

<http://t.me/cahemantsomani>

CA FINAL AUDIT

DIGITAL AUDITING (Chp 12)

All Concepts + Questions

(Contains: Tricks & Mnemonics)

(May/Nov'25 & Onwards)



Must Join Telegram Channel For:

For FULL PDF & Other Free Notes / Tips:

<http://t.me/cahemantsomani>

By CA Hemant Somani – AIR 46



CLICK HERE :

Connect me on TELEGRAM:

<http://t.me/cahemantsomani>

CA HEMANT SOMANI (AIR-46)

For Free Notes, Qn Banks & Guidance



A Motivation CUM Story

I always needed a single digit rank in CA Final, But Luck factor was not in my favor, just before 15 days of my exams, me & my family got infected by COVID, and last 15 days are equivalent to 3 months, But I didn't loose hope and gave exam at that time also, During exams also I was suffering from many post COVID symptoms

And Finally, I Secured AIR 46 (Not single digit),

I just want to convey that while doing your preparation, "Always Aim for the BEST & Prepare for the Worst scenario"

**For Free
Notes**



<http://t.me/cahemantsomani>



<https://www.linkedin.com/in/ca-hemant-somani-91749a154/>



https://www.instagram.com/ca.hemant_air46/

For Full PDF & Other Notes: Join →




For Free
Notes

<http://t.me/cahemantsomani>

CA Hemant Somani

CHAPTER 12: DIGITAL AUDITING

➤ Digital Audit: (Review entity Digital assets)

Meaning:	Digital Audit is placing assurance on the effectiveness of IT systems implemented in an organization. Technology is becoming an integral part of day-to-day business operations. Organization shall review their technology-related controls to identify gaps & risks for continuous improvement and to ensure regulatory compliance → will allow organizations to build trust with their stakeholders
Key Features:  Student Specific Code <u>(DIN-COST)</u> Costly director laae digital audit k liye...	<p>[Trick: Trick: NSS se accha comprehensive review karo, Reliable decision le paaoge]</p> <ol style="list-style-type: none"> 1) <u>New Technology & Confidence</u>: Digital audit encourages the auditee to embrace the latest technological advancements and provides confidence to auditee to stay updated in a constantly evolving environment 2) <u>Standardize process</u>: Digital Audit allows to standardize processes and allow controls to be implemented to mitigate risk. 3) <u>Save Time/Cost/effort</u>: 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 4) <u>Comprehensive review of technology</u>: 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 5) <u>Reliable Opinion</u>: A digital audit improves the quality of opinion. This consequently leads to a more reliable audit report 6) <u>Informed decisions</u>: It can help auditee to make informed decisions. 7) <u>Digital Strategy</u>: 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
Advantages: [Trick: Bhai "kam paiso " and "kam time" me me > "acchi audit" hori h .. kyuki "risk" pahle hi "Analyse" Karli thi] <u>OR</u> <u>(BIBLE)</u>	<ol style="list-style-type: none"> 1) <u>L- Lower Costs of Audit</u>: By automating processes that were previously done manually, technology can assist with cost of auditing. It shortens time to complete audit, Save cost. 2) <u>E- Enhanced Effectiveness & Efficiency</u>: Increased efficiency → With use of tools & automation techniques, auditee can standardize processes & routine tasks can be automated like automating a reconciliation process that increase efficiency & saves time & costs. 3) <u>B- Better Audit Quality</u>: Technology can 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. 4) <u>I- Improved Risk Assessment</u>: Creating a number of automations to assist with the audit process and streamlined testing improves the risk assessment procedure. mngt & auditors put their testing efforts on sites with a higher ROMM and make informed decisions. 5) <u>B- Better Analytics</u>: Improved analytics capabilities can aid mngt & 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.
Consideration & Challenge of Digital audit: [Trick: CPT	<p>Considerations that organization should keep in mind while using digital technique & automation:</p> <p>[Trick: haa maana ki "Change Difficult" hota h > para agar "Sahiii Process" lagya > to Bahot "benefit" hai par saamne wala bolega ... kya benefit h ye koi "Single solution" to nahi hoa > Technology se "Security risk" bhi to hogi]</p> <ol style="list-style-type: none"> 1) <u>C- Change Difficult</u>: Think people first and do not underestimate change is difficult

me BSR nhi
thaa.. so abhi
challenge h
isse padhna]

(Special Trick
by CA Hemant
Somani ;-)

- 2) **T- Target the right processes** - this is a key for successful automation.
- 3) **P- Process Standardised**: Ensure the process works and it is standardised before automating. Bots do not easily adapt to process change
- 4) **B- What Benefit**: Know what business benefits organization wants to achieve with automation
- 5) **S- Not standalone solution**: Automation is not a standalone solution & should be part of a broader digitalization strategy
- 6) **R- Security Risk**: Automation introduces new challenges for organization. Don't forget about governance and data security in the risk framework.

