

Chapter 12 DIGITAL AUDITING AND ASSURANCE



DIGITAL AUDITING AND ASSURANCE

1. DIGITAL AUDIT (Digitisation for clients) 🖥️

1.A What is Digital Audit (DA) ?

DA is **placing assurance on the effectiveness of the IT systems** implemented in an organisation.

Why ?

- a Technology is **integral** to business operations.
- b Hence, organisations should review tech-related controls to identify **gaps and risks**. This assists in continuous improvement; and
- c ensures **regulatory compliance**.
- d Strong controls and security position gains **trust of stakeholders**.

1.B Key Features of DA (for auditee): ✨

1. Allows to **standardise** processes and controls to mitigate risk.
2. Leads to **savings** in time, cost and effort.
3. Encourages the auditee to embrace the **latest technological advancements**.
4. Help to create a future for **digital strategy** and paves way for **adopting technologies** such as AI and Robotic, usage of analytics and automation.
5. Help organisation gain a more comprehensive overview of **end-to-end processes** and how technologies are utilized, controlled and optimized against standards set.
6. Help the auditee to make **informed decisions**.
7. Improves the **quality** of opinion, more reliable **audit report**.

1.C Advantages of DA (for auditee) ✓

1. **Enhanced Effectiveness & Efficiency:**
With use of tools and automation techniques, auditee can standardise processes and routine tasks like automating a reconciliation process that previously involved hours, and increase efficiency, saves time & costs.
2. **Better Audit Quality:** Technology can correctly evaluate massive volumes of data quickly. This assist in determining areas that require more testing, lowering detection risk of auditor.

3. **Lower Costs:** By automating processes the cost of auditing and the time needed is reduced.

4. **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.

5. **Improved Risk Assessment:** Automations assist the audit process and streamlined testing improves the RAP. Management and auditors put their testing efforts on sites with a higher RoMM and make informed decisions.

1.D Consideration and Challenges of DA (for organisation) ⚠️

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

Know what **business benefits** the organisation wants to achieve with automation. 1

2 Think **people first** and do not underestimate, **change is difficult**.

Target the right processes – this is a key for successful automation. 3

4 Automation is not a standalone solution and should be **part of a broader digitalization strategy**.

5 Ensure the **process works** and it is **standardised** before automating. BOTs do not easily adapt to process change.

6 Automation introduces **new challenges** for organisation. Don't forget about **governance and data security** in the risk framework.

2. Auditors will obtain an understanding of management's implementation and oversight of new technologies. Then perform procedures to understand the changes to the company's business, including any changes to the IT environment. **Areas of focus** include understanding of:

1. 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).

2. **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.

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

2. AUDITING DIGITALLY (for auditor) 🤖

Let's start with an

Example

BOTs usage in Audit

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**

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

(ii) Based on population, BOT will **select the samples** of changes to be tested.

(iii) Further, BOT will **pull the correct file** with approved changes from SharePoint.

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

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

(vi) 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.A Concept of DA 💡

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.

① Auditing Digitally is **using advancements in technology** for effective and efficient audit.

② It involves **digitizing the way an audit is delivered** through automation and innovation.

③ There are **new technologies** to help **capture data, automate procedures, analyse information and focus on the real risks** of the client.

④ 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).

2.B Key Features or Advantages of auditing digitally 🏆

1. 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 & fewer errors**, but the benefits are wider reaching & personal.

This also results in **improved retention of talent and confidence**.

2. 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.

3. 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.

4. 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.

5. 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.

2.C Considerations of auditing digitally ⚙️

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

1🔑 What problems are you trying to solve?

Continuously evaluate the emerging technologies and latest tools to see what can benefit the audit.

Think about what would make your audit easier or better and how you will measure return on your investment. -----

2🔑 Which technology can help you?

There are a number of tools available and many vendors and start-ups use **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.

