CA FINAL - ADVANCED

AUDITING

ASSURANCE AND PROFESSIONAL ETHICS

NEW COURSE

Brahmastra

Notebook style multicoloured book penned by CA SJ

ADDITIONAL CHAPTER NOTES

- DIGITAL AUDITING AND ASSURANCE
- SUSTAINABLE DEVELOPMENT GOALS (SDG) & ENVIRONMENT, SOCIAL AND GOVERNANCE (ESG) ASSURANCE

F.A.S.T
first attempt success tutorials

F.A.S.T
first attempt success tutorials

JOIN FR & AUDIT

with CA. Sarthak Niraj Jain

Financial Reporting

- **FR-Regular** (Cover FR in 275 hours)
- **FR-Faster** (Cover FR in 140 hours)
- **FR-Power** (Revise Full FR in 75 hours)

Audit

- **Audit-Regular** (Cover Audit in 145 hours)
- **Audit-Faster** (Cover Audit in 75 hours)
- **Audit-Power** (Revise Full Audit in 50 hours)

CA. Sarthak Jain

NOW JOIN
FR & AUDIT
Live @
HOME
By
CA. Sarthak Niraj Jain

Join us for
FR & AUDIT

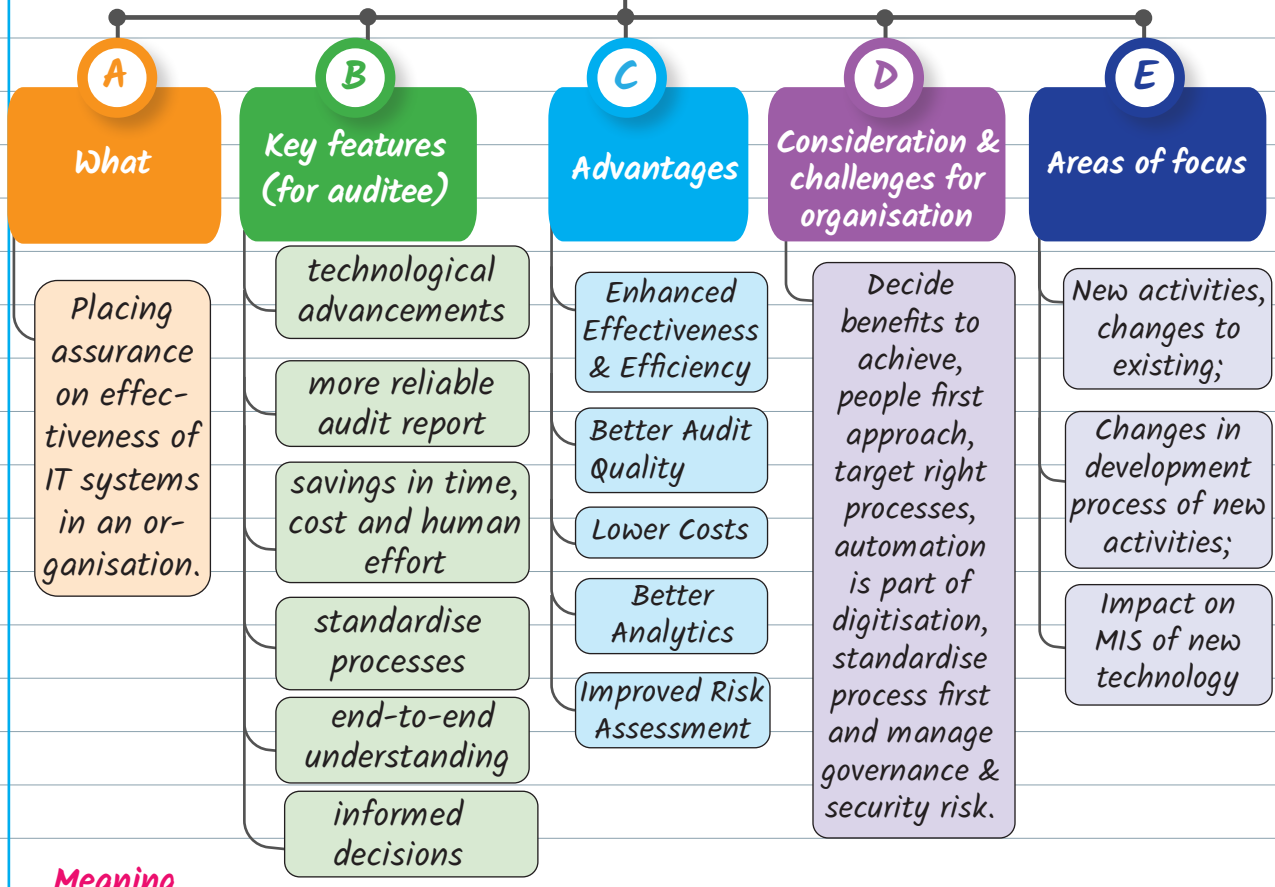
LECTURE | BOOKS
TEST SERIES | MENTORING

(Instead of live at home, virtual centre, video lecture and books.....)

95225 64050 /esarthak /casarthakjain /FAST Education /casarthakjain /SarthakJainCA

Chapter-12 DIGITAL AUDITING AND ASSURANCE

1 DIGITAL AUDIT (Digitisation for clients)



(1) Meaning

- Digital Audit is **placing assurance on the effectiveness of the IT systems** implemented in an organisation.
- Technology is an integral part of regular business operations. Organisations should review their technology-related controls to identify gaps and risks for continuous improvement and to ensure regulatory compliance.
- A strong controls and security position gains trust of stakeholders.

(2) Key Features (for auditee)

- Encourages the auditee to embrace the latest technological advancements.
- Improves the quality of opinion, more reliable audit report.
- Leads to savings in time, cost and human effort. Many of today's digitally enabled processes operate autonomously 24x7, driving real-time transactions.
- Allow to standardise processes and allow controls to be implemented to mitigate risk.

- Help organisation gain a more comprehensive overview of end-to-end processes and how technologies are utilized, controlled and optimized against standards set.
- Help to create a future for a digital strategy and paves way for adopting new technologies such as AI and Robotic, usage of analytics and automation.
- Help the auditee to make informed decisions.

(3) Advantages

- **Enhanced Effectiveness & Efficiency:** With the use of tools and automation techniques, auditee can standardise the processes and routine tasks like automating a reconciliation process that previously involved hours, and thus increases the efficiency and saves time and costs.

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

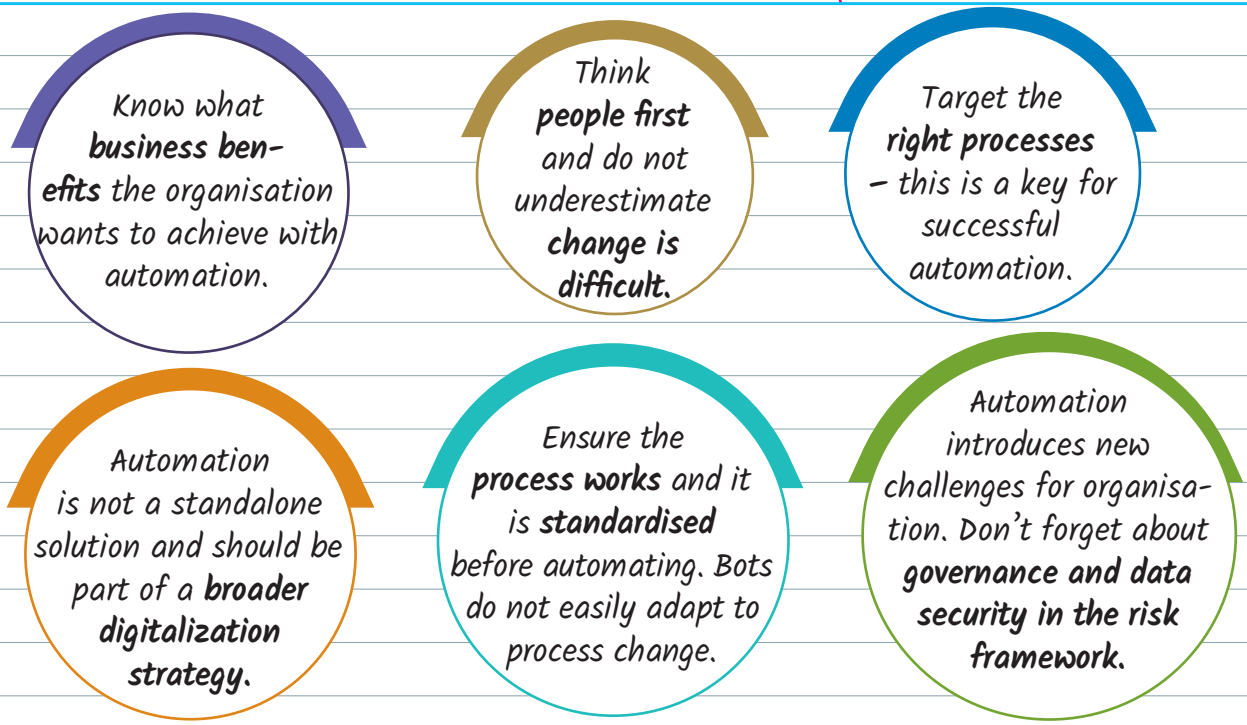
- **Lower Costs:** By automating processes the cost of auditing and the time needed to complete an audit, is reduced.

- **Better Analytics:** Aid management and auditors in seeing trends and patterns that may be challenging to spot manually. For instance, AI can examine a lot of financial data to spot possible fraud, which is hard for auditors to spot manually.

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

(4) Consideration and Challenges

I. Considerations that organisation should keep in mind while using digital techniques & automation:



2. **Auditors will obtain an understanding of management's implementation and oversight of new technologies, and perform procedures:** To understand the changes to the company's business, including any changes to the information technology environment.

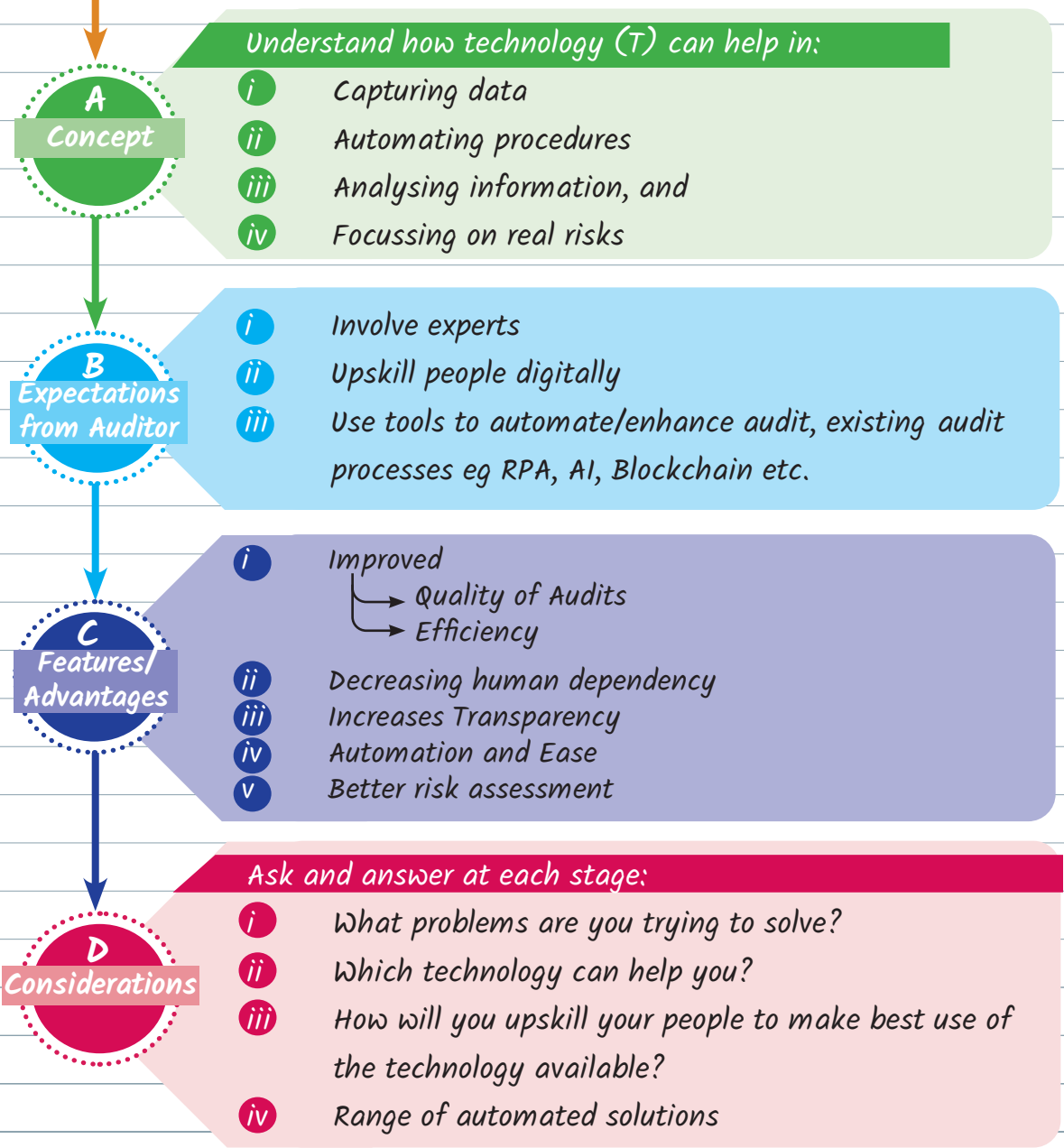
Areas of focus include understanding of the following:

- New activities or changes to existing processes **due to new technology** (e.g., new revenue streams, changes in the roles and responsibilities of entity personnel, automation of manual tasks, changes in staffing levels that affect an entity's IC environment).

- Changes in the way the entity's systems are developed and maintained and whether these changes introduce new risks and require new controls to respond to those risks.

- Impact of new technology on how to obtain or generates use relevant information on the functioning of internal control.