Auditors will obtain understanding of mngt's implementation & oversight of new technologies, Area include understanding of following:

[Trick: "IC" → "System" & "Process" ki understanding lo]

- a) The **impact the new technology** as how the organization obtains or generates and uses relevant, quality information to support the **functioning of internal control**.
- b) **Changes in the way entity's systems are developed and maintained** and whether these changes introduce new risks and require new controls to respond to those risks
- c) **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)

➤ **Auditing Digitally** : (Doing Audit using Digital tools)

Means:	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. There are new technologies to help capture data, automate procedures, analyse information and focus on the real risks of the client.
Expectations from an Auditor:	<ul style="list-style-type: none">• Involve Expert: Audit teams need to involve the experts on different software applications & technologies. Having right level of expertise of new technology (eg. RPA, AI, blockchain tech)• Automate and enhance existing processes: Investment in technology on developing tools and using tools to automate and enhance existing processes, such as data analytics & collaboration and sharing tools, help to drive quality in audits today• Evolving Scope of audit: Using such technology will also evolve scope of audit
Key Feature / Advantage:	<p>[Trick: ab Jaldi Jaldi kaam koga .. kyuki "Human" to "inefficient" hote h .. "automation" se fatafat kaam ho jaaega > orr "Audit quality" bhi improve hogi.. kyuki "risk" saari "transparent" hogi ab]</p> <ol style="list-style-type: none">i) Improved Efficiency: What used to take weeks to learn and programmes using deep experts, is now easily available to auditors after some simple training and digital upskilling. The result may be increased efficiency & fewer errors, but benefits are wider reaching & personal.ii) Decreasing human dependency: Using technology minimizes the manual intervention which ultimately results in reducing the risk of manual errors. decreases the errors which occur from the judgement of different individuals.iii) Automation and Ease: Automating tasks like recording work in repositories, extracting data & sampling have improved quality of audit & reduced the manual error. Using dashboards (e.g., Power BI) for reporting helps in understanding & helps auditor to form opinion.iv) 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. It free up time for audit teams to analyses the information and better understand the business they audit.v) Increases Transparency: New ERPs and tools have audit trail feature available to trace the

(Special Trick
by CA Hemant
Somani ;-)

	transaction end to end. 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.										
	vi) Better risk assessment : With usage of automation in audit, auditor may focus on real challenges & assess potential risk precisely. It gives time to auditors to focus on the bigger picture rather than being involved with repetitive tasks. Dashboards, visual presentations & other tools helps in understanding where the risk lies & what all areas need more attention.										
Considerations in Auditing Digitally:	There are few questions it is important to ask and answer - at all stages of tech journey:										
	What Problem?	What problems are you trying to solve? → Continuously evaluate emerging technologies & latest tools → to see what can benefit the audit (easier or better)									
	Which tech?	Which technology can help you? → There are number of tools available & many vendors 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									
Join "CA Hemant Somani" Telegram Channel for Full PDF	Upskill People:	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									
	Range:	Range of automated solutions: There is a range of automation solutions, from low to high sophistication → helps to standardize the repeatable tasks → using robotics and automation for data gathering → data analytics									
		<table border="1"> <thead> <tr> <th>Macros and Scripts</th><th>Business Process Automation (BPA)</th><th>Robotic Process Automation (RPA)</th><th>Intelligent Process Automation (IPA)</th></tr> </thead> <tbody> <tr> <td>Rules-based automation within a specific application</td><td>Reengineering existing business processes e.g., workflows</td><td>Automating labour intensive, repetitive Activities across multiple systems</td><td>Combining RPA with artificial intelligence technologies to identify patterns learn over time, and optimize workflows</td></tr> </tbody> </table>	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	Combining RPA with artificial intelligence technologies to identify patterns learn over time, and optimize workflows	
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	Combining RPA with artificial intelligence technologies to identify patterns learn over time, and optimize workflows								

Q1. Briefly describe the advantages and challenges of Auditing digitally. [ICAI SM - AMBIGUOUS]

Hint: ICAI has given Hint in ICAI SM answer as Follows: [ICAI Hint seems to be mixture of Above topic "Digital Audit" & "Auditing Digitally". As per Author, It should be as per Topic "AUDITING DIGITALLY" .. so in exam, Elaborate the answer .. below is just an Hint Given by ICAI]:

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

Challenges - Reluctance to change, challenges with data security and governance, choosing the right tool & automating the right process, ensuring standardisation and correct configurations to avoid error and bias, evaluating business benefits the organization wants to achieve with automation and roadmap for digital strategy.

➤ Understand the AUTOMATED ENVIROMENT (IT):

Q2. Auditor is of view that understanding & using the auditee's automated environment is optional and not required. Do you agree? illustrate by giving one example [AUTOMATED ENVIRONMENT] [OLD]

- 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.

3 Stages as follows:



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

- 1) The **applications** that are being used by the company;
- 2) Details of the **IT infrastructure** components for each of the application;
- 3) The **organisation Structure** and governance;
- 4) The **Policies**, procedures and processes followed;
- 5) IT **risks and Controls**.

The auditor is **required to document** the understanding of a company's automated environment as per **SA 230**.