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

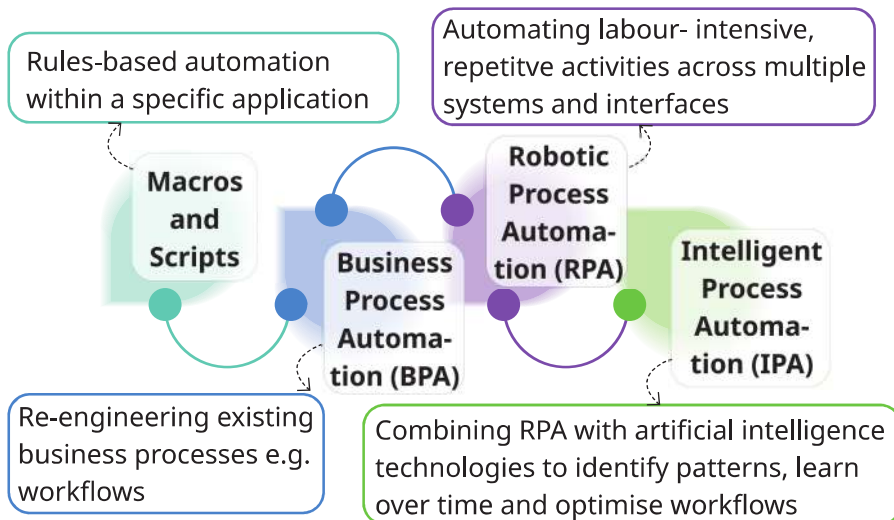
Technology is only as good as the people using it. Training and development are critical to ensure teams understand how and why they are using the technology. **Reluctance to change** is obvious, however **continuous training** help them to get better.

4🔑 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. -----

Range of automated solutions



2.D 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.

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 risks arising 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
 - 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 environment:

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

3. Understand the IT Environment

4. Identifying the Risks arising from usage of IT

5. Assessing Cyber Risks (Including Remote Audit)

Stages

1
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.

2
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.

5
Assessing the complexity of the IT environment:

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

- (a) **Automation** used in the organisation,
- (b) Entity's **reliance on system generated reports**,
- (c) **Customisation** in IT applications,
- (d) **Business model** of the entity,
- (e) Any **significant changes** done during the year; and
- (f) **Implementation** of emerging technologies.

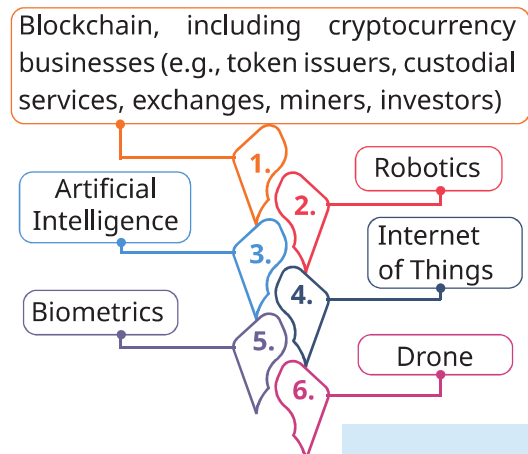
After considering the above factors for each application the over complexity is assessed of the IT environment.

3
Identification of Manual and Automated Controls:

- (a) 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).
- (b) An entity's mix of manual and automated elements **varies with the nature and complexity** of the entity's use of IT.
- (c) The characteristics of manual or automated elements are **relevant to the auditor's identification and assessment of the risks of material misstatement**.

4
Identification of the technologies used:

- (a) The need to **understand the emerging technologies implemented, role they play (in the entity's information processing or other FR activities)**, and consider whether there are **risks arising from their use**.
- (b) 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 FR processes and may give rise to risks from the use of IT.
- (c) Examples of **emerging technologies** are:



4. IDENTIFYING THE RISKS ARISING FROM USAGE OF IT ⚠

1 How to identify the IT Risks? 🔍

Consider the **nature of the identified IT application**.

Applicable risks 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 maintenance of underlying information.

2 Risks arising from use of IT ✨

i. **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**.

ii. Possibility of IT personnel **gaining access privileges** beyond those necessary to perform their assigned duties thereby:

- (a) **breaking down segregation of duties**;
- (b) **unauthorised changes to data in master files**.

iii. **Unauthorised changes** to IT applications or other aspects of the IT environment.

iv. **Failure** to make necessary **update** IT applications or other aspects of the IT environment.

v. **Inappropriate manual intervention**.

vi. **Data loss or data corruption**: 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**.

vii. 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.

viii. 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.

ix. 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.

x. **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. Understand the IT Environment

4. Identifying the Risks arising from usage of IT

5. Assessing Cyber Risks (Including Remote Audit)

Stages

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:

1 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.