2 AUDITING DIGITALLY (for auditor)



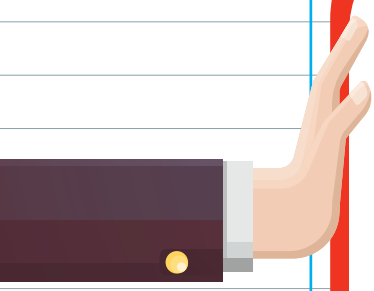
(I) Concept

- Auditing Digitally is using advancements in technology for effective and efficient audit.

  For 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 involves digitizing the way an audit is delivered through automation and innovation.
- There are new technologies to help **capture data**, **automate procedures**, **analyse information** and **focus on the real risks** of the client.

Expectations from an Auditor

- ✔ Audit teams need to involve experts on different applications and technologies.
- ✔ A right level of expertise of new technology, such as RPA, AI, blockchain technology, allows auditors to provide highest quality of audit.
- ✔ Investment in technology helps to focus on developing and using tools to automate and enhance existing processes, such as data analytics and collaboration and sharing tools, which help to drive quality in audits today.
- ✔ Advanced technologies such as AI and drones may also play a role in evolving the scope of the audit (e.g., using data analytics and machine learning to help identify fraud).



Example

A manager on a weekly basis performs a manual control to review if vendor master additions and changes in the system are done post appropriate approvals. This control can be tested and re-performed by the auditor using RPA technology

BOTs can login into the system and generate the report and write the output in an excel file.

Based on population, BOT will select the samples of changes to be tested.

Further, BOT will pull the correct file with approved changes from SharePoint.

Then it will perform the testing wherein it will populate the details of approvals (date, approved by) and identify if changes made without approvals.

Lastly, BOT will summarise the results for all the selected samples in an excel file.

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

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

(2) Key Features or Advantages

Improved

- ✔ **Quality of Audits:** The impact on quality is evident, through automation, for e.g. by using 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 analyse the information and better understand the business they audit.

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

- **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 judgment of different individuals.

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

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

- **Better risk assessment:** With usage of automation and technology in audit, auditor may **focus on the real challenges and assess the potential risk** precisely. It gives time to auditors to focus on the bigger picture rather than being involved with repetitive tasks. Dashboards, visual presentations and other tools help in understanding where the risk lies and what all areas need more attention.

(3) Considerations

Some of the crucial questions to ask and answer- at all stages of tech journey:

- **What problems are you trying to solve?**

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

- **Which technology can help you?**

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

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

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

Range of automated solutions:

There is a range of automation solutions, which helps to **standardize the repeatable tasks and optimise the efforts** resulting in doing better. Some of the techniques are using robotics and automation for data gathering activities, use of data analytics for planning and budgeting and reporting by dashboards.

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

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

(4) Challenges

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

? Briefly describe the advantages and challenges of Auditing digitally. **(ICAI SM)**

3 UNDERSTAND THE IT ENVIRONMENT

Understanding the ways in which

- ✔ **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
  - ✔ whether to include specialists in the complexity assessment.

Understanding of the Automated Environment

- The auditor's understanding of the automated environment should include the following:
  - ✔ **Applications** that are being used by the company.
  - ✔ Details of the **IT infrastructure components** for each of the application.
  - ✔ **Organisation structure and governance.**
  - ✔ **Policies, procedures and processes** followed.
  - ✔ Extent of **IT integration, use of service organisations.**
  - ✔ **IT risks and controls.**

The illustration below is an example of how an auditor can document details of an automated enviornment:

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

(I) Key Areas for an Auditor to Understand IT Environment

- **Understand the flow of transaction:** Auditor's understanding of the IT environment

may focus on **identifying and understanding the nature and number of the specific IT environment** that are relevant to the flows of transactions and processing of information in the information system. **Changes in the flow of transactions, or information** within the information system may **result from program changes to IT applications,** or direct **changes to data in databases** involved in processing or storing those transactions or information.

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

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

- **Identification of the technologies used:**
  - ✔ The need to **understand the emerging technologies implemented, role they play (in the entity's information processing or other financial reporting activities),** and consider whether there are **risks arising from their** use.
  - ✔ Given the potential complexities of these technologies, the engagement team may decide to **engage specialists and/or auditor's experts** to help understand whether and how their use impacts the entity's financial reporting processes and may give rise to risks from the use of IT.
  - ✔ 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

Assessing the complexity of the IT environment:

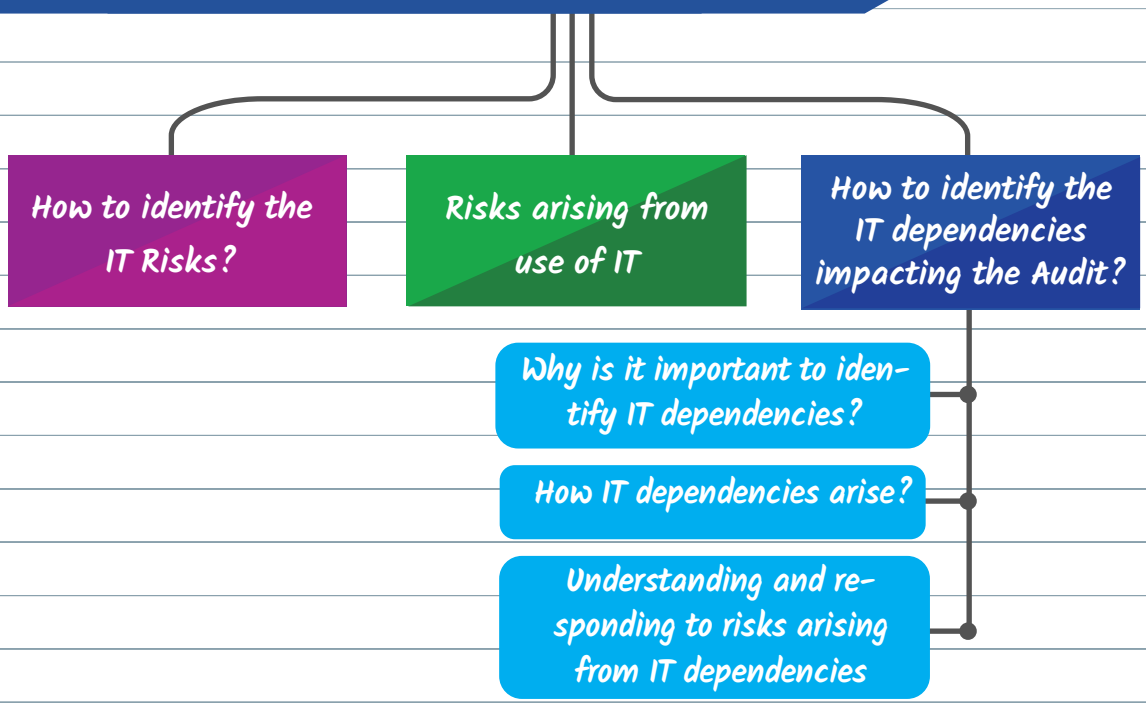
The level of complexity for individual characteristics differs across applications. Complexity is based on the following factors –

- ✔ **Automation** used in the organisation,
- ✔ Entity's **reliance on system generated reports,**
- ✔ **Customisation** in IT applications,
- ✔ **Business model** of the entity,
- ✔ Any **significant changes** done during the year; and
- ✔ **Implementation** of emerging technologies.

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

? What are the stages involved in understanding the IT environment and what key considerations auditor should consider. **(ICAI SM)**

4 IDENTIFYING THE RISKS ARISING FROM USAGE OF IT



(1) How to identify the IT Risks?

- 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.**
- There will be more risks arising from the use of IT when the **volume or complexity of automated application controls is higher, and management is placing greater reliance on those controls** for effective processing of transactions or the effective maintenance of the integrity of underlying information.

(2) Risks arising from use of IT

- **Unauthorised access to data** that may result in destruction of data or improper changes to data, including the recording of unauthorised or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database.
- Possibility of IT personnel **gaining access privileges** beyond those necessary to perform their assigned duties thereby breaking down segregation of duties. Unauthorised changes to data in master files.
- **Unauthorised 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 cyber security controls and protocols not followed it may lead to loss of sensitive data, hackers might encrypt the system or illegally break into the 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, cyber attacks or power outage. It means the IT systems will not be operational or will be unavailable /offline which may hamper the business.
- **System integration and System compatibility:**

  System integration:

  Meaning: it means integrating one or more systems.

  Risk involved: 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:

Meaning: it means sharing compatible hardware, software and operating system while performing the integration.

Risk involved: 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.
  For example, a FMCG sector will be subject to different regulatory requirements than a financial company, however both businesses will need to manage their respective compliance risks.
- **Performance issues** arises with the way requests are processed in the IT systems. Heavy data load, network usage impacts the application performance and its responsiveness.
  To overcome the performance issues of IT systems, resources or hardware can be added to an existing nodes, which is known as scaling.

(3) How to identify the IT dependencies impacting the Audit?

1. Why is it important to identify IT dependencies?

Identifying and documenting the entity's IT dependencies in a consistent, clear manner helps to:

- identify the **entity's reliance upon IT,**
- understand **how IT is integrated into the entity's business model,**
- identify **potential risks arising from the use of IT,**
- identify related **IT General Controls;** and
- enables us to **develop an effective and efficient audit approach.**

2. How IT dependencies arise?

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

There are **five types of IT** dependencies as described below:

Automated Controls

- Automated controls are designed into the IT environment to **enforce business rules**.
- For example, Purchase order approval via workflow or format checks (e.g., only a particular date format is accepted), existence checks (e.g., Duplicate customer number cannot exist), and/or reasonableness checks (e.g., maximum payment amount) when a transaction is entered.

Reports

- System generated reports are information generated by IT systems.
- These reports are often **used in an entity's execution of a manual** control, including business **performance reviews**, or may be the source of entity information used **by auditors** when selecting items for testing, performing substantive tests of details or performing a substantive analytical procedure.
  E.g. (Vendor master report, customer ageing report).

Calculations

- Calculations are accounting **procedures that are performed by an IT system instead of a person**.
- For example, the system will apply the 'straight-line' depreciation formula to calculate depreciation of an asset (i.e., cost of the asset, less the residual value of the asset at the end of its useful life divided by the useful life of the asset) or the system will calculate the value of the amount invoiced to a customer by multipiling the item price times the quantity shipped.

Security

- Security including segregation of duties is enabled by the IT environment **to restrict access to information** and to determine the separation of roles and responsibilities that could allow an employee to perpetrate and conceal errors or fraud, or to process errors that go undetected.

Interfaces

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

3. **Understanding and responding to risks arising from IT dependencies**

- When auditor identify IT dependencies that are relevant to the entity's flow of transactions and processing of financial information, he need to understand **how management responds to the associated risks that may arise from them.**
- Management may **implement Information Technology General Controls (ITGCs) to address risk** related to IT dependencies.

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

Access Security Objective:	**Program Change Objective:**	**Data Centre and network operations objective:**
To ensure that access to programs and data is authenticated and authorised to meet financial reporting objectives. ▸ Access requests to the application are properly reviewed and authorised by management. ▸ Access to terminated user is removed on a timely basis. ▸ Access rights to applications are periodically monitored for appropriateness. ▸ Transactions of administrative and sensitive generic IDs are monitored. ▸ Security policies and procedures are maintained. ▸ Access to operating system and database is restricted.	**To ensure modified systems continue to meet financial reporting objectives** ▸ Change Management policy and procedures are maintained. ▸ Development, testing and production environments are segregated for changes to application configurations. ▸ Changes are adequately tracked and recorded. ▸ Changes to application configurations are adequately tested and approved before being migrated into production. ▸ Emergency changes are approved. ▸ Segregation of duties is maintained between developer and implementor.	**To ensure production systems are appropriately backed up to meet financial reporting objectives** ▸ Policies and procedures for data backup and recovery is maintained. ▸ Data is appropriately backed up and recoverable. ▸ Restoration testing is performed. ▸ Monitoring and compliance of service level agreements. ▸ Batch job scheduled are monitored for failures and access is restricted.

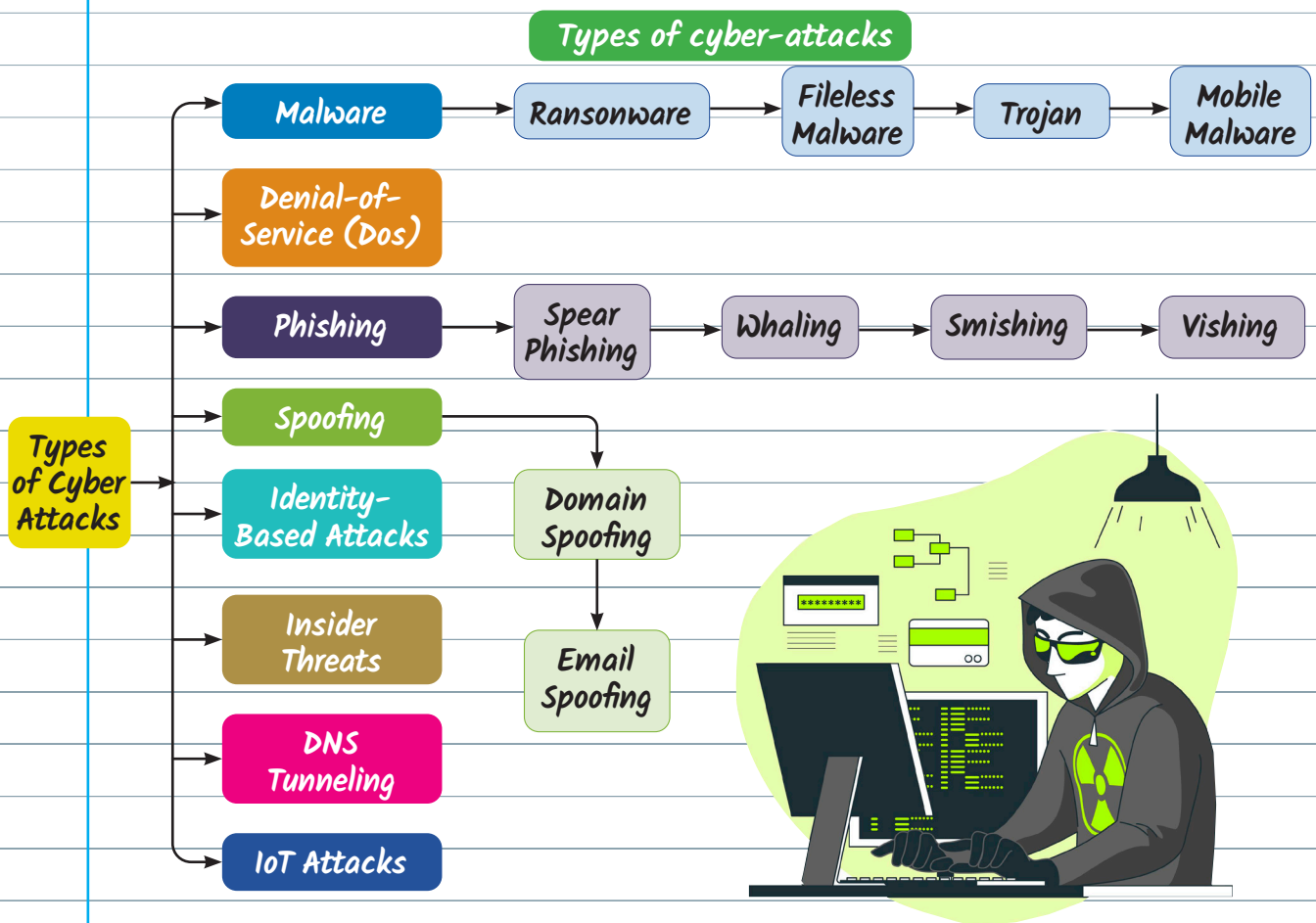
- IT dependencies may also **affect the design of the entity's controls and how they are implemented.**
  Therefore, auditor should **consider IT dependencies relevant to audit and evaluate the related risks.**
- Auditor should **scope in ITGCs to tests when there are IT dependencies identified in the system.** If the controls around IT environment are not implemented or operating effectively it will result in not relying on ITGCs which means the IT dependencies could not be relied upon.