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

➤ Key Areas for an Auditor to Understand IT Environment:

Q3. What are the stages involved in understanding the IT environment and what key considerations auditor should consider? Or explain the key areas for an auditor to understand IT environment

Hint: 3 Stages are → Understand - Identify - Assess

Trick: *Konsi Technology, system, & control (TCS) use leti h company h > uska flow Flow & Complexity*

Understand flow of transaction:	Auditor's understanding of IT environment may focus on identifying & understanding 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 info. system. Changes in the flow of transactions, or information within the info. 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.
Identification of Significant Systems:	The auditor may identify the IT applications and supporting IT infrastructure concurrently with the auditor's understanding of how info. relating to significant classes of transactions, account balances and disclosures flows into, through and out the entity's info. system.
Identification of Manual and Automated Controls	An entity's system of I.C. contains manual elements and automated elements (i.e., manual and automated controls and other resources used in the entity's system of I.C.). 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 ROMM.
Identification of	The need to understand technologies implemented & role they play in entity's info.

the technologies used:

processing or other F.R. activities & consider whether there are risks arising from their use.

If complex technology → engage expert to 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	Robotics	Artificial Intelligence	Drone
	Internet of Things	Biometrics	

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 Factors such as: automation used in organisation, 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.)

➤ IDENTIFYING THE RISKS ARISING FROM USAGE OF IT

How to identify IT Risk?

Consider the nature of identified IT application → may also be identified related to cybersecurity

More Risks arising use of IT when:

- Volume or complexity of automated application controls is higher
- Mngt placing greater reliance on those controls for effective processing of transactions or the effective maintenance of the integrity of underlying information.

Risk arising from use of IT:

[Data, IT Application, System, Bande]

(Special Trick by CA Hemnt Somani :-)

- Unauthorized access to data that may result in destruction of data or improper changes to data (recording of unauthorized or non-existent transactions)
- Data loss or data corruption (Lack of cyber control → lead to loss of sensitive data/hackers, physical security breach/theft of data)
- Unauthorized changes to IT applications
- Failure to make necessary update IT applications
- There is a risk of system downtime (hardware failures, faulty configurations, cyberattacks or power outage)
- System integration risk: companies uses more than one IT systems, integrating one or more systems) and system compatibility → In case of system failure in one system may also lead to widespread failure in integrated systems (or if hardware/software is not compatible → Risk)
- Possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties (breaking SOD)
- Inappropriate manual intervention.
- With advancement in usage of IT the risk of regulatory compliances increases → Any change in the law, order, guidelines → (Related cost & investment is higher)
[FMCG have different regulatory requirement than Finance company]

Scaling: When performance issue arises in IT system due to heavy data load / network issue → IT systems, resources or hardware can be added to an existing nodes, which is known as scaling (However its expensive)

➤ Know how to identify the IT dependencies impacting the Audit

Why 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.

How IT dependencies arise?

[TYPES]

[Trick: SIA - Ram Chandra]

Join "CA Hemant Somani" Telegram Channel for Full PDF

Q4. Auditor should scope in ITGCs to tests when there are IT dependencies identified in the system. Briefly describe the types of IT dependencies.

How it arise ? : IT Dependencies are created **when IT is used to initiate, authorize, record, process, or report transactions** or other financial data for inclusion in FS

5 Types of IT Dependencies: [SIA - Ram Chandra]

Security	Security including segregation of duties is enabled by the IT environment to restrict access to information and to determine the separation of roles
Interfaces (Qn)	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 subledger to the general ledger
Automated Controls	Automated controls are designed into the IT environment to enforce business rules. For Eg, 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 (Qn)	System generated reports are info. 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 source of entity info. used by us when selecting items for testing, performing substantive TOD or performing a SAP. E.g. (Vendor master report, customer ageing report)
Calculations	accounting procedures that are performed by an IT system instead of a person. (Depreciation by SLM etc.)

Understand & respond risk arise from IT dependency:

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.

ITGC:

- **Mngt** may **implement I.T general controls (ITGCs)** to address risk related to IT dependency
- Auditor should consider **IT dependency relevant to audit** because → IT dependency affect the entity controls
- Auditor should **test ITGC**
- **Do not Rely on ITGC** (i.e., Do not rely on IT dependency) → When controls around IT environment are not implemented

[Refer "Additional PDF Booklet"]

Q5. IT dependencies also arise due to "system generated reports" and "interfaces". How do such IT dependencies arise? Why it is important to identify IT dependencies for Audit?

Hint: refer above → "System generated reports" & "Interfaces" and "Why to identify IT dependency"

➤ Assessing Cyber Risk:

Q6. What does cyber risk explain it with some examples. [Length & points of answer will depend on Marks]

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

Most common types of cyberattacks are:

Malware: Malicious **software is any program or code** that is created with the **intent to do harm** to a computer, network or server (**ransomware**, fileless Malware **trojans**, **viruses** etc.)

