MagnetCA
CA in you

AARTI LAHOTI AUDIT LEARNING

CA FINAL

NEW SCHEME – GROUP - I

ADVANCED AUDITING, ASSURANCE AND PROFESSIONAL ETHICS

MODULE - II

Chapters 12 to 19

3rd Edition

Author

CA Aarti N. Lahoti

By India's Most Dynamic Faculty For Audit

www.aartilahoti.com

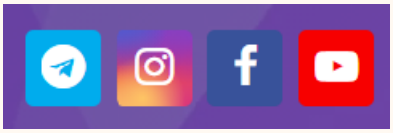
MODES OF LEARNING : Pendrive / Google Drive / Virtual / Face to Face / Livestream

Price : Rs. 1495

Every effort has been made to avoid errors or omissions in this publication. In spite of this, errors may creep in. Any mistake, error or discrepancy noted may be brought to our notice which shall be taken care off in the next edition. It is notified that neither the Author nor the Seller will be responsible for any damage or loss of action to any one, of any kind, in any manner, therefrom. It is suggested that to avoid any doubt the reader should cross-check all the facts, law & contents of the publication with the Institute's publication or notifications.

CA Aarti N. Lahoti

Connect to CA Aarti N. Lahoti on **www.aartilahoti.com**, Telegram, Instagram, Facebook & Subscribe to the YouTube Channel – Aarti Lahoti



Preface to the Second Edition

Dear Students,

IT'S ALL ABOUT AUDIT!

It gives me immense pleasure to present before you the 3rd Edition of Advanced Auditing, Assurance & Professional Ethics – Module I & II - for CA Final.

I have made an humble attempt to include all theory, Q & A & Amendments released by ICAI through its different mediums viz. Latest Study Material, Suggested Answers, Mock Test Papers & Revision Test Papers in this book.

Any constructive criticism is always welcome. @ aartinlahoti9@gmail.com

The greatest strength of this book is its wholistic approach towards the subject - a one stop solution for the entire subject of CA Final Auditing. It covers each & every topic of the syllabus in a tabular & pointwise format & also the myriad varieties of questions in relation to the same.

Having CONCEPTUAL CLARITY about the topics is half the battle won!!! To complete it you need to do a lot of WRITING PRACTICE. As a general problem faced by students is that though they understand the concepts but they are not able to put it in words & this happens merely due to lack of writing practice. So never forget that!

And one final piece of advice would be to do CUMULATIVE REVISIONS of the subject so that you are able to retain the subject better.

Wishing you all the very best for your exams and for a brightful future!

Happy Auditing!

Regards,

CA Aarti N. Lahoti
www.aartilahoti.com
www.magnetca.com

CA Aarti Lahoti Classes

Chapter 12

DIGITAL AUDITING & ASSURANCE

1 DIGITAL AUDIT

1. What is a Digital Audit?

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

2 Key Features of a Digital Audit

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

3 Advantages of Digital Audit

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

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

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

(iv) Better Analytics: Improved analytics capabilities can aid management & auditors in seeing trends & 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.

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

4 Consideration & Challenges of Digital Audit

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

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

Areas of focus could include understanding of the following:

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

2 AUDITING DIGITALLY

1 What is the concept of Auditing Digitally?

- Auditing Digitally is using advancements in technology for conducting an effective & efficient audit. With a rapidly growing IT environment it is essential to adapt technology in auditing practices.

Example:

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

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

2 Expectations from an Auditor

- Audit teams need to involve the experts on different software applications & technologies. Having the right level of expertise of new technology (such as RPA, AI, blockchain technology allows auditors to provide the highest quality of audit.
- Investment in digitally upskilling people is the real secret to quality technology audit.
- Investment in technology across the profession has largely been focused on developing & using tools to automate & enhance existing processes, such as data analytics & collaboration & sharing tools, which help to drive quality in audits today.
- While this will remain core to the role of technology in the audit, there are many opportunities where more advanced technologies such as AI & drones could have an even bigger impact.
- Such technologies may also play a role in evolving the scope of the audit (e.g., in using data analytics & machine learning to help identify fraud).
- Due to the usage of BOT manual intervention has been reduced, more accurate results are populated, it results in saving auditors time as well & exceptions highlighted can be readily reviewed.

3 Key Features or Advantages of Auditing Digitally

(i) Improved Quality of Audits: The impact on quality is evident, through automation, data analytics techniques we can easily move from sample auditing to full population of transactions being reviewed or re-performed. This ultimately free up time for audit

teams to analyses the information & better understand the business they audit.

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

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

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

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

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

4 Considerations in Auditing Digitally

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

(i) What Problems are you trying to solve?

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

(ii) Which Technology can help you?

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

(iii) 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 & development are critical to ensure teams understand how & why they are using the technology. Reluctance to change is obvious, however continuous training help them to get better.