? Auditor should scope in ITGCs to tests when there are IT dependencies identified in the system. Briefly describe the types of IT dependencies. **(ICAI SM)**

5 ASSESSING CYBER RISKS (INCLUDING REMOTE AUDIT)

(1) What is Cyber Risk?

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



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 cyber attack, its subsets are ransomware, fileless Malware, trojans, viruses etc.

Ransomware

- In a ransomware attack, an adversary **encrypts a victim's data** and offers to **provide a decryption key in exchange** for a payment.
- Ransomware attacks are usually **launched through malicious links delivered via phishing emails,** but unpatched vulnerabilities and policy misconfigurations are used as well.

Fileless Malware

- Fileless malware is a type of **malicious activity that uses native, legitimate tools built into a system** to execute a cyber-attack.
- Unlike traditional malware, fileless malware **does not require an attacker to install any code** on a target's system, making it hard to detect.

Trojan

- A trojan is malware that **appears to be legitimate software disguised as native operating system programs or harmless files** like free downloads.
- Trojans are **installed through social engineering techniques** such as phishing or bait websites.

Mobile Malware

- Mobile malware is any type of **malware designed to target mobile devices.**
- Mobile malware is delivered through **malicious downloads, operating system vulnerabilities, phishing, smishing, and the use of unsecured Wi-Fi.**

Denial-of-Service (DoS) Attacks:

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

Phishing: Phishing is a type of cyber attack 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.

Spear Phishing

- Spear-phishing is a type of phishing attack that **targets specific individuals or organisations typically through malicious emails.**
- The goal 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 pretending to be from reputable companies** in order to induce individuals to **reveal personal information,** such as passwords or credit card numbers.

Vishing

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

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

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 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 and interact with its contents, such as a malicious link or attachment.

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

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

- ***DNS Tunneling:*** *DNS Tunneling is a type of cyber attack that* ***leverages Domain Name System (DNS) queries and responses*** *to bypass traditional security measures and transmit data and code within the network.*
  This tunnel ***gives the hacker a route to unleash malware and/or to extract data, IP or other sensitive information*** *by encoding it bit by bit in a series of DNS responses.*

- ***IoT-Based Attacks:*** *An IoT attack is any cyber attack 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.*

(2) Stages of Cyber Risks

Following are 3 Stages of cyber risk: (Each risk differs from entity to entity and attack to attack)

STAGE 01

Assessing the cyber risk

No organisation is completely immune to a cyber-risk, hence every organisation should consider at least the **common threats-**

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

STAGE 02

Impact of cyber risk

Cyber-attack can impact one, two or more types of risks. Some of the indicative areas of impact of attack can be –

- **Regulatory costs**
- **Business interruptions:** Causing operational challenge.
- **Data loss, reputational loss and litigation.**
- **Ransomware:** Most common, entire systems are encrypted.
- **Intellectual property theft:** Loss of competitive advantage, & risk & impairment/impediment charge because of loss of IP.
- **Incident response cost:** For investigations & remediations.
- **Breach of Privacy, if personal data of a consumer is hacked.**
- **Fines and penalties**

STAGE 03

Managing the cyber risk

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

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

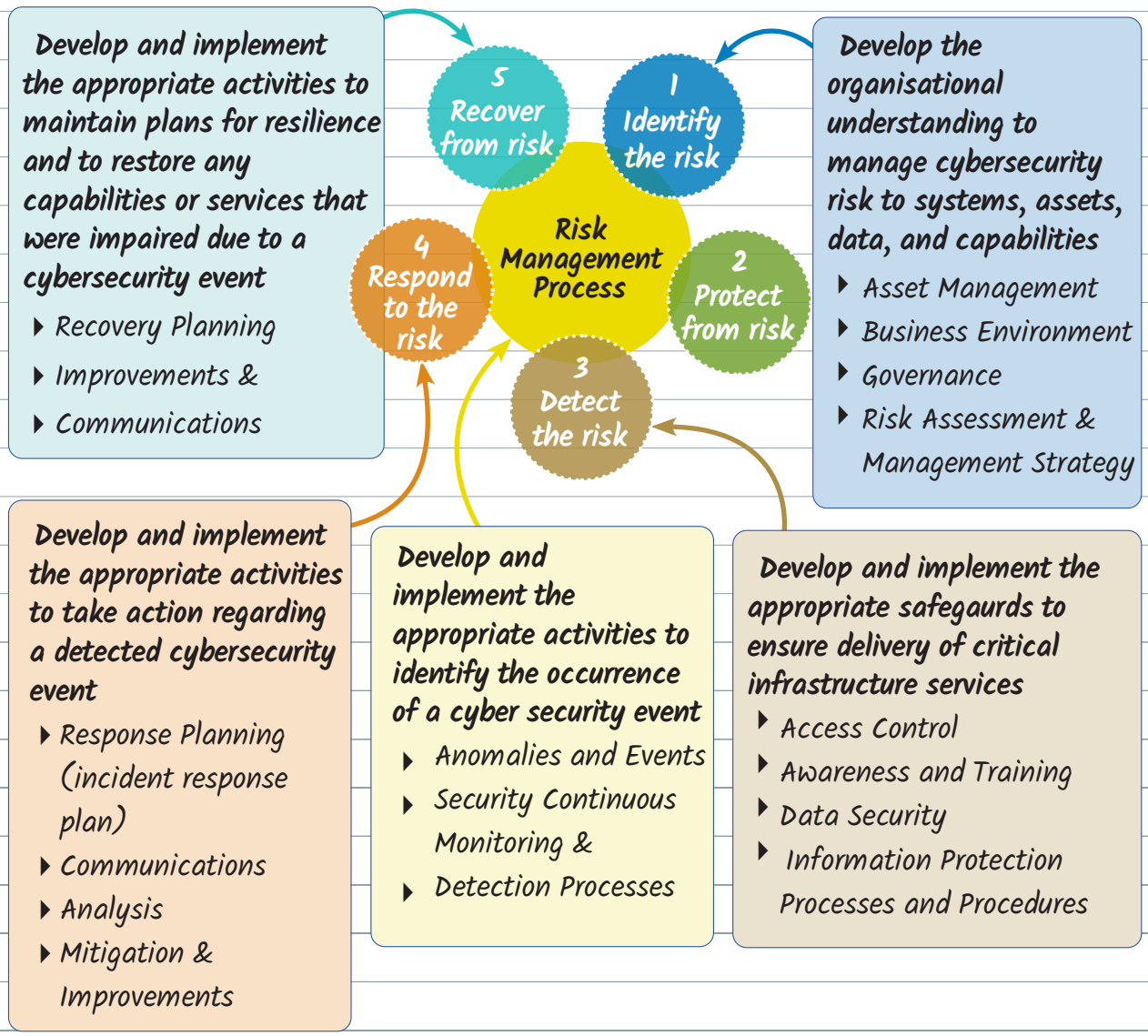
? What does cyber risk explain it with some examples. **(ICAI SM)**

(3) **Cybersecurity Framework**

Cybersecurity framework includes:

i. how management is
   - **identifying the risk.**
   - **protecting and safeguarding its assets** (including electronic assets) from the risk.

ii. **Management preparedness to detect the attacks, anomalies and responsiveness** to the adverse event.



I. **Identify the risk**

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

- Entity should conduct a **periodic risk assessment & develop a management strategy** which identifies cybersecurity risks around IT system failure affecting the entity's primary business or potential loss of data or inability to access data as required, risk of unauthorised access to the IT network.
- Entity should maintain and periodically reviews an inventory of their information assets i.e., **Asset Management** (e.g., intellectual property, patents, copyrighted material, trade secrets and other intangibles).
- Entity should **classify and prioritize protection of their information assets based on sensitivity** and business value and periodically reviews the systems connected to the network on which digital assets reside.
- From governance perspective, management should **review how cyber security risks** affect **ICs over financial reporting.** In case of adverse attack how management is going to assess the impact on the recoverability of financial data and impact on revenue recognition.
- Management needs to **identify if any established risk-based cyber security program** can be leveraged e.g. (NIST, ISO etc.)
- To determine overall responsibility for cyber security in the business environment entity should **establish roles and responsibilities over cyber security** (CISO, CIO).
- Further the risk assessment should be discussed with TCWG (e.g., Audit Committee or Board of Directors).

2. Protect the risk

- Obtain an **understanding of the entity's processes for safeguarding of assets** subject to cyber security.
- Entity should:
  - ✔ Monitor whether there has been **unauthorised access to electronic assets** and any related impact on financial reporting.
  - ✔ Implement **effective controls** for data security.
  - ✔ Have a process & procedures in place for **identifying material digital/electronic assets on the B/S** subject to cyber security risk (e.g., intellectual property, patents, copyrighted material, trade secrets) and prioritizing their protection based on criticality.
- **Formal training** should be conducted to make teams aware of the risk associated with cyber- attacks.

3. **Detect the risk**

- Entity should have controls and procedures that:
  - ✔ Enable it to **identify cyber security risks and incidents**
  - ✔ To **assess and analyse their impact** on its business,
  - ✔ Evaluate the **significance associated with such risks and incidents,** and
  - ✔ Consider **timely disclosures.**
- Review entity's processes to **monitor and detect security breaches or incidents.**
- If management has implemented **anti-virus** in the system to secure it from anomalies or if **firewall logs are being continuously monitored** to detect any repetitive attacks.
- A **monitoring process** should be established to review how many such events have been denied by the firewall. Monitoring process should also include any **upgrades or updates** 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 and how the incident or data breach was identified.**
- Entity should have a **response planning** in place to capture the details of nature of incident and the same needs to be **communicated** with those who are ultimately responsible for this framework and with TCWG.
- The security incident response plan helps in **analysing the impact and severity of the attack** and helps the organisation in taking the **appropriate actions.**
  Management should **assess-**
  - ✔ Litigation costs,
  - ✔ Regulatory investigation costs, and
  - ✔ Remediation costs

  as a part of **mitigation process and improvement.**
- Management should assess the **future action plans** that needs to be taken to safe-guard the organisation from such attacks.

5. **Recover from risk**

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

- Once the impact **evaluated and communicated with the regulators the recovery plan** needs to be implemented to overcome the impact.
- **Necessary improvements** – like patch upgrades, better controls, improved technology in terms of firewall, anti-virus, tools, etc. needs to be implemented to safeguard the entity.

? Briefly describe the cyber security Framework. **(ICAI SM)**

(4) Control considerations for Cyber Risks

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

Controls around		
Vendor setup and modifications	**Electronic transfer of funds**	**Patch management**
■ Certain cyber schemes exist in which changes to bank account or other **critical vendor information are requested** through email phishing scams by **individuals**	■ Wire transfers or electronic funds transfers, similar to vendor changes noted earlier, cyber schemes **pertaining to fraudulent requests for wire transfers** are made	■ Cyber and ransomware attacks **exploit known security vulnerabilities** resulting in the manipulation or the destruction of data. Exploitations of known

claiming to be authorised vendor personnel. ▪ Entities have ***inappropriately dispersed funds*** to these individuals and therefore, inappropriately ***reduced the liability owed to the actual vendor***, resulting in an impact to the FS (i.e., loss of cash and related expense) ✓ Who is responsible for making changes to vendor master data? Is the process centralized or decentralized? ✓ Are other communication channels, such as email, used to request changes to vendor master data? (If yes, consider if multi-factor authentication is enabled for email). ✓ What systems and technologies are used to initiate, authorise and process requests related to changes to vendor master data? ✓ Are authentication protocols defined to verify modifications to vendor master data (e.g., call back procedures, multi-factor authentication)?	relating to business transactions and vendor payments, as well as ***fraudulent requests appearing to come from financial institutions*** requesting disbursement from customer asset accounts. ✓ Are personnel responsible for wire transfers educated on the relevant threats and information related to common phishing scams associated with fraudulent requests for wire transfers? ✓ Are authentication protocols defined to verify wire transfer requests (e.g., call back procedures, dual-authentication procedures)? ✓ What systems and technologies are used to facilitate the request/initiation, authorisation and release of 0 wire transfers?	security vulnerabilities are often ***caused by unapplied patches or upgrades***. ✓ Does the entity have a patch management program? ✓ Does the entity run periodic vulnerability scans to identify missing/unapplied patches? ✓ How is the entity notified of patches by external vendors (e.g., Microsoft for Windows patches)?