Type	Description
Ransomware	Adversary encrypts a victim's data and offers to provide a decryption key in

		exchange for a payment. (malicious links, phishing emails etc.)										
	Fileless Malware	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	legitimate software disguised as native operating system programs or harmless files like free downloads. → installed through social engineering techniques such as phishing or bait websites										
	Mobile 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.										
Denial-of-Service (DoS) Attacks:	Malicious, targeted attack that floods a network with false requests in order to disrupt business operations → unable to perform routine and necessary tasks (i.e., accessing email, websites, online accounts or other resources) → 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:	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.											
	<table><tr><th>Type</th><th>Description</th></tr><tr><td>Spear Phishing</td><td>phishing attack that targets specific individuals or organizations typically through malicious emails. (Steal sensitive info. i.e as login credentials) or infect malware. (Eg, CEO received email from Fake bank, Looks like original, to enter ID/Pass to update the account)</td></tr><tr><td>Whaling</td><td>Social engineering attack specifically targeting senior or C-level executive employees (Purpose of stealing money or information)</td></tr><tr><td>Smishing</td><td>fraudulent practice of sending text messages purporting to be from reputable companies (Reveal personal info. Like passwords & credit card no.)</td></tr><tr><td>Vishing</td><td>voice phishing, is the fraudulent use of phone calls & voice messages pretending to be from a reputable organization (to reveal private info.)</td></tr></table>	Type	Description	Spear Phishing	phishing attack that targets specific individuals or organizations typically through malicious emails. (Steal sensitive info. i.e as login credentials) or infect malware. (Eg, CEO received email from Fake bank, Looks like original, to enter ID/Pass to update the account)	Whaling	Social engineering attack specifically targeting senior or C-level executive employees (Purpose of stealing money or information)	Smishing	fraudulent practice of sending text messages purporting to be from reputable companies (Reveal personal info. Like passwords & credit card no.)	Vishing	voice phishing, is the fraudulent use of phone calls & voice messages pretending to be from a reputable organization (to reveal private info.)	
Type	Description											
Spear Phishing	phishing attack that targets specific individuals or organizations typically through malicious emails. (Steal sensitive info. i.e as login credentials) or infect malware. (Eg, CEO received email from Fake bank, Looks like original, to enter ID/Pass to update the account)											
Whaling	Social engineering attack specifically targeting senior or C-level executive employees (Purpose of stealing money or information)											
Smishing	fraudulent practice of sending text messages purporting to be from reputable companies (Reveal personal info. Like passwords & credit card no.)											
Vishing	voice phishing, is the fraudulent use of phone calls & voice messages pretending to be from a reputable organization (to reveal private info.)											
Spoofing:	Technique through which a cybercriminal disguises themselves as a known or trusted source. Engage with target & access their systems or devices with the ultimate goal of stealing info. (Installing malware)											
	<table><tr><th>Type</th><th>Description</th></tr><tr><td>Domain Spoofing</td><td>Domain appears to be legitimate at first glance, but a closer look will reveal subtle differences.</td></tr><tr><td>Email Spoofing</td><td>Email spoofing is a type of cyberattack that targets the businesses by using emails with forged sender addresses. they are more likely to open the email and interact with its contents, such as a malicious link or attachment.</td></tr></table>	Type	Description	Domain Spoofing	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. they are more likely to open the email and interact with its contents, such as a malicious link or attachment.					
Type	Description											
Domain Spoofing	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. they are more likely to open the email and interact with its contents, such as a malicious link or attachment.											
Identity-Based Attacks:	When valid user's credentials have been compromised & 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 a/c.											
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 that would help carry out such an attack.											
DNS Tunneling:	DNS Tunneling is a type of cyberattack that leverages domain name system (DNS) i.e., (Website domain) queries and responses to bypass traditional security measures and transmit data & code within the network. This tunnel gives the hacker a route to unleash malware and/or to extract											

(Spoof)	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. If compromised, hacker assume control of device, steal data, or join a group of infected devices

Stages of Cyber Risks:

Stage 1 - Assessing the cyber risk:	<p>Different clients will have different levels of risks, even with the same industry. Every organization should consider at least the common threats:</p> <p><i>[Trick: Inside se sab me 1 common chi h > sab handsome hote h andar se]</i></p> <ul style="list-style-type: none"> • 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 disclosure of information theft and frauds.
Stage 2 - Impact of cyber risk: <i>Trick [RIB RIB Fines & Penalty]</i>	<p>Cyber-attack can impact one, two or more types of risks. The impact of the attack would vary from organization to organization, 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:</p> <p><i>[Trick: "Cost" lagegi > "ransomware" ne attack kara to "Privacy" breach ho jaaegi saara "data" uske paas chale jaage, apka main "IP right" bhi > to "business" hi bank ho jaaega]</i></p> <ul style="list-style-type: none"> • R - Regulatory costs • Fines and penalties • R- Ransomware - more common these days where entire systems are encrypted • B- Breach of Privacy, if personal data of a consumer is hacked it could have a significant impact on the organization. • Data loss, reputational loss and litigation • I- 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 • B- Business interruptions causing an operational challenge for an organization. • I- Incident response cost which could be for investigations & remediations
Stage 3 - Managing the cyber risk	<p>A strategic approach to cyber risk management can help an organization to:</p> <p><i>[Trick: "Understand Risk" > uss risk ke against kya "cysbersecurity h" > "security align karo objective se" end me agar fir bhi koi "Risk bache to usse Document karlo .. against Control"]</i></p> <ul style="list-style-type: none"> • Gain a holistic understanding of the cyber risks, threats facing their organization and other financial institutions • Assess existing IT & cybersecurity program and capabilities against the relevant regulatory requirements • Align cybersecurity & IT transformation initiatives with strategic objectives and critical risks • Understand accepted risks & documented compensating controls