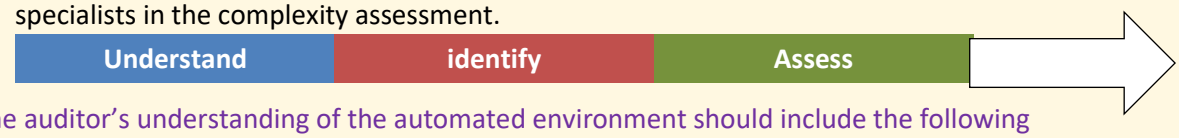
(iv) Range of Automated Solutions

- There is a range of automation solutions, from low to high sophistication, which helps to standardize the repeatable tasks & optimize the efforts resulting in doing better. Some of the techinques are using robotics & automation for data gathering activities, use of data analytics for planning & budgeting & reporting by dashboards

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

3 UNDERSTAND THE IT ENVIRONMENT

- Understanding the ways in which the entity relies upon IT & 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 &/or execution of the audit, including initial consideration of whether to include specialists in the complexity assessment.



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

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

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

Key Areas for an Auditor to Understand IT Environment

1. Understand the flow of transaction:

- The auditor's may focus on identifying & understanding the nature & number of the specific IT applications & other aspects that are relevant to the flow of transactions & processing of information.
- Changes in the flow of transactions may result from program changes to IT applications, or direct changes to data in databases involved in processing or storing those transactions or information.

2. Identification of Significant Systems:

- The auditor may identify the IT applications & supporting IT infrastructure concurrently with the auditor's understanding of how information flows into, through & out the entity's information system.

3. Identification of Manual & Automated Controls:

- An entity's mix of manual & automated elements varies with the nature & complexity of the entity's use of IT. The characteristics of manual or automated elements are relevant to the auditor's identification & assessment of the risks of material misstatement.

4. Identification of the technologies used:

- The need to understand the emerging technologies implemented & the role they play in the entity's information processing or other financial reporting activities & consider whether there are risks arising from their use.
- The engagement team may decide to engage specialists &/or auditor's experts to help understand whether & how their use impacts the entity's financial reporting processes & may give rise to risks from the use of IT.

Some examples of emerging technologies are:

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

5. Assessing the complexity of the IT environment:

- Not all applications of the IT environment have the same level of complexity.
- 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 & implementation of emerging technologies.

4 IDENTIFYING THE RISKS ARISING FROM THE USE OF IT

1 How to identify the IT Risks?

- In identifying the risks arising from the use of IT, the auditor may consider the nature of the identified IT application.
- Applicable risks arising from the use of IT may also be identified related to cybersecurity.
- It is more likely that there will be more risks arising from the use of IT when the volume or complexity of automated application controls is higher, & management is placing greater reliance on those controls.

2 Risks arising from use of IT

- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database.
- The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties. Unauthorized changes to data in master files.
- Unauthorized changes to IT applications or other aspects of the IT environment.
- Failure to make necessary update IT applications or other aspects of the IT environment.
- Inappropriate manual intervention.
- Data loss or data corruption is a major risk which arises from use of IT. If appropriate cybersecurity controls & protocols not followed it may lead to loss of sensitive data, hackers might encrypt your system or illegally break into your system. Risk of fraud can arise if users alter the information or there is a case of physical security breach or theft of sensitive information.
- There is a risk of system downtime which is caused by hardware failures, faulty configurations, cyberattacks or power outage. It means the IT systems will not be operational or will be unavailable/offline which may hamper the business.

- Since companies uses more than one IT systems to support their business system integration (means integrating one or more systems) & system compatibility comes in place. However, system integration & compatibility have some risks. In case of system failure in one system may also lead to widespread failure in integrated systems or if the integration between two systems is not appropriate the end result would be incorrect. System compatibility means sharing compatible hardware, software & operating system while performing the integration. Compatibility risks arises if different versions of same software are used, if the patches are not upgraded which may lead to bugs.
- With advancement in usage of IT the risk of regulatory compliances increases. Any change in the law, order, guidelines or agreements will impact the business, its related costs, investments etc. A FMCG sector will be subject to different regulatory requirements than a financial company, however both businesses will need to manage their respective compliance risks.
- Performance Issues arises with the way requests are processed in the IT systems. Heavy data load, network usage impacts the application performance & its responsiveness. To overcome the performance issues of IT systems, resources or hardware can be added to an existing nodes, which is known as scaling. However, scaling can be expensive therefore an informed decision should be made in case of adding a hardware or changing the architecture.

3 Know how to identify the IT Dependencies impacting the audit

1. Why is it important to identify IT dependencies?

- Identifying & 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 & enables us to develop an effective & efficient audit approach.