(5) Remote Audit

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

I. Considerations for remote audit

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

(a) Feasibility and Planning

- Planning should involve agreeing on **audit timelines, meeting platform** (Zoom calls/ Microsoft Teams/Google Meet) to be used for audit sessions, data exchange mechanisms, any access authorisation requests. Ensure feasibility is determining what technology may be used, if auditors and auditees have competencies and that resources are available.
- The execution phases of a remote audit involve video/tele conferencing with auditees. The documentation for audit evidence should be transferred through a **document sharing platform**.

(b) Confidentiality, Security and Data Protection

- To ensure data security and confidentiality, **access** to document sharing platform should be **sufficiently restricted** and secured by encrypting the data that is sent across the network.
- The information, **once reviewed and documented by auditor**, is **removed from** the **platform**, and stored according to applicable archiving standards and data protection requirements.
- Auditors should **take into consideration legislation and regulations**, which may require additional agreements from both sides (e.g., there will be no recording of sound and images, or authorisations to using people's images).
- Auditors should **not take screenshots of auditees** as audit evidence. Any screenshots of documents or records or other kind of evidence should be

previously authorised by the audited organisation.

- In case of accessing the auditee's IT system auditor should **use VPN** (Virtual private network).
  - ✔ VPN is a service which creates safe and encrypted online connection.
  - ✔ It prevents unauthorised users to enter into network and allows the users to perform work remotely.

C **Risk Assessment**

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

2. Advantages and Disadvantages of remote audit

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

DOS 'N' DONTS: (Opportunity, Flexibility, Data Privacy, List of People working remotely, VPN, Resignation of staff)

- Remote auditing plays a vital part, and provides an opportunity for organisations and auditors to **leverage communication technology tools.**
- In addition, management perception is changing as it **provides flexibility in terms of time, along with the reductions in cost.**
- Auditor should also consider, if **access to system and network is provided post appropriate approvals,** and if data is transferred through encrypted means to maintain data privacy.
- Management should **maintain and review the list of people who are working remotely** and make sure they access the system and network through VPN (Virtual Private Network) only and such accesses should be approved.
- Further once the **employee leaves the organisation** or audit is completed such **VPN access** should be **terminated timely**. Auditors can test such controls while performing remote audit.

? What are the advantages and disadvantages of remote audit. **(ICAI SM)**

6 EMERGING TECHNOLOGIES IN AUDIT

- Some **examples of emerging technologies** are – Data analytics (CAATs (ACL, Alteryx, Power BI, CaseWare), Artificial Intelligence (AI), Robotic Process Automation, and blockchain).
- These technologies are **changing the way business gets done**, and auditors are leading by transforming their own processes.
- Some important **considerations** for auditors are:
  - ✔ to assess the **impact of emerging technologies on business**
  - ✔ evaluate whether management is properly **assessing the impact of emerging technologies on IC over financial reporting.**

A Data Analytic Techniques

- **Generating and preparing meaningful information from raw system data** using processes, tools, and techniques is known as Data Analytics.
- Audit analytics or audit data analytics involves **analysing large sets of data to find actionable insights, trends, draw conclusions and** for **informed decision making.**

- The use of audit analytics enables **greater efficiencies and more accurate findings** from the review process.
- As a result, businesses will be able to create **strategies based on verifiable data and professional assumptions and** auditors can **improve the audit quality**.
- It allows auditors to **more effectively audit the large amounts of data held and processed in IT systems** in larger clients.
- Audit analytics helps:
  - ✔ To **discover and analyse patterns**
  - ✔ **Identifying anomalies**
  - ✔ **Extract other useful information** in data
- The data analytics methods used in an audit are known as **Computer Assisted Auditing Techniques (CAATs)**.
  - ✔ It involves **use of multiple data analytical tool or visualization tools** that can help the auditor to deep dive into the problem statement and hence increase the audit quality.
  - ✔ This also **minimises the scope of missing out on key attributes** that might be of a higher risk to the organisation and its respective business.

Tools used as a part of CAATs

Auditor performing audit analytics can make use of various applications and tools that help them to analyse large data sets and obtain insights that help them to make the quality of the audit better.

Some of the popular tools used across the industry as part of CAATs are listed below:

	Audit Command Language (ACL)	Alteryx	Power BI	CaseWare
Description	• It 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.	• It is used to **consolidate financial or operational data** to assess controls. • A fully **transparent audit trail of every action** is performed in Alteryx in form of a workflow which makes it easier for the user to learn as **no prior knowledge of coding or scripting is required**. • It 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.	• It is a **business intelligence (BI) platform** that provides non-technical business users with **tools for aggregating, analysing, visualising and sharing data**. • From audit perspective, such **visualisation tools can be used to find the outliers in the population**, it can also be **used for reporting** purpose in an interactive dashboard to the higher management.	• It 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** and helps in **streamlining processes and eliminating the routine tasks**. • Used by accounting firms, governments and corporations worldwide.
Example	ACL is **used to analyse and check complete data sets to perform Trial Balance reconciliations** during the audits.	Alteryx used for **logistics organisation** to recompute the revenue entries recorded by the system to match with the financials that showcased the expected revenue turnover.	Power BI dashboard used for checking the outliers of the **apparel company.**	• Provides solutions to **build accounting software** which turns any document, including FS into cost

Example	In such case scenarious, the entity provided the General Ledger dump and system Trial Balance. Using ACL, the completeness of the data can be ensured as the data set exceeded beyond the capacity of the excel and baisc functions like record count, sum, pivoting can be performed within ACL where excel could not perform such actions.	Due to Alteryx's processing speed and ease to implement functions, auditors could perform re-computation for all the transactions entry and noted that the revenue was being understated as the expected revenue was more than the actual calculated. This was due the fact that the addendum between the logistic company and the client was not revised in the system and old versions of rates were used to compute the revenue. Alteryx helped in analysing and recomputing the huge data set and to focus on actual risk.	Auditors were required to analyse the trends of the sales during the year. By the use of Power BI, the sales data provided by the client was further converted into dashboard to analyse the trends and patterns as per the market standards. In analysis performed on untimely sales, it was noted that sales transactions were performed during non-business hours.	• effective client ready report. • Automatically links to client data and securely communicate with the client in real time. • Regardless of location, all authorised users have access to the same documents. • Consistency of data is ensured.

? *In an automated environment, the data stored and processed in systems can be used to get various insights into the way business operates. This data can be useful for preparation of management information system (MIS) reports and electronic dashboards that give a highlevel snapshot of business performance. In view of above you are required to briefly discuss the meaning of data analytics and example of such data analytics techniques.* **(ICAI SM)**

7 AUTOMATED TOOLS IN AUDIT

- *Automation and use of technology often requiring auditors to understand and perform procedures on a larger group of systems that produce information relevant to the production of FS.*
- *Based on management's and auditors' independent risk assessment procedures, the audit's scope may need to include peripheral systems, as well as testing general IT and application controls relative to those systems due to the increased use of technology that is relevant to financial reporting.*
- ***Robotic Process Automation (RPA), blockchain, machine learning, Internet of Things (IOT)** and **Artificial Intelligence (AI)** are some prime examples of automation.*

	Internet of Things	Artificial Intelligence (AI)	Blockchain	Robotic Process Automation (RPA)
Description	• IoT is the concept of **connecting any device** (cell phones, coffee makers, washing machines, and so on) **to the internet**. • Key components of IoT are data collection, analytics, connectivity, and people and process. • IoT not only changes the business model, but also affects the strategic objectives of the organisation. • The risk profile of the entity changes with exposure to new laws & regulations.	• It refers to a **system or a machine that can think and learn.** • It **utilises data analysis and algorithms** to make decisions based on predictive methods. • Complex algorithms are developed to propose decisions based on a pattern or bahavior learned over time. • The self-deploying robots can determine how much vacuuming there is to do based on a room's size, uses AI to scan room size, identify obstacles and remember the most efficient routes for cleaning. • Siri to help find your Air Pods or told Amazon Alexa to turn off the lights, quick commands to open a phone camera or start a particular playlist, AI to predict when to book the lowest prices for flights, hotels, car and vacation home rentals.	• It is based on a **decentralized and distributed ledger** that is secured through encryption. • **Each transaction is validated** by the blockchain participants, creating a block of information that is replicated and distributed to all participants. • All blocks are sequenced so that any modification or deletion of a block disqualifies the information.	• It is the **automation of the repetitive processes** performed by users. • It is a software technology that **emulate humans' actions interacting with digital systems and software.** • **Process efficiency, customer experience and control effectiveness** contributed to RPA. • RPA software bots **can interact with any application or system** the same way people do except that RPA bots can operate around the clock, nonstop, much faster and with 100% reliability and precision.
Example	• Connected Cars, connected manufacturing equipment's, smart home security or Data from	• Self-driving cars, manufacturing robots, smart assistants, marketing chatbots, virtual travel booking agent.	• Bitcoin, crypto-currency transfer application - Blockchain in	

	Internet of Things	Artificial intelligence (AI)	Blockchain	Robotic Process Automation (RPA)
Example	whether equipment will break machines can be used to predict down, giving manufacturers advance warning to prevent long stretches of downtime. Or a refrigerator placing an order with a grocery store whenever the supply of eggs falls below a certain number. Or smart oven works by scanning QR or bar codes and connecting to wi-fi, which it then uses to determine the best temperature and time to cook the food to avoid undercooking or burning. Researchers uses IoT devices to gather data about customer preferences and behaviour, though that can have serious implications for privacy and security.	The self-deploying robots can determine how much vacuuming there is to do based on a room's size, uses AI to scan size, identify obstacles and remember the most efficient routes for cleaning.	money transfer, blockchain smart contracts.	
Audit Implications	• A shift to connected devices and systems may result in auditors not being able to rely only on manual controls. • Audit firms may need to train and upskill auditors to evaluate the design and operating effectiveness of automated controls. • Consumer-facing tools that connect to business environments in new ways can impact the flow of transactions and introduce new risks for management and auditors to consider. • For example, consider payment processing tools that allow users to pay via credit card at	• Given the invisible nature of algorithms, audits must focus on the logical flow of processes. • A review of AI should ascertain whether unintended bias has been added to the algorithms. • Auditors should assess the effectiveness of algorithms and whether their output is appropriately reviewed and approved. • Auditors must also consider	• Auditors should consider appropriate governance and security transactions around the transactions. • Although blockchain's core security premise rests on cryptography, there are risk factors associated with it. • As blackchain interacts with legacy systems and business partners, concerns	• Auditors should understand RPA processes, which include data extraction, aggregation, sanitisation and cleansing. • To perform substantive testing,auditors must have an understanding

	Internet of Things	Artificial intelligence (AI)	Blockchain	Robotic Process Automation (RPA)
Audit Implications	a retail location through a mobile device. This could create a new path for incoming payments that may rely, in part, on a new service provider supplying and routing information correctly. Auditors would need to consider the volume of those transactions and the processes and controls related to it.	cybersecurity and search for possible bugs and vulnerabilities that can be exploited to impact AI functionality, as AI is built on software modules. • Auditors should confirm their understanding of how the use of AI affects the entity's flows of transactions, including the generation of reports or analytics used by management. • Auditors also should consider whether the AI is making decisions—or being utilised by management as partof the decision-making process. • If management shifts its focus on oversight by relying on AI, auditors should understand: ✔ what shift occurred, ✔ how new risks might be addressed, ✔ whether existing risks may not be getting the same level of attention. •Understanding these changes could drive changes in the audit approach.	related to insecure application programming interfaces (APIs), data confidentiality and privacy cannot be ignored. Weak blockchain application development protocols are something auditors cannot overlook. • Auditors must be able to determine whether the data put on blockchain will expose the enterprise to liability for non-compliance with applicable laws and regulations.	of the tools used to develop and maintain RPA.This will be helpful when auditors review logs, configuration controls, privileged access controls and the like. • General IT controls are applicable as always.
Common Risks	Key risks associated with IoT, including, device hijacking, data siphoning, denial of service	• **Security:** It is one of the key risks – the more data the system uses, from more sources, the more entry points and connections are formed and the greater the potential risks. • **Inappropriate configuration:** AI may also be used to diagnose medical conditions. If it is	• **Inability to reverse transactions:** The inability to reverse transactions and to access data without the	• **Operational and execution risks:** ✔ Robots are deployed without proper

	Internet of Things	Artificial intelligence (AI)	Blockchain	Robotic Process Automation (RPA)
Common Risks	attacks, data breaches and device theft.	badly configured or malfunctions, it could harm people before the problem is spotted. • **Data privacy:** The data used and shared should have the necessary explicit consent from data providers.	• required keys make the system secure, but also mean that organisations need specific protocolsand management processes to ensure that they are not locked out and have clear contingency plans. • **Cyber-attacks and data hacks:** Operating through network nodes could also expose the organisation to cyber-attacks and data hacks. • Auditors should also ensure that the organisation has the necessary data management processes and complies with regulations. • **Regulatory compliances:** The regulatory landscape is still evolving for blockchain, so audit teams should check that compliance managers are following developments constantly and adapting processes accordingly.	operating model. ✔ Buying the wrong tool, making wrong assumptions, taking shortcuts, and threatening security and compliance. ✔ Assigning proper responsibilities, training and clearly stating about changing roles also can help you reduce operational risk to a great extent. • **Change management risks:** Not following the change management implementation lifecycle, improper and incomplete testing (not covering all scenarios) leads to inaccurate results. • **RPA Strategy Risk:** ✔ Setting wrong expectations, improper KPIs, and unrealistic business goals creates an environment of uncertainty. ✔ Management should discuss, and analyse the complete working characteristics, potential, and limitations of RPA before drafting a RPA.