Q7. Sukanya is of view that **cyber risks are issues of IT** and result only in information loss. → **cyber-attacks are not directly targeted at financial systems** and do **not pose risk of MMS to FS**. Is her view proper?

Hint: [Mention above "STAGE 2 - IMPACT OF CYBER RISK"] & Below Additional Answer

May cyber-attacks are not directly targeted at financial systems. However, the access gained by the attackers may provide them the ability to:

(1) **modify financial records** (2) **Modify key automated business rules** (3) **Modify automated controls**

Further, auditor should **consider whether cyber risk (like other business risks) represents a ROMM to the FS as part of the audit risk assessment activities.**

➤ Cyber Security Framework (Risk Management Process): - RR - PDI

Q8. Briefly describe the cyber security Framework. [ICAI SM]

Identify the Risk: <u>ABC-G</u>	Determine whether entity's RAP considers cybersecurity risks. <ul style="list-style-type: none"> • Conduct periodic risk assessment: Entity should Conduct periodic risk assessment & develop a management strategy to identify cyber-risk & loss against it • Asset management: should maintain and periodically reviews an inventory & asset (Intellectual property, patents, copyrighted material) • Governance: Mngt should review how cybersecurity risks affect IC-FR, how mngt will recover financial data & impact on revenue recognition. • Business environment: For cybersecurity establish roles and responsibilities over cybersecurity (CISO, CIO) → Risk asses should also to be discuss with TCWG
Protect the Risk: <u>[DAAI] ko protect krna paani se</u>	Obtained an understanding of the entity's processes for, safeguarding of assets: <ul style="list-style-type: none"> • Access Control: monitors whether there has been unauthorized access to electronic assets and any related impact on financial reporting • Awareness and Training: To make the teams aware of the risk associated with cyberattacks. • Data Security: implement effective controls for data security • Information Protection Processes and Procedures: for identifying material digital/electronic assets on the balance sheet subject to cybersecurity risk & prioritizing their protection based on criticality
Detect the Risk:	controls and procedures that enable it to identify cybersecurity risks and incidents and to assess and analyse their impact on the entity's business → monitor and detect security breaches. Implemented anti-virus or monitor fire-wall logs on continuous basis <ul style="list-style-type: none"> • Anomalies and Events (identify karo timely basis pe) • Security Continuous Monitoring • Detection Processes
Respond the Risk: <u>[RCM]</u>	If material cybersecurity or data breach → mngt should capture details of nature of incident and how the incident or data breach was identified → Entity should have response planning <ul style="list-style-type: none"> • Response Planning (incident response plan) → plan helps in analysing impact & severity of attack, taking the appropriate actions • Communications → same need to communicate to who is responsible for framework & TCWG. • Mitigation & Improvements → Management should assess Litigation costs, investigation costs, Remediation costs, future action plans for safeguard
Recover from Risk: <u>[RIC]over</u>	<ul style="list-style-type: none"> • Recovery Planning → Should have recovery plan action to recover from the attack, once impact evaluated, communicate with regulator. • Improvements → like patch upgrades, better Controls, improved technology in terms of firewall, anti-virus, etc. • Communications → Communicate to regulatory

➤ 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:

Controls around vendor setup & modifications:	Cyber schemes exist in which changes to bank account or other critical vendor information are requested through email phishing scams <u>[Trick: agar "Communication" aaya kisika details update karne k liye .. to "Kon" karega ? kis "system" me karega ? hone k baad "Verify" kon karega ?]</u>
----------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

NOV'24

- (i) **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).
- (ii) **Who is responsible for making changes** to vendor master data? Is the process centralized or decentralized?
- (iii) **What systems and technologies** are used to initiate, authorize and process requests related to changes to vendor master data?
- (iv) Are **authentication protocols defined to verify modifications** to vendor master data (e.g., call back procedures, multi-factor authentication)?

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** → fraudulent **requests appearing to come from financial institutions** requesting disbursement"

[Trick: pai har kisis "system" se har koi transfer nahi karega .. ho "Educated hoga" usse ho ye authority do .. baad me "Authentication review / approval" bhi karo]

Join "CA Hemant Somani" Telegram Channel for Full PDF

- (i) **What systems and technologies are used** to facilitate the request/initiation, authorization and release of 0 wire transfers?
- (ii) 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?
- (iii) Are **authentication protocols** defined to verify wire transfer requests (e.g., call back procedures, dual-authentication procedures)?