2. How IT dependencies arise?

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

There are five types of IT dependencies as described below:

Type	Description
Automated Controls	➡ Automated controls are designed into the IT environment to enforce business rules. ➡ For 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), &/or reasonableness checks (e.g., maximum payment amount) when a transaction is entered.
Reports	➡ System generated reports are information generated by IT systems. These reports are often used in an entity's execution of a manual control, including business performance reviews.
Calculations	➡ Calculations are accounting procedures that are performed by an IT system instead of a person. ➡ For eg., the system will apply the 'straight-line' depreciation formula to calculate depreciation of an asset or the system will calculate the value of the amount invoiced to a customer by multiplying the item price times the quantity shipped.
Security	➡ Security including segregation of duties is enabled by the IT environment to restrict access to information & to determine the separation of roles & responsibilities that could allow an employee to perpetrate & conceal errors or fraud, or to process errors that go undetected.

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

3. Understanding & responding to risks arising from IT dependencies

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

Access Security

Objective -	Activities -
To ensure that access to programs & data is authenticated & authorized to meet financial reporting objectives	➡ Access requests to the application are properly reviewed & authorized by management ➡ Access of terminated user is removed on a timely basis ➡ Access rights to applications are periodically monitored for appropriateness ➡ Transactions of administrative & sensitive generic IDs are monitored ➡ Security policies are procedures are maintained ➡ Access to operating system & database is restricted.

Program Change

Objective -	Activities -
To ensure modified systems continue to meet financial reporting objectives	➡ Change Management policy & procedures are maintained. ➡ Development, testing & production environments are segregated for changes to application configurations ➡ Changes are adequately tracked & recorded. ➡ Changes to application configurations are adequately tested & approved before being migrated into production ➡ Emergency changes are approved. ➡ Segregation of duties is maintained between developer & implementor.

Data Centre & network operations

Objective -	Activities -
To ensure production systems are appropriately backed up to meet financial reporting objectives	➡ Policies & procedures for data back & recovery is maintained. ➡ Data is appropriately backed up & recoverable ➡ Restoration testing is performed ➡ Monitoring & compliance of service level agreements. ➡ Batch job scheduled are monitored for failures & access is restricted.

5 ASSESSING CYBER RISKS (INCLUDING REMOTE AUDIT)

What is Cyber Risk?

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

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

Most Common Types Of Cyberattacks Are:

Malware

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

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

Denial-of-Service (DOS) Attacks

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

Phishing

- Phishing is a type of cyberattack that uses email, SMS, phone, social media, & social engineering techniques to entice a victim to share sensitive information — such as passwords or account numbers — or to download a malicious file that will install viruses on their computer or phone.

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

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

Spoofing

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

Type	Description
Domain Spoofing	Domain spoofing is a form of phishing where an attacker impersonates a known business or person with fake website or email domain to fool people into the trusting them. The domain appears to be legitimate at first glance, but a closer look will reveal subtle differences.
Email Spoofing	Email spoofing is a type of cyberattack that targets the businesses by using emails with forged sender addresses. Because the recipient trusts the alleged sender, they are more likely to open the email & interact with its contents, such as a malicious link or attachment.

Identity-Based Attacks

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

Insider Threats

➡ When current or former employees that pose danger to an organization because they have direct access to the company network, sensitive data, & intellectual property (IP), as well as knowledge of business processes, company policies or other information that would help carry out such an attack.

DNS Tunneling

➡ DNS Tunneling is a type of cyberattack that leverages domain name system (DNS) queries & responses to bypass traditional security measures & transmit data & code within the network. This tunnel gives the hacker a route to unleash malware &/or to extract data, IP or other sensitive information by encoding it bit by bit in a series of DNS responses.

IOT-Based Attacks

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

1 Stages of Cyber Risks:

Following are 3 Stage of cyber risk:

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

➡ Ransomware disabling their organization

➡ Common criminals using email phishing & hacks for fraud & theft.

➡ Insiders committing malicious activities or accidental activities resulting in unintended discourse of information theft & frauds.

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

➡ Regulatory costs

➡ Business interruptions causing an operational challenge for an organization.

➡ Data loss, reputational loss & litigation.