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

➡ **RPA to check IND AS, IFCoFR and Standards on Auditing (See RPA workflow chart at end of this chapter)**

Incorporating Standards on Auditing, IFCoFR, INDAS (para-wise details of | Para reference | Accounting policy | Relevant data to be captured | Relevant calculation to be made | Presentation in FS | IFCoFR | Audit procedures as per Standards on auditing |) in audit practices **ensures accurate financial reporting, effective ICs, and reliable audit procedures.** Leveraging RPA in conjunction with these frameworks can significantly enhance audit efficiency, accuracy, and compliance. **RPA developers and auditors should collaborate to align RPA workflows**

with relevant standards and guidelines, ultimately improving the effectiveness of audits and enhancing client assurance given at the end of this chapter.

7A NFT (NON-FUNGIBLE TOKEN) (Blockchain Technology)

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

Key Features of NFT

- **Digital Asset:** NFT is a digital asset that **represents Internet collectibles** like art, music, and games with an authentic certificate created by blockchain technology that underlies Crypto-currency.
- **Unique:** It **cannot be forged or** otherwise **manipulated.**

Exchange: NFT **exchanges take place with cryptocurrencies such as Bitcoin** on specialist sites.

Challenges of NFT

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

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

8 CONTROL CONSIDERATIONS OR OBJECTIVES OF AUDITING DIGITALLY

(Holistic approach, New Tech Risk, Upskill)

Auditors should focus on the following control considerations:

- 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.

- Auditors 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.
- 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.

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

- Reliance on systems or programs that are **inaccurately processing data, processing inaccurate data, or both.**
- **Unauthorised access to data** that might result in destruction of data or improper changes to data, including the recording of unauthorised or non-existent transactions or inaccurate recording of transactions (specific risks might arise when multiple users access a common database)
- Possibility of IT personnel **gaining access privileges beyond those necessary** to perform their assigned duties, thereby leading to insufficient segregation of duties.
- **Unauthorised or erroneous changes to data in master files.**
- **Unauthorised changes to systems or programs.**
- **Failure to make necessary or appropriate changes to systems or programs.**
- **Inappropriate manual intervention.**
- **Potential loss of data or inability to access data as required.**
- **Risks introduced when using third-party service providers.**
- **Cybersecurity risks**

(I) Key steps for Auditors in a Changing Technology Environment

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

- **Maintain sufficient professional skepticism** when reviewing management's risk assessment for new systems.
- **Understand direct and indirect effects of new technology** and determine how its use by the entity impacts the auditor's overall risk assessment.

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

9 NEXT GENERATION AUDIT

The Next Generation Audit is **human-led, tech-powered and data-driven.** It is based on

FROM		TO
Sampling populations	→	Full population analysis
Multiple datasets	→	One data set
Disconnected tools	→	Integrated ecosystem services
Manual risk assessments	→	Dynamic, data-driven risk assessment
Separated communication	→	Embedded communication
Repetitive tasks	→	High value work and capacity for growth
Manual work	→	Automation
Ad-hoc insights	→	Insights from a broader audit

3D printing, Augmented Reality (AR) and Virtual Reality (VR), biotechnology, auditing through drones [also known as an 'Unmanned Aerial Vehicle' (UAV)] and quantum technology are some of the most rapidly advancing areas, with many implications for society.

For example, Drone Technology: Using drone technology in the remote locations for stock counts. Drones have great payload capacity for carrying sensors and cameras, thus they can photograph and physically examine the count of large quantities of fixed assets and inventory. Drone captured audit information can be combined with various alternative sources of information such as QR code readers, handheld bar scanners, manual counts etc. to optimize quality of deliverables, consolidate audit information and enhance the execution speed while ensuring correctness and completeness of data.

A Drone Technology:

- Using drone technology in the **remote locations for stock counts.**
- Drone have great payload capacity for carrying sensors and cameras, thus they can photograph and physically examine the count of large quantities of fixed assets and inventory.
- Drone captured audit information can be **combined with various alternative sources of information** such as QR code readers, handled bar scanners, manual counts etc. to optimise quality of deliverables, consolidate audit information and enhance the execution speed while ensuring correctness and completeness of data.

B Augmented Reality:

Technology **allows users to view the real-world environment with augmented (added) elements,** generated by digital devices.

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

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

Examples of Augmented and Virtual Reality:

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

In **health sector,** AR can provide surgeons with additional information when operating on a patient, such as heartbeat and blood pressure monitoring and virtual x-rays. Vision Pro is essentially an Augmented-Reality (AR) headset that "seamlessly" blends the real and digital worlds. The device can switch between augmented and full Virtual Reality (VR) using a dial.

C Metaverse

- Metaverse is the emerging **3-D digital space that uses Virtual Reality, Augmented Reality, and other advanced internet technology** to allow people to have lifelike personal and business experiences online.

- It represents a **convergence of digital technology** to combine and extend the reach and use of Cryptocurrency, Artificial Intelligence (AI), Augmented Reality (AR) and Virtual Reality (VR).
- The internet offers many experiences today, but tomorrow's Metaverse will feel more interconnected than ever before. We are heading towards mature landscape of virtual spaces with transferable identities and assets enabled by blockchains (NFTs) that are interoperable or interchangeable. It further includes **highly automated systems, immersive interfaces, hyperconnected networks and digital reflections.**

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

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

(a) **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 personalised financial dashboards, and perform transactions using virtual currencies.**
- ✔ Customers can **seamlessly transfer funds, make virtual purchases, and engage in virtual commerce,** all within the immersive environment of the metaverse.
- ✔ Example, XYZ Bank leverages the metaverse to provide a convenient and interactive banking experience, attracting tech-savvy customers who value digital innovation.

(b) **Digital Asset Management:**

- A digital asset management company, recognises the growing popularity of virtual assets in the metaverse. They launch **a virtual asset trading platform within the metaverse, allowing users to buy, sell, and trade NFTs and other digital assets.**
- Investors can **diversify their portfolios, participate in virtual auctions, and even showcase their virtual art collections in virtual galleries.**
- Example, Crypto Investments Ltd. leverages the metaverse's decentralized and secure infrastructure to facilitate transparent and efficient transactions of virtual assets.

(c) **Virtual Financial Education and Training:**

- A Financial Learning Academy aims to enhance financial literacy using the metaverse. They create a **virtual classroom environment** where participants can attend interactive financial education sessions. Students can engage in simulated investment activities, learn about budgeting and financial planning, and gain hands- on experience through virtual trading simulations. Financial Learning Academy leverages the immersive nature of the metaverse to provide an engaging and practical financial education platform, preparing individuals for real-world financial challenges.

(d) **Virtual Meetings and Conferences:**

- For a leading industry even an organisation hosts a **virtual conference** within the metaverse. Participants from around the world can access the conference through their virtual avatars. They can attend keynote speeches, panel discussions, and networking events in virtual conference halls. Attendees can interact with industry experts, explore virtual exhibition booths, and establish valuable connections in the financial sector.
- Example, Global Finance Summit leverages the metaverse to create a global and inclusive conference experience, fostering collaboration and knowledge sharing.

(e) **Data Visualisation and Analytics:**

- A company utilises the metaverse to offer **advanced data visualisation and analytics tools** to financial professionals. Their **virtual analytics platform allows users to visualise complex financial data in interactive and immersive 3D environments.**

- Users can **explore data trends, conduct simulations, and analyse financial performance** through intuitive interfaces within the metaverse.
- Example, Analytics Solutions Inc. leverages the metaverse's immersive capabilities to enhance data-driven decision-making, enabling financial professionals to gain deeper insights into market trends and make informed investment decisions.

(f) Common Risks associated:

- 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 (location) 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, and governance to make it more regulated.

? Give example of emerging technologies available for Next Generation Audit along with the risks associated with it. **(ICAI SM)**

10 Conclusion

- Emerging technologies bring opportunities to organisations, but they also expose the enterprise to new risk.
- Auditors are expected to identify the **right balance between cost and benefit of ICs** for mitigating these risk factors. This includes:
  - understanding **how technology integrates with business,**
  - **how it is governed,**
  - which **activities are automated and how they are controlled,**
  - **business impact** as a result of this automation, and how negative impact are controlled and monitored.
- Auditors should be **able to identify the risk inherent with these technologies**. This includes understanding the:
  - **technology architecture,**
  - **IC framework** embedded in the technology and its integration with business.

RPA work flows
Columnar Presentation of IND AS 16 – Property, Plant & Equipment with IFCoFR and Audit Procedures

Para Ref. 6

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

Para Ref. 7

- **Accounting policy** → Recognises an item of PPE as an asset if it is probable that future economic benefits associated with the item will flow to the entity; and the cost of the items can be measured realiably.
- **Relevant data to be captured** → Assess the probability and reliability of future economic benefits and cost of PPE items.
- **Relevant calculation to be made** → Apply cost model or revaluation model for subsequent measurement of PPE items.
- **Presentation in FS** → Disclose the basis of recognition and measurement of PPE items.
- **IFCoFR** → Establish ICs over the assessment of probability and reliability of future economic benefits and cost of PPE items.
- **Audit procedures as per Standards on auditing** → Verify the recognition criteria and measurement basis of PPE items by inspection, confirmation, vouching, analytical procedures, etc.

Para Ref. 8

- **Accounting policy** → Measure the cost of an item of PPE as the cash price equivalent at the recognition date. If payment is deferred beyond normal credit terms, measure the cost at the present value of all future payments.
- **Relevant data to be captured** → Identify the cash price equivalent and the present value of deferred payments for PPE items.
- **Relevant calculation to be made** → Calculate the present value of deferred payments using an appropriate discount rate.
- **Presentation in FS** → Disclose the cash price equivalent and the present value of deferred payments for PPE items.
- **IFCoFR** → Establish ICs over the identification and calculation of cash price equivalent and present value of deferred payments for PPE items.
- **Audit procedures as per Standards on auditing** → Verify the cash price equivalent and present value of deferred payments for PPE items by inspection, confirmation, vouching, analytical procedures, etc.

Para Ref. 9

- **Accounting policy** → Include in the cost of an item of PPE any costs directly attributable to bringing the asset to the location and condition necessary for it to be capable of operating in the manner intended by management. Exclude any costs that are not directly attributable to bringing the asset to that location and condition.
- **Relevant data to be captured** → Identify directly attributable costs and non-attributable costs for PPE items.
- **Relevant calculation to be made** → Allocate directly attributable costs to PPE items based on a rational and consistent basis. Exclude any non-attributable costs from PPE items.
- **Presentation in FS** → Disclose directly attributable costs and non-attributable costs for PPE items.
- **IFCoFR** → Establish ICs over the identification and allocation of directly attributable costs and non attributable costs for PPE items.
- **Audit procedures as per Standards on auditing** → Verify directly attributable costs and non-attributable costs for PPE items by inspection, confirmation, vouching, analytical procedures, etc.

Para Ref. 10

- **Accounting policy** → Include in the cost of an item of PPE any borrowing costs that are directly attributable to the acquisition, construction or production of a qualifying asset as part of the cost of that asset in accordance with Ind AS 23 Borrowing Costs. A qualifying asset is an asset that necessarily takes a substantial period of time to get ready for its intended use or sale.
- **Relevant data to be captured** → Identify the borrowing costs and qualifying assets for PPE items.
- **Relevant calculation to be made** → Allocate borrowing costs to qualifying assets based on a rational and consistent basis.
- **Presentation in FS** → Disclose borrowing costs and qualifying assets for PPE items.
- **IFCoFR** → Establish ICs over the identification and allocation of borrowing costs and qualifying assets for PPE items.
- **Audit procedures as per Standards on auditing** → Verify the borrowing costs and qualifying assets for PPE items by inspection, Confirmation, vouching, analytical procedures, etc.

Para Ref. 11

- **Accounting policy** → Exclude from cost of an item of PPE any trade discounts and rebates.
- **Relevant data to be captured** → Identify trade discounts and rebates for PPE items
- **Relevant calculation to be made** → Deduct trade discounts and rebates from the cost of PPE items.
- **Presentation in FS** → Disclose trade discounts and rebates for PPE items.
- **IFCoFR** → Establish ICs over the identification and deduction of trade discounts and rebates for PPE items.
- **Audit procedures as per Standards on auditing** → Verify trade discounts and rebates for PPE items by inspection, confirmation, vouching, analytical procedures, etc.

Para Ref. IS

- **Accounting policy** → Recognise the cost of a self-constructed asset as the cost of an item of PPE.
- **Relevant data to be captured** → Identify self-constructed assets and cost components.
- **Relevant calculation to be made** → Apply same principles as for an acquired asset.
- **Presentation in Fs** → Disclose self-constructed assets and their costs.
- **IFCoFR** → Establish ICs over the identification and measurement of self-constructed assets.
- **Audit procedures as per Standards on auditing** → Verify self-constructed assets and their costs by inspection, confirmation, vouching, analytical procedures, etc.

Para Ref. 31

- **Accounting policy** → Review the residual value, useful life and depreciation method of an asset at least at each financial year-end and, if expectations differ from previous estimates, account for the change as a change in an accounting estimate in accordance With Ind AS 8 Accounting Policies, Changes in Accounting Estimates and Errors.
- **Relevant data to be captured** → Identify residual value, useful life and depreciation method of PPE items.
- **Relevant calculation to be made** → Assess whether there is any indication of change in expectations from previous estimates.
- **Presentation in FS** → Adjust the depreciation charge accordingly and disclose the nature and effect of the change in estimate.
- **IFCoFR** → Establish ICs over the review and adjustment of residual value, useful life and depreciation method of PPE items.
- **Audit procedures as per Standards on auditing** → Verify the residual value, useful life and depreciation method of PPE items by inspection, confirmation, vouching, analytical procedures, etc.

Para Ref. 41

- **Accounting policy** → Recognise the cost of replacing part of an item of PPE as an asset if it is probable that the future economic benefits embodied within the part will flow to the entity, and the cost of the item can be measured reliably. Derecognise the carrying amount of the replaced part.
- **Relevant data to be captured** → Identify the replacement parts and their costs for PPE items.
- **Relevant calculation to be made** → Assess the probability and reliability of future economic benefits and cost of replacement parts.
- **Presentation in FS** → Allocate the cost of replacement parts to PPE items and remove the carrying amount of replaced parts. Disclose the replacement parts and their costs for PPE items.
- **IFCoFR** → Establish ICs over the recognition and measurement of replacement parts for PPE items.
- **Audit procedures as per Standards on auditing** → Verify the replacement parts and their costs for PPE items by inspection, confirmation, vouching, analytical procedures, etc.