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**

[Trick: Antivirus/patch lene k liye kon "bolta/notify" karta h ? "scan" karte ho timely basis pe > koi "manage" karne wala h ki nhi...]

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

➤ Remote Audit/ Virtual Audit:

Meaning:

- When **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 auditee
- **Audit planning** and scoping is crucial in every audit → **scope and schedule**, and ways to **conduct audit**.

➤ Consideration for Remote Audit:

Q9. key considerations should CA address to ensure the effectiveness & security of remote audit? (MTP'24 & SM)
(Auditors must develop tailored strategies to ensure the remote audit meets the requirements)

Feasibility & 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.
- **Execution phases** of a remote audit **involve video/tele conferencing** with auditees. **Documentation for audit evidence** should be transferred through a document **sharing platform**.

Confidentiality, Security and Data Protection	<ul style="list-style-type: none"> To ensure data security and confidentiality, access to document sharing platform should be sufficiently restricted and secured by encrypting the data information, once reviewed and documented by auditor, is removed from the platform Auditors should take into consideration legislation and regulations, which may require additional agreements from both sides Auditors should not take screenshots of auditees as audit evidence (Unless authorized by the audited organization) Use VPN
Risk assessment	<p>The communication from auditor as well as auditees need to be clear and consistent, and this becomes crucial during remote audit.</p> <p>The assessment to be done that 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.</p>

Q10. What are the advantages and disadvantages of remote audit?

Trick: kahi aana jaan nhi padega > cost save bhi hogi & flexibility bhi rahegi ...aaram se evidence aa jaaenge .. Globally audit krenge.. dhandha bhi badhega

Advantages and Disadvantages of remote audit	
Advantages (trick - Evidence of Widen CTC)	Disadvantages (trick - Do Not SCN)
Auditor can get first-hand evidence directly from the IT system as direct access may be provided.	<u>Doctored documents</u> → 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.
Widens the selection of auditors from global network of experts.	<u>Network Issue</u> → Due to network issues, interviews and meetings can be interrupted.
Comfort & flexibility to the audit team as they would be working from home environment,	<u>Sensitive IT Sys may not be allowed</u> → Remote access to sensitive IT systems may not be allowed. Security aspects related to remote access and privacy needs to be assessed
Time required to gather evidence can spread over several weeks, instead of concentrated into a small period that takes personnel from their daily activities	<u>Cultural challenges</u> → 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.
Cost and time effective: No travel time and travel costs involved	<u>No ability to visualize facility</u> → Limited or no ability to visualize facility culture of the organization, and the body language of the auditees. Time zone issues could also affect

➤ Emerging Technologies in Audit

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 → evaluate whether management is properly assessing the impact of emerging technologies on internal control over financial reporting (ICFR).

Data Analytic Techniques:	
Data Analytics:	Generating & preparing meaningful information from raw system data using processes, tools, and techniques is known as Data Analytics
Audit analytics or audit data analytics:	<p>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.</p> <p>Allows auditors to more effectively audit the large amounts of data held and processed in IT systems.</p>

Audit Analytics Helps:	<ul style="list-style-type: none"> To discover and analyze patterns Extract other useful information in data Identifying anomalies
CAAT:	<ul style="list-style-type: none"> Data analytics methods used in an audit are known as Computer Assisted Auditing Techniques Involves use of multiple data analytical tool or visualization tools → can help the auditor to deep dive into the problem statement and hence increase the audit quality Use various applications & tools that help them to analyse large data sets and obtain insights
Some of the popular tools used across the industry as part of CAATs are listed below: <i>[Trick: AA-BC]</i>	
ACL:	Audit Command Language → 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. Eg. Reconcile TRIAL BALANCE with GENERAL LEDGER to verify COMPLETENESS, it's beyond MS Excel skill to handle such a large data.
Alteryx:	It's 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. [i.e., For Hotel: No of room given on rent * Room Rate = Revenue]
Power BI:	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. [i.e., it's advance version of MS excel, used for Graphs & various reporting's]
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. [i.e., Like SAP & Advance version of Tally with many features]

Q11. discuss the **meaning of data analytics** and **example** of such data analytics techniques.

Hint: Refer above meaning of "Data analytics" & "Examples" i.e., ACL, alteryx, Power BI etc....

Q12. 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?**

Answer:

[Trick: Payment check karte wqt "Payment" ka RECORD & CALCULATION dekhi hoti h "record" > "Complete" & "consistent" nahi h ... "calculation" me "Error" & "exception" hai.... > payment "authorisation" se jyada ho gya]

- Duplicate payments:** Establish relationship between two or more tables as required. For example, duplicate payment for same invoice
- Existence of records:** Identify fields, **which have null values**. Eg, invoices which do not have vendor name
- Data completeness:** Identify whether **all fields have valid data**. Eg, null values in any key field such as date, invoice number or value or name.