2 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).**

3 Calculations

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

4 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.

5 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.

Understand the IT Environment

4.

Identifying the Risks arising from usage of IT

5.

Assessing Cyber Risks (Including Remote Audit)

Stages

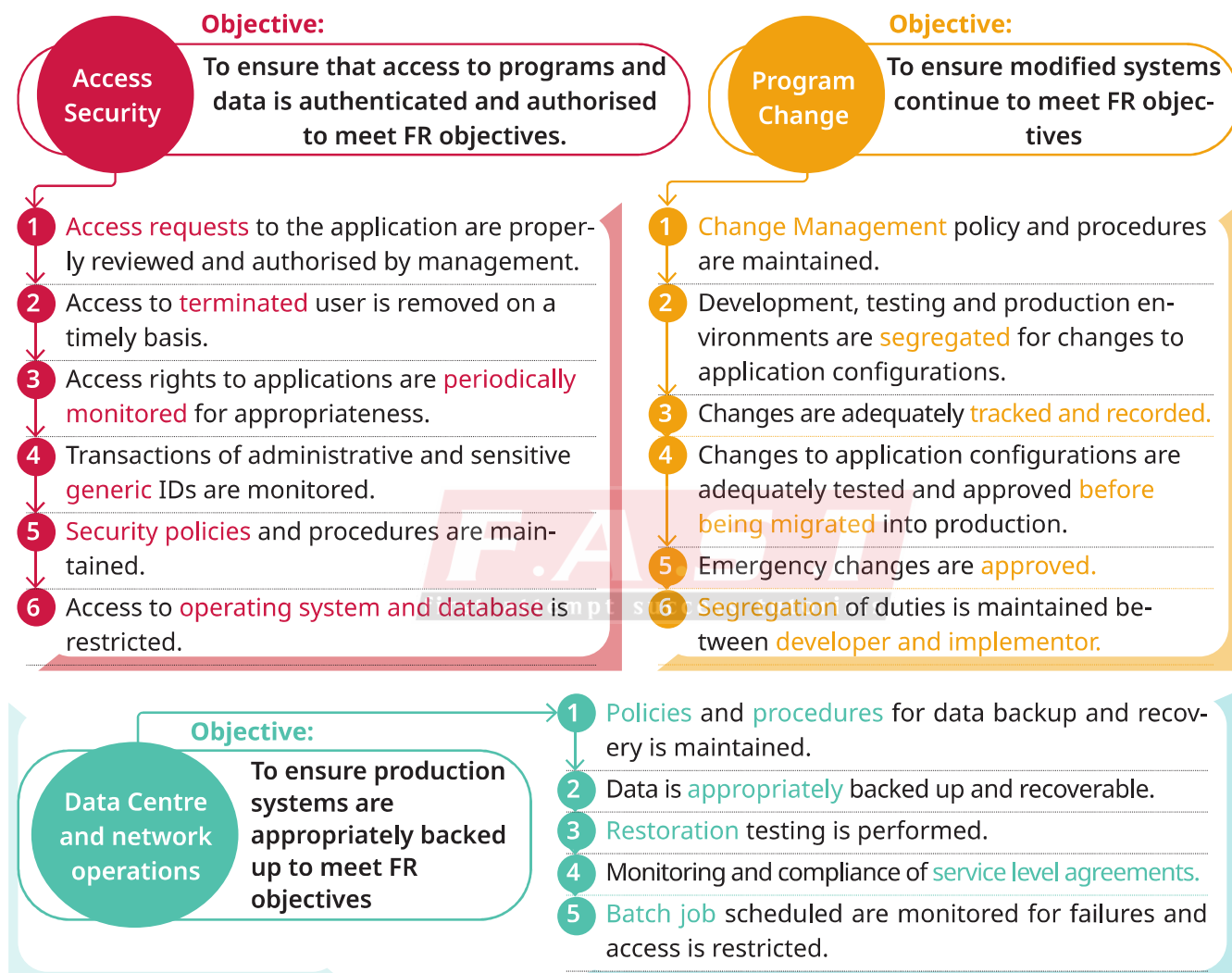
3.9 Understanding and responding to risks arising from IT dependencies

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.