Para Ref. 57

- **Accounting policy** → Derecognise an item of PPE on disposal or when no future economic benefits are expected from its use or disposal. Gain or loss arising from derecognition is included in profit or loss when the item is derecognised.
- **Relevant data to be captured** → Identify the disposed or retired PPE items and their carrying amounts.
- **Relevant calculation to be made** → Calculate the gain or loss on derecognition as the difference between net disposal proceeds and carrying amount.
- **Presentation in FS** → Recognise the gain or loss on derecognition in profit or loss. Disclose the disposed or retired PPE items and their gain or loss on derecognition.
- **IFCoFR** → Establish ICs over the identification and calculation of gain or loss on derecognition of PPE items.
- **Audit procedures as per Standards on auditing** → Verify the disposed or retired PPE items and their gain or loss on derecognition by inspection, confirmation, vouching, analytical procedures, etc.

Chapter-18 SUSTAINABLE DEVELOPMENT GOALS (SDG) & ENVIRONMENT, SOCIAL AND GOVERNANCE (ESG) ASSURANCE

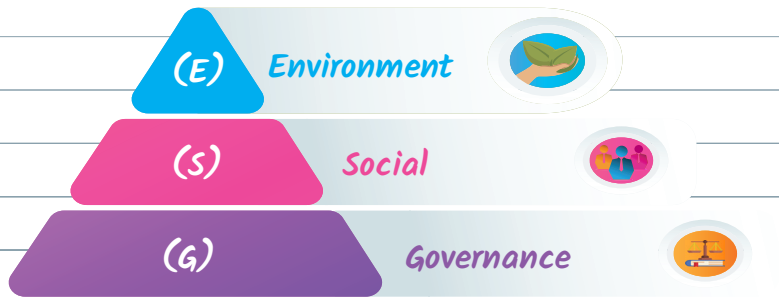
1 INTRODUCTION

- Sustainability is a concept related to the **development of products, goods and services that involves meeting our present needs without compromising the ability of future generations** to fulfill their own needs.
- Sustainability recognises that the environment is an exhaustible resource. Therefore, it is important to **use the environment and its resources rationally and protect it** for the good of the Earth, our environment, humanity, and all living things.
- The concept of sustainable development is named after the Brundtland report, which reports sustainable consumption in developed countries.

In this report Sustainable Development is defined as:

"Sustainable development is development that strives to meet the needs of developing countries seeking to achieve a more sustainable world. Sustainable development addresses the needs of the present moment without compromising current and future generations to meet their own sustainable lifestyles."

- Sustainable development can be applied to business corporate policy as it encompasses the following three pillars of sustainability:



These three pillars constitute the term ESG

Environment (E)

- ✔ It stands for **corporate climate policies**, energy use, waste, pollutions, natural resource conservation, and treatment of animals.
- ✔ It includes **natural resources** that every entity absorbs for its functioning like coal, electricity, water, etc. Processing this energy into products / services which will leave behind certain wastes like carbon emissions, water

discharges, e-wastes, discharges, e-wastes, etc. Thus, one is dependent on the environment for carrying out its operations.

Social (S)

- ✔ It addresses the **relationships the entity has and the reputation it fosters with people and institutions** in the communities where business is conducted and the value chain is involved.
- ✔ It further includes **labour relations, diversity, and inclusions.**
- ✔ Every company operates within a broader and diverse society.

Governance (G)

- ✔ It is the **internal system of practices, controls, and procedures** entity adopts in order to govern itself, make effective investment decisions, comply with the law, and meet the needs of all stakeholders.
- ✔ Every entity, which is itself a legal creation, requires governance.

The above pillars include the following elements as under:

ENVIRONMENT

- **Climate Change:**
  - Carbon Emissions
  - Product Carbon FootPrints
  - Financing Enviornmental Impact
  - Climate Change Vulnerability
- **Natural Resources:**
  - Water Stress
  - Bio-diversity & land use
  - Raw Material sourcing
- **Pollution & Waste:**
  - Toxic emission and waste
  - Packing Material and waste
  - E-Waste
- **Environment Opportunity:**
  - Clean Tech
  - Green Building
  - Renewable Energy

SOCIAL

- **Human Capital:**
  - Labour Management
  - Health & Safety
  - Human Capital Development
  - Supply Chain Labour Standards
- **Product Liability:**
  - Product Safety & Quality
  - Chemical Safety
  - Financial Product Safety
  - Privacy & Data Security
  - Responsible Investment
- **Stakeholders Opposition:**
  - Controversial Sourcing
- **Social Opportunity:**
  - Access to communication
  - Access to Finance
  - Access to Health Care
  - Opportunities in Nutrition and Health

GOVERNANCE

- **Corporate Governance:**
  - Broad Diversity
  - Executive Pay
  - Ownership
  - Accounting
- **Corporate Behaviour:**
  - Business Ethics
  - Anti-Competitive Practices
  - Corruption & Instability
  - Financial system & stability
  - Tax Transparency

ESG Reporting:

- ESG reporting is all about disclosure of information, data, metrics that explain the added value in these three areas.
  - **Types of ESG reports:**
    - ✔ **Qualitative Report:** tend to describe a company's strategy or policy around the relevant topics.
    - ✔ **Quantitative Report:** includes metrics, and key performance indicators (KPIs) linked to each area in order to measure progress against goals and report on achievements.
  - A mixed approach that makes use of both qualitative and quantitative information tends to add the maximum value to the quality of disclosures.

2 SUSTAINABLE DEVELOPMENT GOALS

Adoption: In 2015, sustainable development was adopted by all **United Nations Members States to provide a blueprint, which mentioned the Sustainable Development Goals** (SDGs).

There were **17 SDGs which are considered as an urgent** call for action by all countries, whether developed or developing countries.

Purpose: They recognised that **ending of poverty** and other deprivations must go hand in hand with strategies that **improve health and education, reduce inequality, and spur economic growth** – all while tackling **climate change** and working to **preserve our oceans and forests.**

Today, the Division for Sustainable Development Goals (DSDG) in the United Nations Department of Economic and Social Affairs (UNDESA) provides substantive support and capacity building for the SDGs and their related thematic (connected) issues **including** water, energy, climate, oceans, urbanisation, transport, science and technology, the Global Sustainable Development Report (GSDR), partnerships and Small Island Developing States.

SDG plays a key role in the evaluation of UN system wide implementation of the **2030 Agenda** and on advocacy and outreach activities relating to the SDGs.

Following are the 17 SDGs:

01 No Poverty	10 Reduced Inequalitites
02 Zero Hunger	11 Sustainable Cities & Communitites
03 Good Health & Well Being	12 Responsible Consumption & Production
04 Quality Education	13 Climate Action
05 Gender Equality	14 Life Below Water
06 Clean Water & Sanitization	15 Life on Land
07 Affordable & Clean Energy	16 Peace, Justice & Strong Institutions
08 Decent Work & Economic Growth	17 Partnership for the Goals
09 Industry Innovation & Infrastructure	

3 GLOBAL TRENDS IN SUSTAINABLE REPORTING

- **Mandatory for:** public sector or government- run companies, large corporations, multinational business conglomerates, and listed companies in stock exchanges.
- **Reporting provisions:** sector-specific, and thematic reporting provisions.
- **Framework used:** Global Reporting Initiative (GRI) Sustainability Reporting Standards, having 93% of the world's largest 250 corporations report on their sustainability performance through GRI.
- **GRI Sustainability Reporting Standards** are developed with true multi-stakeholder contributions and rooted in the public interest.

Global Reporting Initiative (GRI)	Carbon Disclosure Project (CDP)	International Integrated Reporting Framework (IIRC)
▸ Helps the organisations to **report on economic, environmental, and social impacts.** ▸ **General disclosures** which are required to be reported are **Economic, Environment and Social.** ▸ This report is **addressed to all the stakeholders of the entity.**	▸ **Captures the environmental performance** data which is related to GHG emissions, water, forests, and supply chain. ▸ Major details required to be **reported** are **climate change, Forest,** and **Water security.** ▸ This report is **addressed to** all the **investors, buyers,** and **other stakeholders** of the entity.	▸ **Established guiding principles and content elements** in order to allow the companies to produce integrated reports. ▸ This **report consists of Organisational overview, Governance structure, Business model, risks and opportunities, strategy, performance, outlook etc.**

Comprehensive Corporate Reporting System

In Sep 2022

In September 2020, these frameworks & standard setting institutions came together to show a commitment to working towards a comprehensive corporate reporting system.

The intent of the collaboration was:

- ✔ **Joint market guidance** on how the frameworks & standards can be applied in a complementary and additive way.
- ✔ **Joint vision** of how these elements could complement Financial GAAP and serve as a natural starting point for progress towards a more coherent, comprehensive corporate reporting system.
- ✔ **Joint commitment** to drive towards this goal, through an ongoing programme of deeper collaboration between the 5 institutions and stated willingness to engage closely with other interested stakeholders.

In Nov 2021

In **November 2021,** the IFRS Foundation Trustees published a revised **Constitution and a Feedback Statement** that responds to the feedback from Exposure Draft Proposed Targeted Amendments to the IFRS Foundation Constitution to Accommodate an International Sustainability Standards Board to Set IFRS Sustainability Standards.

International investors with global investment portfolios are increasingly calling for high quality, transparent, reliable, and comparable reporting by companies on climate and other Environmental, Social and Governance (ESG) matters.

On 3 November 2021, the IFRS Foundation Trustees announced the creation of a new standard-setting board-the **International Sustainability Standards Board (ISSB)** to help meet this demand.

The intention is for the ISSB to deliver a **comprehensive global baseline of sustainability-related disclosure standards** that provide investors and other capital market participants with information about companies sustainability-related risks and opportunities to help them make informed decisions.

Further, the ISSB has taken the technical guidance for developing IFRS Sustainability Disclosure Standards.

In 2015

Task Force on Climate-Related Financial Disclosures (TCFD)

- ✔ It was created in 2015 by the Financial Stability Board (FSB)
- ✔ The goal is to help companies to create consistent climate-related disclosures.

- ✔ Unlike GRI, which works on a wide range of organizations, TCFD is targeted at companies that predominantly handle financial-related interests, such as banks and insurance firms.

- **Climate Disclosure Standards Board (CDSB)**
  - ✔ An international group of business which is committed to making climate-related disclosures in the mainstream global corporate reporting.
  - ✔ CDSB framework was formed to help organizations to disclose climate related risks and opportunities. The CDSB framework has also set out an approach for reporting environmental information.

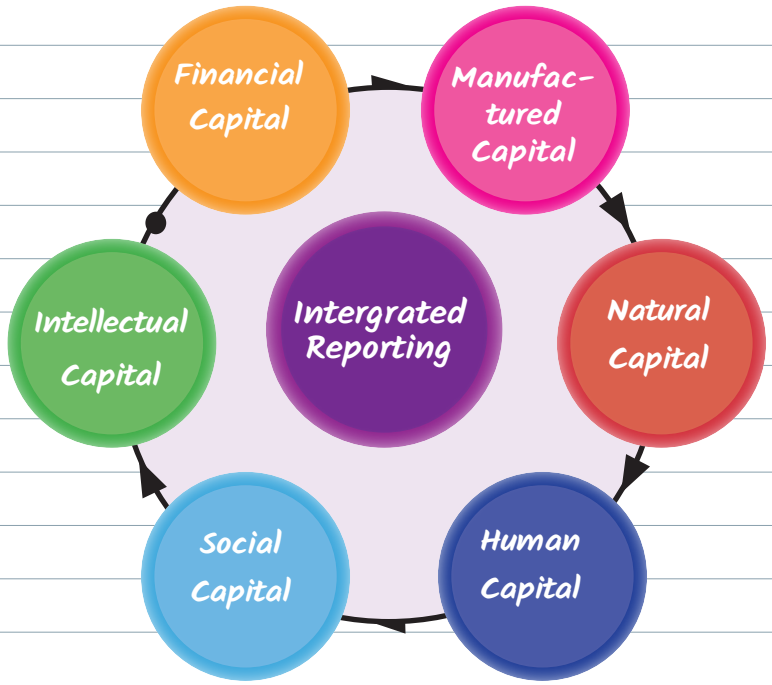
- **Value Reporting Foundation (VRF)**

VRF is a non-profit organisation which was a result of the merger between SASB Foundation and the International Integrated Reporting Council (IIRC). The International Accounting Standards Board (IASB) and the ISSB has agreed to work together in order to build an Integrated Reporting Framework.

- 2022 **International Sustainability Standards Board (ISSB)** in March 2022 launched a consultation on its first **two proposed standards—one on climate-related disclosures and one on general sustainability-related disclosures.**
- The proposed standards, when finalised, would form a comprehensive global baseline of sustainability-related disclosures designed to meet the information needs of investors in assessing enterprise value.
- **IFRS S1:** The proposed requirements in the Exposure Draft IFRS S2 Climate-related Disclosures (Climate Exposure Draft) build upon the recommendations of the Task Force on Climate-Related Financial Disclosures (TCFD) and incorporate industry-based disclosure requirements derived from the Sustainability Accounting Standards Board (SASB) Standards.

> **Dream is not that thing you see in sleep but is that thing that doesn't let you sleep**
>
> – Dr. A P J Abdul Kalam

4 INTEGRATED REPORTING



There are **6Cs of Integrated Reporting**-also known as 6 capitals:

- **Financial Capital:**
  - **Pool of funds that is available to the organization** for use in the production of goods or provision of services.
  - **Obtained through financing,** such as debt, equity, or grants, or generated through operations or investments.

- **Manufactured Capital**
  - Seen **as human-created, production-oriented equipment and tools.**
  - Available to the organisation for **use in the production of goods or the provision of services, including buildings, equipment, infrastructure** (such as roads, ports, bridges & waste, and water treatment plants).

