session.
iii) Time required to gather evidence can spread over several weeks, instead of concentrated into a small period that takes personnel from their daily activities	iii) The opportunity to present doctored documents and to omit relevant info is increased.

iv) Auditor can get first-hand evidence directly from the IT system as direct access may be provided

v) Widens the selection of auditors from global n/w of experts.

iv) Remote access to sensitive IT systems may not be allowed. Security aspects related to remote access and privacy needs to be assessed.

v) 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.

Q15. What are the emerging technologies in audit / explain Data analytics techniques along with example of such techniques?

a) Meaning

① Generating and preparing meaningful info from raw system data using processes, tools, and techniques is known as Data Analytics.

② Audit analytics or audit data analytics involves analyzing large sets of data to find actionable insights, trends, draw conclusions and for informed decision making.

B) Audit analytics helps:

i) To discover & analyze patters

(ii) Identifying anomalies

(iii) Extract other useful info in data.

C) Some of the popular tools.

1. **ACL** - Audit Command Language (ACL) Analytics is a data extraction and analysis S/w used for fraud detection and prevention, and risk mgt.

It samples large data sets to find irregularities or patterns in txn's that could indicate control weaknesses or fraud.

2. **Alteryx** - Alteryx is used to consolidate financial or operational data to assess controls.

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.

3. **Power BI** - Power Bi is a business intelligence (BI) platform that provides non technical 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.

4. **Case Ware** - is a data analysis s/w & 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.

Q16. Give 3 examples of automated tools used as a part of emerging technology along with the risk and audit consideration associated with these tools.

Robotic process automation (RPA), block chain, machine learning, Internet of things (IOT) and artificial intelligence (AI) are examples of automation.

a) IOT

① IOT is the concept of connecting any device (cell phones, coffee makers, washing machines, and so on) to the internet.

② 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 org.

③ The risk profile of the entity changes with exposure to new laws and regulations.

b) Artificial Intelligence (AI)

① refers to a system or machine that can think and learn.

② AI systems utilize data ~~analytics~~ analysis and algorithms to make decisions based on predictive methods.

③ Complex algorithms are developed to propose decisions based on a pattern or behavior learned over time.

c) Blockchain

① is based on a decentralized and distributed ledger that is secured through encryption.

② Each txn is validated by the blockchain participant creating a block of info that is replicated and

distributed to all participants.

iii) All blocks are sequenced so that any modification or deletion of a block disqualifies the info.

Q17. Explan Non fungible Token.

a) Meaning

① NFT means something is unique and cannot be replaced.

② NFTs are digital assets, e.g. photos, videos, artwork, sports collectibles etc.

③ NFTs are tokens used to represent ownership of unique items.

④ NFT ~~ad~~ are secured by the blockchain and can only have one official owner at a time.

b) Key Features of NFT

- Digital Asset - NFT is a digital asset that represents wherever 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.

c) Challenges of NFT

① NFTs has its own challenges like ownership and copyright concerns, security risks, market is not that wide, online frauds etc.

② NFT audit considerations includes comprehensive code review for verifying the safety of a token, valid contract, data privacy and potential cyber threat.

Q18. What are the examples of technology risk of digital system and control consideration to consider while assessing technology risk?

① Following are the examples of risk: [LUCI-FE]

Refer Q5

② Following are the control considerations:

① The auditor should gain a holistic understanding of changes in the industry and the info technology environment to effectively evaluate mgt's process for initiating, processing, and recording txn's 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 understanding of the design, implementation, and operating effectiveness of controls.

Q19. Give examples of technologies for Next Generation Audit along with the risk associated with it

Refer Q10 QB Pg 205

Refer Integrated Case MCQ Pg 12.50 module and
Refer 3 test your understanding.