4.9 General IT Control: Illustration: 🛡️

Overview of the control objectives and controls for each area of General IT Controls:



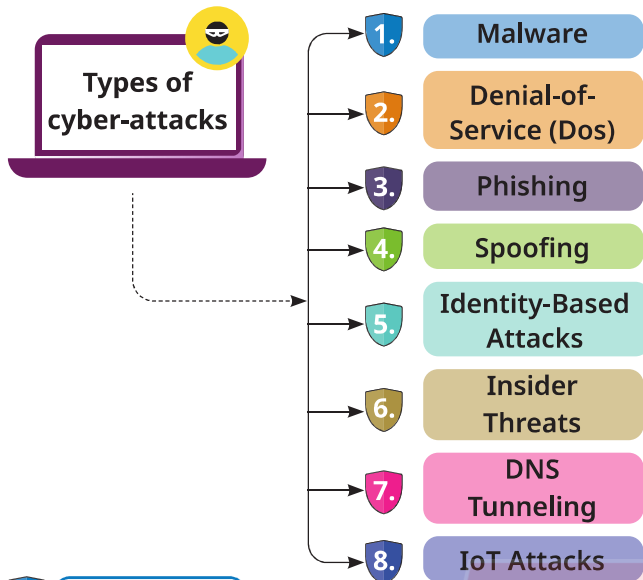
5.9 IT dependencies may also affect the design of the entity's controls and how they are implemented.

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.



5.1 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.**



1. 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.

(1.1) 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.

(1.2) 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.

(1.3) 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.

(1.4) 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.**

2. 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.

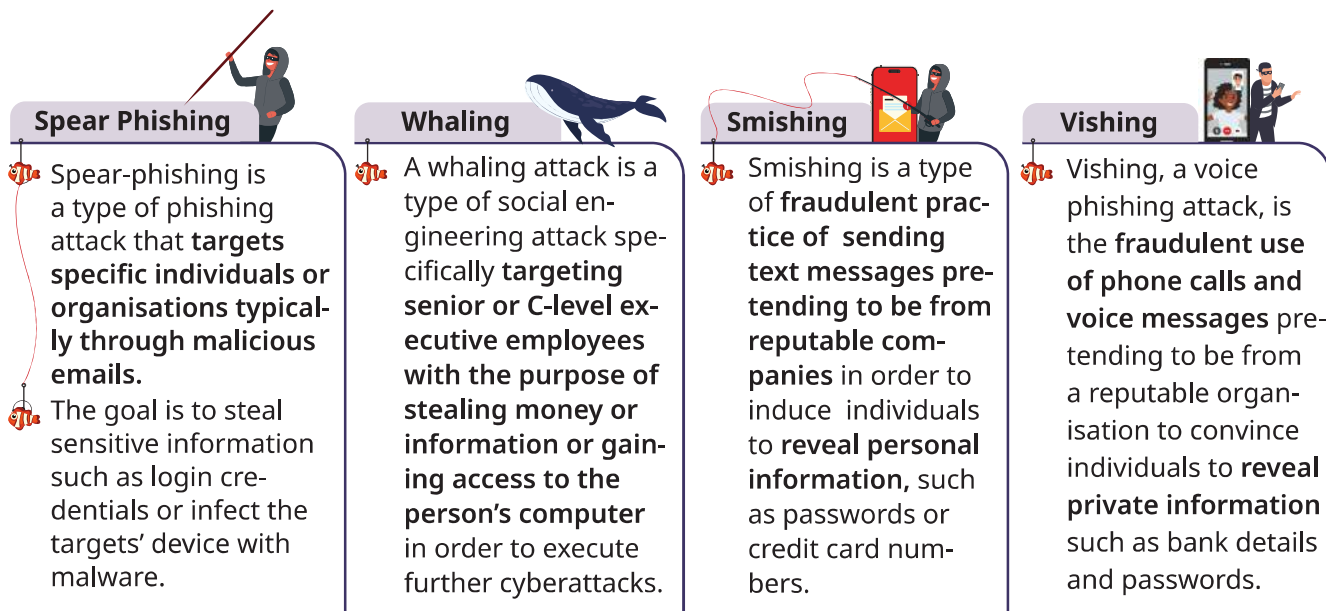
 In a DoS attack, users are **unable to perform routine and necessary tasks**, such as accessing email, websites, online accounts or other resources that are operated by a compromised computer or network.