- (iv) **Data consistency:** Identify data, which are not consistent with the regular format. Eg, invoices which are not in the required sequence
- (v) **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
- (vi) **Identify exceptions:** Identify exceptional transactions based on set criteria. Eg, cash transactions above Rs. 10,000
- (vii) **Identify errors:** Identify data, which is inconsistent or erroneous. For e.g.: A/c number which is not numeric
- (viii) **Accounts exceeding authorized limit:** Identify data beyond specified limit. For Eg, transactions entered by user beyond their authorized limit or payment to vendor beyond amount due or overdraft allowed beyond limit.

➤ AUTOMATED TOOLS IN AUDIT

Enterprises are adopting emerging technologies → Automation and use of technology often requiring auditors to understand and perform procedures on a larger group of systems that produce information relevant to FS audit's scope may need to include peripheral systems, as well as testing general IT and application controls relative to those systems relevant to F.R (It's based on mngt & auditor Risk assessment)

➤ Internet of Things (IOT)

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. (Change Business model, affect business objective, risk may arise due to new L&R)

Audit Implication	Common risks
<p><i>(Trick: Manual control nii chalega.. new system chahiye hoga.. auditor ko bhi apni skill badhaani padegi.. kyuki new risk hogi)</i></p> <ul style="list-style-type: none"> 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. impact the flow of transactions and introduce new risks for management. payment processing tools that allow users to pay via credit card at a retail location through a mobile device → create a new path for incoming payments that may rely, in part, on a new service provider supplying and routing information correctly (i.e., RazorPay). Auditors would need to consider the volume of those transactions and the processes and controls related to it. 	<p>including, device hijacking, data siphoning, denial of service attacks, data breaches and device theft.</p>

Q13. Describe key components & benefits of IoT, risks associated with IoT implementation, and the implications for the company's audit processes. How should company address these concerns? (RTP'24 & SM)

Hint: Refer Above concept IOT Meaning, Audit Implication, Common Risk, And BELOW KEY COMPONENTS:

- **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 organisation. The risk profile of the entity changes with exposure to new laws and regulations.
- **Example**
 - Connected Cars, connected manufacturing equipment's, smart home security, users can view video feeds when they are away from home
 - Data from machines can be used to predict whether equipment will break down → warning to prevent long stretches of downtime
 - Refrigerator placing an order with a grocery store whenever the supply of eggs falls below a certain number

- Researchers use IoT devices to gather data about customer preferences and behavior.

➤ AI (Artificial intelligence)

System or a machine that can think and learn. AI systems utilize data analysis and algorithms to make decisions based on predictive methods (Self driving cars, Smart robots, Siri, Google assistant etc.)

Audit Implication	Common risks
<ul style="list-style-type: none">• Algorithm:<ul style="list-style-type: none">✓ Logical Flow Process: Given the invisible nature of algorithms, audits must focus on the logical flow of processes✓ whether unintended bias has been added to the algorithms✓ assess the effectiveness of algorithms and whether their output is appropriately review & approved• Consider cybersecurity and search for possible bugs and vulnerabilities• confirm their understanding of how the use of AI affects the entity's flows of transactions, generation of report• AI Decision: whether the AI is making decisions or being utilized by management• Oversight by AI: If management shifts its focus on oversight by relying on AI, auditors should understand what shift occurred, how new risks might be addressed & changes in the audit approach	<p>Data privacy - The data used and shared should have the necessary explicit consent from data providers</p> <p>Security: more data the system uses, from more sources, the more entry points and connections are formed</p> <p>Inappropriate configuration: AI may also be used to diagnose medical conditions. If it is badly configured or malfunctions, it could harm people</p>

Q14. What are common risks for Blockchain technology? Also discuss probable audit implications for this. (SM)

Answer:

➤ BLOCKCHAIN:

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. [i.e., Bitcoin, cryptocurrency transactions] security premise rests on **cryptography**

Audit Implication	Common risks
<p>(Trick: gold ki chain ko Secure & private rakho.. bahar pahen k mat gummo .. tumhe weak samaj ke le jaaenge ... L&R/police bhi kuch nii karegi)</p> <ul style="list-style-type: none">• Governance and security transactions: Auditors should consider the appropriate security & governance around the transaction• Confidentiality & Privacy: 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 Block chain development protocols : something auditors cannot overlook• Data privacy L&R : Data are communicated across geographic boundaries, Data put on blockchain will expose the enterprise to liability for noncompliance with applicable laws and regulations.	<ul style="list-style-type: none">• The strengths of blockchain can <u>also be its weaknesses</u> Inability to reverse transactions & access data without the required keys (System is secure) → but also need specific protocols to ensure that they are not locked out and have clear contingency plans• Cyber-attacks and data hacks: (Security issue)• Compliance with Regulation: Auditors should also ensure complies with regulations → regulatory landscape is still evolving for blockchain → ensure that compliance managers are following developments constantly and adapting processes accordingly

➤ NFT (Non-Fungible Token):

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. → NFT 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	Challenges of NFT
<ul style="list-style-type: none"> • 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. 	<p>NFTs has its own challenges like ownership and copyright concerns, security risks, market is not that wide, online frauds etc.</p> <p><u>NFT audit considerations</u> include comprehensive code review for verifying the safety of a token, valid contract, data privacy and potential cyber threat.</p>