➡ Ransomware - more common these days where entire systems are encrypted Intellectual

	property theft which may not only take the competitive advantage, but we may also result in any impairment/impediment charge because of the loss of IP. ➡ Incident response cost which could be for investigations & remediations Breach of Privacy, if personal data of a consumer is hacked it could have a significant impact on the organization. ➡ Fines & penalties **Stage 3 - Managing the cyber risk:** A strategic approach to cyber risk management can help an organization to: ➡ Gain a holistic understanding of the cyber risks, threats facing their organization & other financial institutions ➡ Assess existing IT & cybersecurity program & capabilities against the relevant regulatory requirements ➡ Align cybersecurity & IT transformation initiatives with strategic objectives & critical risks ➡ Understand accepted risks & documented compensating controls
2 **Cyber Security Framework**	➡ Cybersecurity framework includes how management is identifying the risk, protecting & safeguarding its assets (including electronic assets) from the risk. Management preparedness to detect the attacks, anomalies & responsiveness to the adverse event.
1 **Identify the Risk**	➡ Auditor has to determine whether the entity's risk assessment process considers cybersecurity risks. ➡ Entity should conduct a periodic risk assessment & develop a management strategy which identifies cybersecurity risks. ➡ The entity should maintain & periodically reviews an inventory of their information assets- i.e., Asset Management (e.g., intellectual property, patents, copyrighted material, trade secrets & other intangibles). ➡ The entity should classify & prioritize protection of their information assets based on sensitivity & business value & periodically reviews the systems connected to the network on which digital assets reside. ➡ Review how cybersecurity risks affect internal controls over financial reporting. In case of adverse attack how management is going to assess the impact on the recoverability of financial data & impact on revenue recognition. ➡ Management needs to identify if any established a risk-based cybersecurity program can be leveraged e.g. (NIST, ISO etc.) ➡ To determine overall responsibility for cybersecurity in the business environment entity should establish roles & responsibilities over cybersecurity (CISO, CIO). Further the risk assessment should be discussed with TCWG.
2 **Protect the Risk**	➡ Obtained an understanding of the entity's processes for safeguarding of assets subject to cybersecurity. Entity monitors whether there has been unauthorized access to electronic assets & any related impact on financial reporting. ➡ Formal training should be conducted to make the teams aware of the risk associated with cyberattacks. ➡ Entity should implement effective controls for data security. Entity should have a process & procedures in place for identifying material digital/electronic assets on the balance sheet subject to cybersecurity risk & prioritizing their protection based on criticality.
3 **Detect the Risk**	➡ Entity should have controls & procedures that enable it to identify cybersecurity risks & incidents & to assess & analyse their impact on the entity's business. ➡ Review entity's processes to monitor & detect security breaches or incidents. If management has implemented anti-virus in the system to secure it from anomalies or if

	firewall logs are being continuously monitored to detect any repetitive attacks. ➡ A monitoring process should be established to review how many such events have been denied by the firewall. Monitoring process should also include if any upgrades or updates are required to safeguard the systems from vulnerabilities.
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 & how the incident or data breach was identified. Entity should have a response planning in place to capture the details of nature of incident & the same needs to be communicated to TCWG. ➡ The security incident response plan helps in analysing the impact & severity of the attack & helps the organisation in taking the appropriate actions. Management should assess Litigation costs, Regulatory investigation costs & Remediation costs as a part of mitigation process & improvement management should assess the future action plans that needs to be taken to safeguard the organisation from such attacks.
5 Recover from risk	➡ Entity should undertake appropriate actions to recover from the attack & make sure the business is up & running. ➡ Once the impact evaluated & communicated with the regulators the recovery plan needs to be implemented to overcome the impact. Necessary improvements - like patch upgrades, better controls, improved technology in terms of firewall, anti-virus, tools etc. needs to be implemented to safeguard the entity.
Case Study	*What has happened:* The CEO of a hotel realized their business had become the victim of wire fraud when the accounts payable executive began to receive insufficient fund notifications for regularly recurring bills. A review of the accounting records exposed a serious problem. Upon investigating it was noted that the CEO had clicked on a link in an email that he thought was from the trusted source. However, it wasn't & when he clicked the link & entered his credentials, the cyber criminals captured the CEO's login information, giving them full access to intimate business & personal details. *Type of Attack:* Social engineering, phishing attack. A phishing attack is a form of social engineering by which cyber criminals attempt to trick individuals by creating & sending fake emails that appear to be from an authentic source, such as a business or colleague. The email might ask you to confirm personal account information such as a password or prompt you to open a malicious attachment that infects your computer with malware. *Result:* The hotel's cash reserves were depleted. The fraudulent transfers amounted to more than million. The hotel also contacted a cybersecurity firm to help them mitigate the risk of a repeat attack. *Impact:* The business lost ₹ 1 million, & the funds were not recovered. Further there was loss of business reputation too. *Lessons Learned:* ➡ Train the staff about the dangers of clicking on unsolicited email links & attachments, & the need to stay alert for warning signs of fraudulent emails. Engage in regular email security training. ➡ Implement stringent wire transfer protocols & include a secondary form of validation (Multi Factor Authentication) ➡ Have a cyber incident response plan ready to implement.
1 Control considerations for Cyber Risks	1. Controls around vendor setup & modifications: ➡ Certain cyber schemes exist in which changes to bank account or other critical vendor information are requested through email phishing scams by individuals purporting to be authorized vendor personnel.