 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.

3. 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.





Example

- Mr. Rajan, the CEO of a mid-sized company, has received an email requesting him to urgently update his account details due to a supposed security breach. The said email, appears to be received from the Company's bank accounts, looks official due to use of bank's logo and branding. Such email also includes a link to a website that resembles the bank's page. Concerned about the security of the company's finances, Mr. Rajan clicks on the link and enters his login credentials. Later, the company's IT department detects unauthorized access to the company's financial accounts and identifies that the CEO's credentials were compromised. The type of cyberattack that Mr. Rajan fell victim to is Spear Fishing.

4. 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

www.fast.edu.in

- 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.

5. Identity-Based Attacks

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

Example

- 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.



6. 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.

7. 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.

8. 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.

5.2 Stages of Cyber Risks

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

Assessing the cyber risk

1 Stage 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.

2 Stage

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**

3 Stage

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.**



5.1 What is Cyber Risk?

5.2 Stages of Cyber Risks

5.3 Cybersecurity Framework

5.4 Control considerations for Cyber Risks

5.5 Remote Audit

Stages

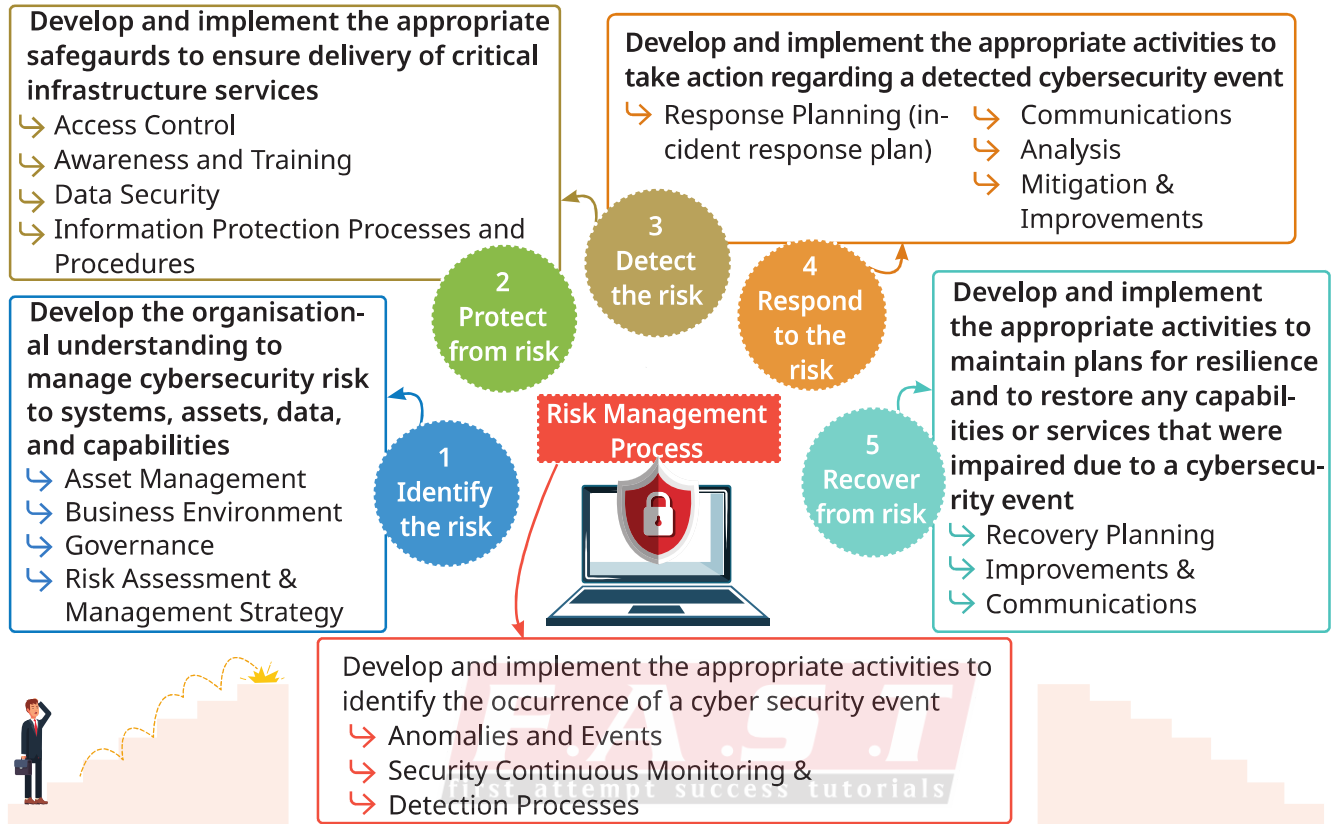
5.3

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.**



(1) Identify the risk

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

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

- 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.

(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 safeguard the organisation from such attacks.

(3) Detect the risk

1 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.

2 Review entity's processes to monitor and detect security breaches or incidents.

3 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.

4 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.

(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.