➤ Robotic Process Automation (RPA):

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 (software bots can interact with any application → the same way people do) → nonstop, much faster and with 100% reliability and precision

Audit Implication	Common risks
<ul style="list-style-type: none"> • Understand RPA processes, which include data extraction, aggregation, sanitization and cleansing • 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. 	<ul style="list-style-type: none"> • Operational and execution risks: Robots are deployed without proper operating model. Buying the wrong tool, making wrong assumptions, taking shortcuts, and jeopardizing security • 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

RPA to check IND AS, IFC-FR 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 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

[Refer "Additional PDF Booklet" For Example]

Q15. A company is planning to use Robotics process automation (RPA) to streamline its hiring process. To reduce recruitment costs, efficient hire yield etc. 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?

Answer:

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.

Q16. Enterprises are adopting 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. [SM]

Hint: Refer above any 3

➤ CONTROL CONSIDERATIONS OR OBJECTIVES OF AUDITING DIGITALLY

Q17. Give some examples of technology risks of digital system & control considerations while assessing risk.

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

While assessing Risk, Auditor shall consider control:

[Trick: "New technology" ki wjh se jo "change" ho aya > ab apan ko bhi "skill" badhani hogi]

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) **Risk From New Technology:** 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. E.g., cybersecurity control experts, IT specialists in the team etc.

Examples of technology risks

[unauthorise > data > system > changes > IT personnel doing manual intervention]

[Approx Same as "RISK ARISING FROM USE OF IT", Already Discussed Above]

- 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 arise when multiple users access a common database)
- Unauthorized or erroneous changes to data in master files
- Potential loss of data or inability to access data as required
- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both
- Unauthorized changes to systems or programs
- Failure to make necessary or appropriate changes to systems or programs

	<ul style="list-style-type: none"> • Possibility of info. technology personnel gaining access privileges beyond those necessary to perform their assigned duties, thereby leading to insufficient segregation of duties • Inappropriate manual intervention • Risks introduced when using third-party service providers • Cybersecurity risks
Key Steps for Auditors in a Changing Technology Environment: <i>(Special Trick by CA Hemnt Somani :-)</i>	<p>As auditors obtain an understanding of the impact of technology on a company's business, its systems of I.C., and its financial reporting, some important reminders include the following:</p> <p><i>[Trick: New Technology lagaai mngt ne .. to Control bhi lagao ... > kya effect hoga uska ? > transaction process pe effect padega ?]</i></p> <ol style="list-style-type: none"> Maintain sufficient professional skepticism when reviewing Mngt risk assessment for new systems. 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. Understand the direct and indirect effects of new technology and determine how its use by the entity impacts the auditor's overall risk assessment Understand how the technologies impact the flow of transactions, assess completeness of the in-scope ICFR systems, and design a sufficient and appropriate audit response.

➤ 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:

SDM MR. Manual

Sampling population → to Full Population analysis

Disconnected tools → to integrated ecosystem service

Manual work → Automation

Multiple data set → to One data set

Repetitive task → high value work & capacity for grow

Manual risk assessment to → Dynamic, data driven risk assessment

Q18. Give example of emerging technologies available for Next Generation Audit along with the risks associated with it [SM]

[TRICK: AR-VR - Drone Metaver]

Auditing Through:	
Drone Technology:	Also known as (Unmanned Aerial Vehicle) UAV : Using drone technology in the remote locations for stock counts → sensors and cameras, thus they can photograph and physically examine the count of large quantities Drone captured audit information can be combined with various alternative sources of information such as QR code readers, handheld bar scanners, manual counts etc
Augmented reality (AR):	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 → catch imaginary Pokémon around physical locations
Virtual reality:	Replaces the real world entirely with a simulated environment , created through digitally

generated images, sounds, and even touch and smell

Example of AR & VR:

- **In architecture and engineering businesses** → AR-VR → allow architects to see their building plans come to life before being built
- **Business sector** → allow products to be previewed / customized, thus improving productivity
- **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

Metaverse:

Emerging 3-D digital space that uses virtual reality (VR), augmented reality (AR), 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 & extend the reach & use of Cryptocurrency, Artificial Intelligence (AI), Augmented Reality (AR) & Virtual Reality (VR) mature landscape of virtual spaces with transferable identities and assets enabled by blockchains (NFTs) that are interoperable or interchangeable

Some considerations for future:

- **Digital monetary systems:** 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:** Governance models will become ever more difficult to balance openness and user contribution with strategic direction and innovation
- **KYC:** 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)
- **Synchronize realtime:** 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.

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

➤ 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.
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
Virtual Financial Education & Training	Aims to enhance financial literacy using the metaverse. They create a virtual classroom environment where participants can attend interactive financial education sessions (learn about budgeting and financial planning etc)

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
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

Join "CA Hemant
Somani" Telegram
Channel for Full PDF

For Full PDF & Other Notes: Join →



For Free
Notes

<http://t.me/cahemantsomani>

CA Hemant Somani