- **Natural Capital**
  - Is an **input to the production of goods or the provision of services.**
  - An **organisation's activities** also impact, positively or negatively, on natural capital.
  - Includes **water, land, minerals and forests, biodiversity, and ecosystem health.**

Human Capital

People's skills and experience, their capacity, and motivations to innovate, including their:

- **Alignment with and support of the organisation's governance framework & ethical values** such as its recognition of human rights.
- Ability to **understand and implement an organisation's strategy.**
- **Loyalties and motivations** for improving processes, goods, and services, including their ability to lead and to collaborate.

Social Capital

- **Institutions and relationships established within and between each community, group of stakeholders and other networks** to enhance individual and collective well-being.
- Includes:
  - ✔ Common **values and behaviour.**
  - ✔ **Key relationships**, the **trust and loyalty** that an organization has developed and strives to build and protect with customers, suppliers, and business partners.
  - ✔ An organization's **social license** to operate.

Intellectual Capital

- **Key element in an organization's future earning potential,** with a tight link and contingency between investment in R&D, innovation, human resources, and external relationships, which can determine the organisation's competitive advantage.

? What are the 6 C's of Integrated reporting? **(ICAI SM)**

5 GLOBAL SCENARIO IN VARIOUS COUNTRIES

United States

- In March 2022, the US Securities and Exchange Commission (SEC) proposed climate-risk disclosure requirements, which would expand the annual reporting requirements of publicly traded companies.
- In their SEC filings, companies would be required to discuss financially material, climate-related risks guided by the TCFD recommendations.
- Reporting would include:
  - ✔ company's climate risk management processes
  - ✔ How the risks identified would impact financial performance

- How these risks are managed and mitigated
- Any scenario analysis, transition plans, and publicly announced climate goals.

United Kingdom

- In 2019, UK passed a law targeting net zero greenhouse gas (GHG) emissions by 2050.
- A key regulation for UK ESG disclosures is the Companies Act of 2006, which includes requirements for annual reporting.
- Applicable to large companies that are either listed, exceed £500 million in annual turnover, or have more than 500 employees.
- Non-financial information has always been required in annual reports, but in 2022, the Act was expanded to include sustainability matters.
- The new requirements align with the recommendations from the Task Force on Climate-Related Financial Disclosure (TCFD).
- Companies are required to discuss the strategy, processes, and due diligence regarding matters of:
  - Environment (including the company's impact on the environment)
  - Company's employees
  - Social matters
  - Respect for human rights
  - Anti-corruption and anti-bribery
- Specifically for the environment, climate-related disclosures must include:
  - Climate change-related risks and opportunities
  - How these risks and opportunities are managed through targets and KPIs
  - How climate change is addressed in corporate governance
  - How climate risk impacts strategy
- Additionally, large UK companies are required to report on their UK energy use and carbon emissions within their annual reports through the Streamlined Energy and Carbon Reporting.
- In 2023, ESG reporting in the UK will be further formalised through the Sustainability Disclosure Requirements (SDRs). The SDRs will provide a framework for corporates to manage sustainability-related risks, opportunities, and impacts, as well as set relevant metrics and targets.

Following table showcases the evolution of sustainable development reporting in the recent past:

March 2021

Sustainable Finance Disclosures Regulation (SFDR) go into effect for asset managers and financial advisors operating in EU.

April 2021

European commission adopts the CSRD proposal, which will require large companies to report on social and environmental impacts starting in 2024.

October 2021

GRI standards updated.

November 2021

IFRS Foundation announces the formation of its global reporting standardisation initiative through the ISSB. UK Financial conduct authority releases sustainability requirements disclosure papers.

December 2021

The European commission published the first delegated act on sustainable activities for the first two environmental objectives of the EU territory.

February 2022

The EU adopts a proposal for a directive on Corporate Sustainability Due Diligence with Rules for companies to respect human rights and the environment in their global value chains.

March 2022

US SEC announces climate change disclosure proposal ISSB exposure draft for public commentary.

April 2022

European Financial Reporting Advisory Board issues exposure draft of the European Sustainbility Reporting Standard (ESRS) for public commentary.

June 2022

China's voluntary guidance for Enterprise ESG disclosures takes effect.

? What are the global trends in sustainable reporting? **(ICAI SM)**

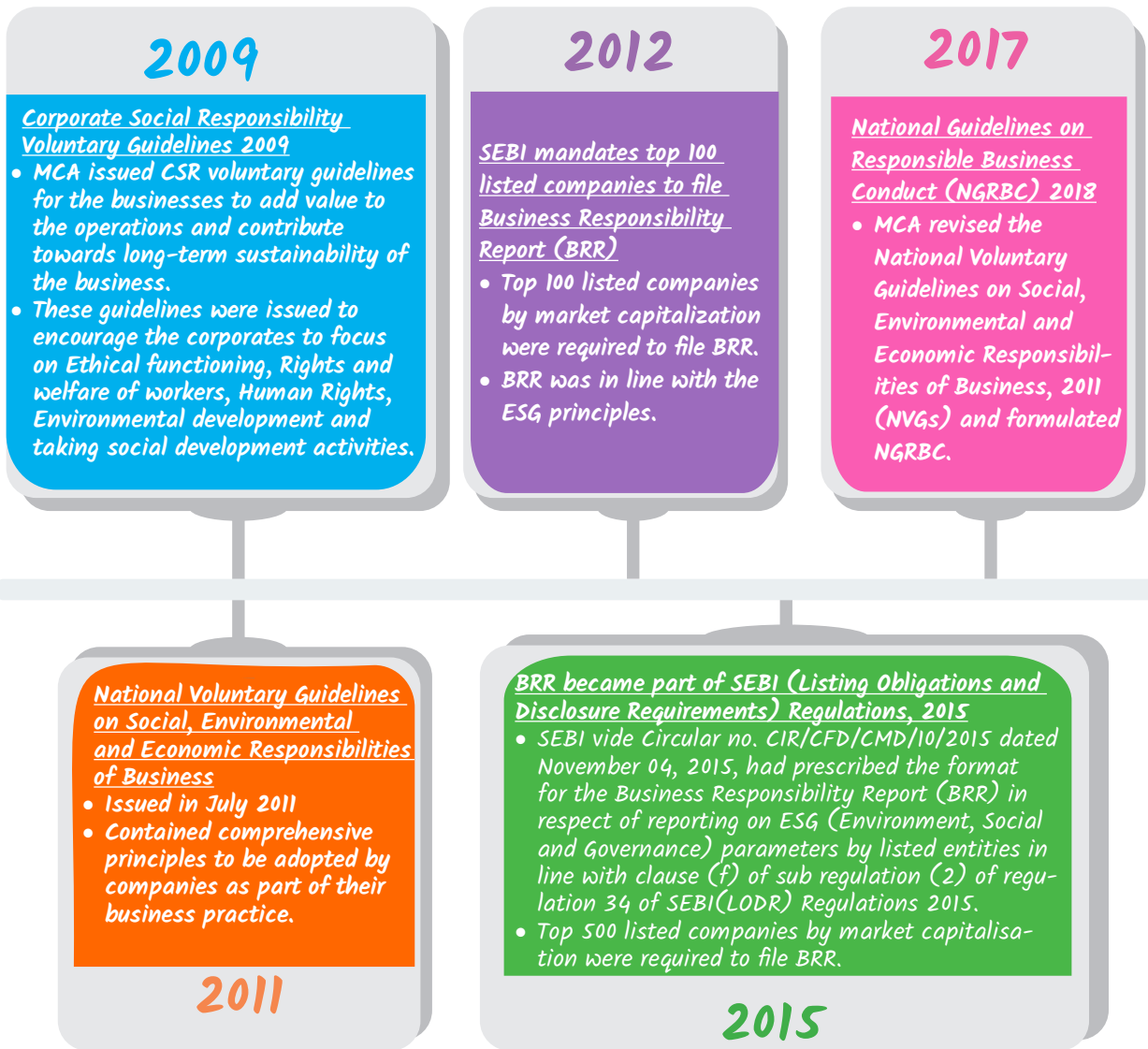
6 EVOLUTION OF ESG IN INDIA

Voluntary Guidelines on Corporate Social Responsibility

- Announced by MCA in 2009
- Ultimate goal was to integrate sustainability into business practices and into decision making process.

National Voluntary Guidelines (NVGs)

- Issued by MCA as additional guidelines on Social, Environmental, and Economic Responsibilities of Business, 2011" (NVGs)
- Emphasizing the importance of corporate entities' environmental, social, and economic responsibilities, as well as the need to integrate them into business practices and investment decision making processes.



2017

SEBI recommended Integrated Reporting for top 500 listed companies

- On 6 February 2017, SEBI issued a circular advising top 500 listed companies which are required to prepare BRR to adopt IR on a voluntary basis from the financial year 2017-18.

2019

National Guidelines on Responsible Business Conduct (NGRBC) 2018

MCA revised the National Voluntary Guidelines on Social, Environmental and Economic Responsibilities of Business, 2011 (NVGs) and formulated the National Guidelines on Resposible Business Conduct (NGRBC)

BRR became mandatory for top 1,000 listed companies

- As per SEBI (Listing Obligations and Disclosure Requirements) (Fifth Amendment) Regulations, 2019, with effect from December 26, 2019, the annual report of the top 1,000 listed entities based on market capitalisation shall contain a BRR as per clause (f) of sub regulation (2) of regulation 34 of Listing Regulations.

2021

New reporting requirements on ESG parameters called the Business Responsibility and Sustainability Report (BRSR).

- Under notification no. SEBI/LAD-NRO/GN/2021/22 dated May 05, 2021, SEBI introduced new reporting requirements on ESG parameters called the Business Responsibility and Sustainability Report (BRSR).
- BRSR seeks disclosures from listed entities on their performance against the nine principles of the 'National Guidelines on Responsible Business Conduct' (NGBRCs) and reporting under each principle is divided into essential and leadership indicators.
- Reporting:
  - ✓ Essential indicators: mandatory in nature
  - ✓ Leadership indicators: voluntary in nature
- Listed entities should endeavor to report the leadership indicators also.
- BRSR is intended towards having quantitative and standardised disclosures on ESG parameters to enable comparability across companies, sectors, and time.

2022

Mandatory reporting of top 1,000 listed companies to file BRSR along with the annual reports.

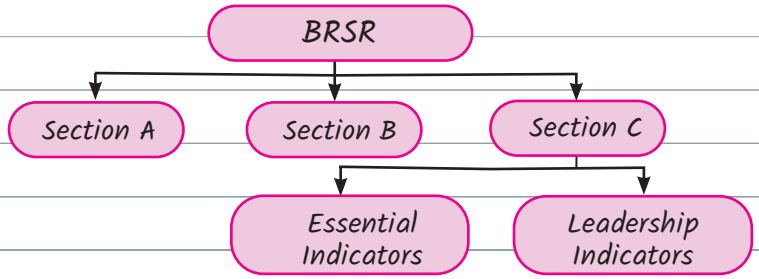
7 INITIATIVES BY ICAI

- In Feb 2020, ICAI constituted Sustainability Reporting Standards Board (SRSB).
- Mission of the SRSB is to take appropriate measures to increase awareness and implement measures towards responsible business conduct, developing audit guidance for Integrated Reporting.
- Encouraged by SEBI, ICAI introduced India's first award to celebrate the business practice of Integrated Reporting, internationally acknowledged as the emerging best practice in corporate reporting.

- Started a Certificate Course on Sustainable Development Goals (SDGs), Business Responsibility Reports (BRR), Integrated Reporting (IR).
- Proposed an ICAI Executive Development Program on Business Responsibility Reporting (BRR).
- In last 2 years, ICAI has issued following publications:
  - Standard on Assurance Engagements (SAE 3410): Assurance Engagements on Greenhouse Gas Statement
  - Background Material on BRSR (revised 2021)
  - Sustainable Development Goals : Accountants creating sustainable World – Part 1 covering SDGs 1 to 5
  - Sustainable Development Goals : Accountants creating sustainable World – Part 2 covering SDGs 6 to 11
  - Sustainable Development Goals : Accountants creating sustainable World – Parts 3 covering SDG 12 to 17
  - FAQs on Sustainability Reporting : Heart of Good Governance
  - Sustainability Reporting Maturity Model (SRMM): Version 1.0

7.1 Business Responsibility and Sustainability Report (BRSR)

- Reporting under BRSR is mandatory from F. Y 2022-23. However, disclosure was voluntary in F. Y 2021-22.



- The reporting questionnaire is divided into three sections:
  - **Section A: General Disclosures**
    This section contains the details of the listed companies, its products, services, operations, employee related details, its holding, subsidiary, associate companies etc.
  - **Section B: Management Process and Disclosures**
    It contains questions related to policy and management processes, governance, leadership, and oversight.

- **Section C: Principle-wise Performance Disclosures**

  Companies are required to report upon Key Performance Indicators (KPIs) in alignment with the nine principles of the NGRBC. The section classifies KPIs into two categories that companies are required to report upon:

  - ✔ **Essential indicators (Mandatory Disclosures)**

    This would include data on training programs conducted, environmental data on energy, emissions, water, waste management, etc.

  - ✔ **Leadership indicators (Optional Disclosures)**

    This would include life cycle assessments, details of conflict management policy, additional data, on biodiversity, energy consumptions, supply chain managements etc.

? What type of companies are required to mandatorily furnish the Business Responsibility and Sustainability Report (BRSR) as per the SEBI circular with effect from FY 2022-23? **(ICAI SM)**

7.1.1 Nine Principles of BRSR

The nine principles in BRSR are categorised into the ESG components of Environment, Social and Governance -with 2 of the nine in environment,

- 3 in social; and
- 4 in governance.

Even though they are separate, they are interlinked to each other in some way. For example, the environmental protection is closely linked to the stakeholder engagement and inclusive growth.

Principle 1: Ethics, Transparency and Accountability

Principle 2: Safe and Sustainable Goals and Service

Principle 3: Promote well-being of all employees including those in the value chain

Principle 4: Respect for stakeholders' interests and responsiveness

Principle 5: Respect and Promote human rights

Principle 6: Protection and Restoration of environment

Principle 7: Influence on Public and Regulatory policy

Principle 8: Promote inclusive Growth and Equitable development.

Principle 9: Provide value to the consumers in a responsible manner.