5.1 What is Cyber Risk?

5.2 Stages of Cyber Risks

5.3 Cybersecurity Framework

5.4 Control considerations for Cyber Risks

5.5 Remote Audit

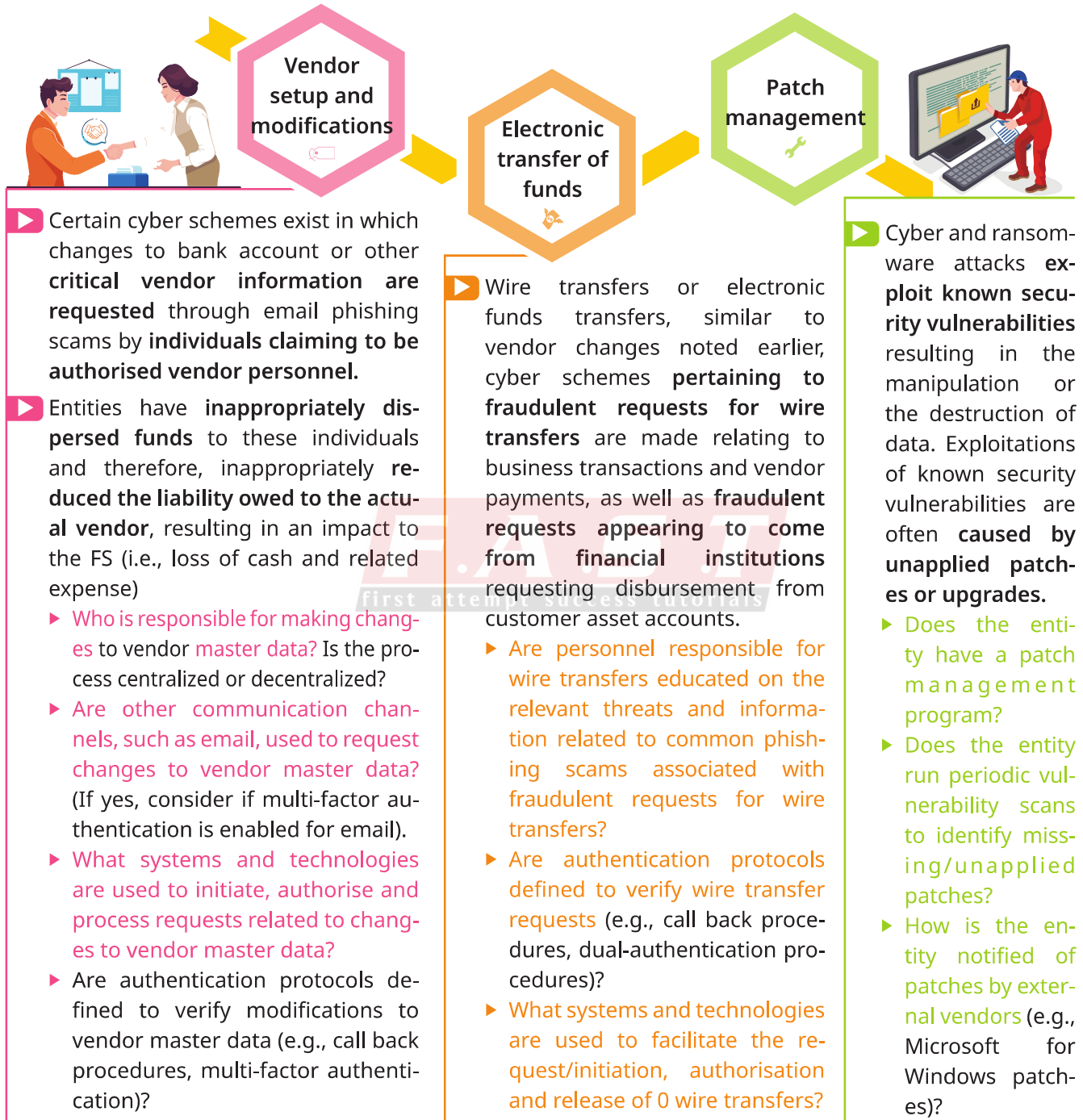
Stages

5.4 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



5.1 What is Cyber Risk?

5.2 Stages of Cyber Risks

5.3 Cybersecurity Framework

5.4 Control considerations for Cyber Risks

5.5 Remote Audit

5.5 Remote Audit

(1) When auditor uses the online or electronic means to conduct the audit.

(2) It could be partially or completely virtual.

5.5.1. Considerations for remote audit

i. Feasibility and Planning

1. Planning involve:

- Agreeing on **audit timelines**, **Meeting platform** (Zoom calls/ Microsoft Teams/Google Meet),
- Access authorization requests.

3. Execution phase involve

video/teleconferencing with auditees.

4. Documentation for AE

transferred through document sharing platform.

2. Feasibility is determining:

- What technology may be used,
- Competence level of auditors & auditees,
- Available resources.

ii. Confidentiality, Security and Data Protection

1 Access to document sharing platform

sufficiently restricted.

2 Info. once reviewed & documented by auditor,

removed from platform.

3 Consider L&R.

4 Auditor not to take screenshots of auditees as AE.

5 Use VPN.

iii. Risk Assessment

1 Clear & Consistent communication from auditor as well as auditees.

2 Risks for achieving the audit objectives:

- Identified,
- Assessed,
- Managed.

3 Assessment if remote audit would be sufficient to achieve the audit objectives should be done & documented

5.5.2. Advantages and Disadvantages of remote audit

• Advantages •

- Cost and time effective: No travel time and travel costs involved.
- Comfort and flexibility to the audit team as they would be working from home environment.
- Time required to gather evidence can spread over several weeks, instead of concentrated into a small period that takes personnel from their daily activities.
- Auditor can get first-hand evidence directly from the IT system as direct access may be provided.
- Widens the selection of auditors from global network of experts.

• Disadvantages •

- Due to network issues, interviews and meetings can be interrupted.
- 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.
- 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.
- Remote access to sensitive IT systems may not be allowed. Security aspects related to remote access and privacy needs to be assessed.
- 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.

5.1 What is Cyber Risk?

5.2 Stages of Cyber Risks

5.3 Cybersecurity Framework

5.4 Control considerations for Cyber Risks

5.5 Remote Audit

Stages

(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.

6. EMERGING TECHNOLOGIES IN AUDIT

1 Some examples of emerging technologies are – Data analytics [CAATs (ACL, Alteryx, Power BI, CaseWare), Artificial Intelligence (AI), Robotic Process Automation (RPA), and Blockchain].

2 These technologies are **changing the way business gets done**, and auditors are leading by transforming their own processes.

3 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 FR**.

6.1 Data Analytic Techniques

Meaning

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

Data

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

Benefit

The use of audit analytics enables **greater efficiencies and more accurate findings** from the review process.

Quality

As a result, businesses will be able to create **strategies based on verifiable data and professional assumptions** and auditors can **improve the audit quality**.

Volume

It allows auditors to **more effectively audit the large amounts of data held and processed in IT systems** in larger clients.