Principle 1: Ethics, Transparency and Accountability

- The first principle emphasizes that the business decisions in an organisation should be open to disclosure and accessible to the relevant interested parties.
- The essence of core elements associated with the first principle are:

Policies & Procedures

(i) The entities' governing structure should **develop policies, procedures, and practices for their offices, factories, and work areas, ensuring that ethics is not compromised**.

Disclose to stakeholders

(ii) The **information** relating to the policies, procedures, and practices along with the performance should be **made available to the stakeholders**.

Transparency

(iii) In case of adverse effects, **more care has to be taken for transparent disclosures**.

Encourage associates

(iv) The entities in the value chain should be **encouraged to adopt these principles** by the governance structure.

Non-Coperate violators

(v) The entities should **proactively respond** to the outside entities that violate the nine principles of the BRSRs. This includes their suppliers, distributors, sub-contractors, or regulatory officers that may engage with the business concern.

Principle 2: Safe and Sustainable Goals and Service

- Entities should make sure that their goods, services, and the operations result in better life for the consumers and end-users.
- The essence of the core elements associated with the second principle is:
  - ✔ When a product is designed by the entity, production methods and technologies have to be devised in such a way so as to **minimise the resource usage** to make it sustainable.
  - ✔ Entities are also responsible to **educate and make aware their consumers and clients about their rights**.
  - ✔ Entities should take measures that **reduce the over exploitation of the nature's resources** by consuming sustainably and encourage methods for reduce, reuse and recycling of the resources.

Principle 3: Promote well-being of all employees including those in the value chain

- The third principle relates to all the initiatives an entity has to take for the benefit of its employees from the point of view of their dignity, health, well-being.

- The essence of the core elements associated with the principle is:
  - ✔ **Entity should:**
    - Ensure compliance with all regulatory requirements as far as employees are concerned.
    - Respect the dignity of employee as a human being and should not restrict their freedom of associations, unions, and other participatory mechanism for collective bargaining of their rights and redressal of issues they face at the workplace.
    - Prevent all kinds of child labour, bonded labour, and any other forms of involuntary labour.
    - Have a system in which the work-life balance of the employees is not compromised.
    - Be responsible :
      - To create a workplace and work environment that is safe, hygienic, and comfortable for people to work for long durations.
      - To create a workplace which is free of harassment and violence.
      - For skill development, career development and training of the work-force employed.
  - ✔ Businesses have to ensure timely payment of the worker's wages and compensation.
  - ✔ Payment of the wages has to be as per the living wages, which can take care of the basic needs and provide economic security to the employees.

Principle 4: Respect for stakeholders' interests and responsiveness

- The concept of interested party or stakeholders to a business has been a point of discussion in all the regulatory and voluntary systems that relate to the management system of any organisation, be it related to the quality, environment or the occupational health and safety of the workers.
- The essence of the core elements associated with the principle is:
  - ✔ The entities have to be **transparent and communicate with the stakeholders** about the impacts of their operations and business decisions on the people and the nature.
  - ✔ The policies, decisions, and the impact of the operations of the organisation to the stakeholders have to be **disclosed transparently** **with no ambiguity** on the

extent of the issues.

- ✔ The entities have to **systematically** determine the context of their operation **and** identify their interested parties.
- ✔ The entities should fairly share the benefits to the stakeholders or give an opportunity to them to benefit from the operations in an equitable manner.

Principle 5: Respect and Promote human rights

- The concept of human rights covers a wide variety of violence and threatening abusive issues faced by people.
- It refers to the human rights issues that happen directly or indirectly due to the operation of the business.
- The essence of the core elements associated with the principle are:
  - ✔ Entities should have a clear understanding **of the human rights and various ways by which human rights** can be violated from the perspective of the Constitution of India, national laws and policies and the content of International Bill of Human Rights.
  - ✔ Entities when developing their management systems, should integrate the human rights element into their policies, procedures, and practices.
  - ✔ Businesses should recognise and respect the human rights **of all relevant stakeholders and groups** within and beyond the workplace, including that of communities, consumers, and vulnerable and marginalised groups.

Principle 6: Protection and Restoration of Environment

- The sixth principle looks at the environmental responsibility as a basic requirement for the economic prosperity and sustainability.
- The core elements associated with this principle are:
  - ✔ Entities should:
    - have policies, procedures, and practices in place to assess and rectify impacts to the environment. This should cover the whole life cycle of the product.
    - Utilize natural and manmade resources in an optimum manner to ensure their sustainability by taking feedback from the stakeholders.
    - measure their performance relating to the prevention of pollution, destruction of forests, waste generation, energy use, land use, etc.

- contribute towards climate change resilience in line with India's commitment to various international mechanisms such as, Paris Agreement and National Action Plans for Climate Change.
- compare its activities with industry best practices to reduce, reuse and recycle/ recover materials, resources.
- look out for avenues by which they can improve their performance towards various environmental responsibilities.

Principle 7: Influence on Public and Regulatory Policy

- The seventh principle of influencing the policy formulation positively recognises that the businesses operate within the framework of statutory and legislative policies of the governing authority.
- The principle further highlights that:
  - ✔ Core elements of BRSR have to met holistically when the organisations go ahead with their contributions to policy formulation and policy advocacy.
  - ✔ Collective associations such as, the trade groups and industry chambers have to be utilised when moving ahead with the policy advocacy and formulation.
  - ✔ Role in policy advocacy by the organisation should be in such a way that it encourages fair competition and prevents human rights abuses.

Principle 8: Promote Inclusive Growth and Equitable Development

- This can work only with close participation and collaboration amongst the entities, authorities, the civil associations contributing to one another for a better livelihood, and assistance to the marginalised communities.
- The core elements of the eighth principle are:
  - ✔ Entities should:
    - have systems in place to identify and address impacts of their activities on the social, cultural, and economic aspects of the people. This includes business created issues like, land acquisition and use and construction activities for new facilities.
    - review, measure, and track the adverse impacts of their activities on the society and environment and make action plans to mitigate them adequately.

- make efforts to bring up creative products, technologies, and business concerns that help the marginalised communities to have well-being and a better quality of life.
- when designing their CSR activities, review local and regional development priorities to help the marginalised groups and communities.
- take care to ensure that business induced displacement or relocation of communities does not happen, and in unavoidable cases, should make sure to have mutually agreed, participative, and informed negotiations to provide fair compensation to the affected people.

✔ All forms of intellectual property and traditional knowledge should get the deserved respect from the organisation, and efforts should be made to ensure that benefits derived from their knowledge are shared equitably.

Principle 9: Provide value to the consumers in a responsible manner

▶ The primary purpose of any business is to create or provide useful products and services to the customer in exchange of reasonable profits.

▶ The core elements associated with the principle are:

✔ Entities should:

- put in their efforts to **reduce the negative impacts of their products and services** on consumers, natural environment, and society at large.
- **transparently and accurately disclose all kinds of adverse impacts** to the user, planet, society, on the biodiversity from their products.
- **inform the customers** on the safe and responsible ways of usage, reuse, recycling, and disposal of their products, and ways to eliminate over-consumption.
- when in the business of providing essential goods and services (e.g., Utilities), **enable universal access**, including to those whose services have been discontinued for any reason, in a non-discriminatory and responsible manner.

✔ When conceptualising, designing, and marketing their products, the organisation should not in any manner prevent the **freedom of choice and fair competition**.

✔ When handling customer data, the **right to privacy** of the customer needs to be maintained.

- ✔ When advertising about their products, the organisations should ensure that **misleading and confusing information is not exposed to the customers** about their products or its usage.
- ✔ Business enterprises should **make available transparent and accessible grievance redressal and feedback management system** for their customers to raise their voices or to seek clarifications.

? What are the nine principles of BRSR? How are the nine principles of BRSR linked with the 17 UN Sustainable Development Goals? **(ICAI SM)**

7.1.2 Alignment of BRSR Principles with SDGs

Principles/ SDGs	P1	P2	P3	P4	P5	P6	P7	P8	P9
SDG 1			✓	✓				✓	
SDG 2		✓				✓	✓	✓	✓
SDG 3			✓					✓	
SDG 4			✓					✓	✓
SDG 5			✓	✓	✓			✓	
SDG 6		✓				✓		✓	
SDG 7		✓				✓	✓		
SDG 8		✓	✓		✓			✓	
SDG 9		✓					✓		
SDG 10		✓					✓		
SDG 11			✓	✓			✓	✓	
SDG 12		✓				✓			✓
SDG 13		✓				✓	✓	✓	
SDG 14		✓				✓	✓	✓	✓
SDG 15		✓				✓	✓	✓	✓
SDG 16	✓		✓	✓	✓			✓	
SDG 17	✓						✓	✓	

7.1.3 Assurance in BRSR

- **Applicability:** SEBI has currently started with the top 1,000 listed companies. But very soon, remaining listed companies would also need to comply with the provisions of BRSR.
- BRSR is expected to be used as a single means for disclosing sustainability related information in India. This would be the main document which the stakeholders, investors would review and do industry analysis.
  Hence, assurance in this reporting becomes more critical.
- **ESG Audit:**
  - ✔ ESG audit would be a process that would help the companies to evaluate the environmental and social risks for the company's products, services, operations, etc.
  - ✔ Conducting an ESG audit also helps businesses look at their supply-chain risks, risk management capabilities and transparency with shareholders.

- **SSAE: 3000 Assurance Engagements on Sustainability Information**
- ICAI has recently issued Standard on Sustainability Assurance Engagements (SSAE) 3000 Assurance Engagements on Sustainability Information.
- This standard deals with assurance engagements on an entity's sustainability information.
- This is an umbrella standard **applicable to all assurance engagements on Sustainability information.**
- The **intended users** of this Standard include:
  - ✔ Assurance providers providing assurance on sustainability information.
  - ✔ Entities seeking to engage a professional auditor.
  - ✔ Regulators, investors, and other users of Sustainability Reporting data.
- **Assurance:** This standard provides reasonable or limited assurance on sustainability information.
- **Effective date of application:**
  - ✔ For assurance reports covering periods ending on 31st March 2023 - Voluntary basis
  - ✔ For assurance reports covering periods ending on or after 31st March 2024 - Mandatory basis

- ICAI has also issued SSAE 3410, Assurance Engagements on Greenhouse Gas Statements which deal with assurance engagements on an entity's sustainability information including assurance of BRSR.

7.1.4 Methodology to provide assurance on BRSR

? What is the methodology of providing assurance in BRSR? **(ICAI SM)**

7.1.5 Social Audit Standards

- The Sustainability Reporting Standards Board (SRSB) of the ICAI has recently issued Social Audit Standards (SAS 100 to 1600).
- **Aim:** To provide the Social Auditor with the necessary guidance in relation to independent impact assessment engagement of Social Enterprises engaged in various areas and the audit steps and procedures that should be applied while conducting the social impact assessment.
- The Standard sets out the minimum requirements to be followed while conducting impact assessment.

  However, laws or regulations may establish additional requirements which should be followed, as applicable.

8 ROLE OF AUDITOR: CONSIDERATION OF CLIMATE RELATED RISKS IN AN AUDIT OF FINANCIAL STATEMENTS

Auditor's Objective:

The role of the auditor is to obtain reasonable assurance about whether the FS as a whole are free from material misstatement, whether due to fraud or error, to enable auditor to report whether the FS are prepared and presented fairly, in all material respects, in accordance with the A-FRFW.

Obtain understanding of the entity:

In developing the understanding of an entity, the auditor should include the consideration of climate related risks and how these risks may be relevant to the audits. The climate-related risks could be more relevant in certain sectors or industries, e.g., banks and insurance, energy, transportation, materials and buildings, agriculture, food, and forestry products.

Usage:

Investors and stakeholders are seeking information from auditor's reports about how climate-related risks were addressed in the audit. With this increased user focus on climate change, auditor need to be aware of, and may face, increasing pressure for transparency about climate matters in his audit reports.

Audit Report:

- Must follow the requirements of applicable auditing standards.
- A key mechanism of communication to users about the audit that was performed.
- In addition to the audit opinion, it provides information about auditor's responsibilities and, when required, an understanding of the matters of most significance in the audit and how they were addressed.
- It may, also, warrant inclusion of an Emphasis Of Matter (EOM) paragraph to draw attention to disclosures that are of fundamental importance to users' understanding of the FS.

Auditor's Responsibilities:

- Determine whether the entity has appropriately disclosed relevant climate-related information in the FS in accordance with the A-FRFW e.g., Indian Accounting Standards or Accounting Standards, when relevant before considering climate-related matters in the auditor's report.
- Read the other information for consistency with information disclosed in the FS and information that may be publicly communicated to stakeholders outside the FS, such as management report narratives in the annual report, press releases, or investor updates (As per ISA 720 and SA 720)

What is the auditor's role on ESG aspects in an audit of financial statements of the Company? (ICAI SM)

8 Conclusion

- The overarching importance of sustainability reporting continues to gain momentum globally with demands from various stakeholders and substantial research and developments toward a uniform set of sustainability standards.
- The uniformity is not achieved yet due to lack of a common language for sustainability reporting.
- As reporting of sustainability information becomes the trend being observed globally, the demand for independent assurance of sustainability information is anticipated to grow as entities around the globe look to enhance the integrity of their sustainability reporting.
  Hence, it is imperative that auditors and assurance providers understand the current landscape and continue to monitor ongoing developments.
- The demand for assurance on "sustainability branded" reporting continues to grow and therefore there is an urgent need for globally accepted sustainability/ ESG assurance standards that can be used by all assurance professionals.

> If you want to shine like a sun, first burn like a sun.
>
> – Dr. A P J Abdul Kalam

PROUD STUDENTS OF CA SJ

AIRs in Last 3 attempts!

F.A.S.T
first attempt success tutorials

F.A.S.T
first attempt success tutorials

FOLLOW US ON

/casarthakjain

/SarthakJainCA
Scan QR & Open with Telegram App

/elearn.fast.edu.in

tiny.cc/FastApp

/esarthak

/casarthakjain

/@esarthakjain

/Fast Education

9522564050

AMENDMENTS TO THIS BOOK
http://tiny.cc/framendments