Audit Analytics

Audit analytics helps:

- ▶ To **discover and analyse patterns**
- ▶ **Identifying anomalies**
- ▶ **Extract other useful information in data**

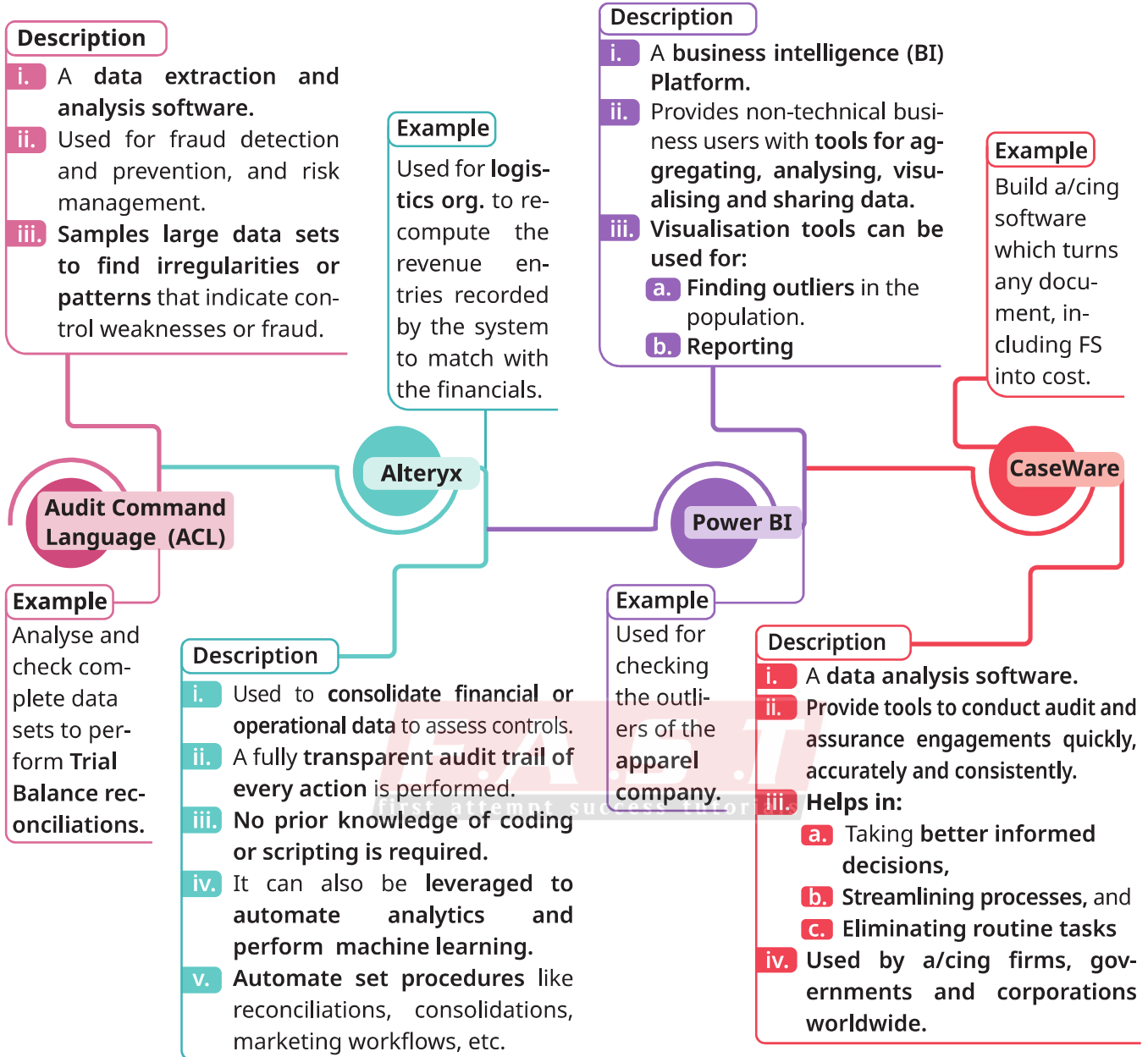
Computer Assisted Auditing Techniques (CAATs)

The data analytics methods used in an audit are known as **CAATs**.

It involves **use of multiple data analytical tool or visualization tools**.

This **minimizes the scope of missing out on key attributes**.

Tools used as a part of CAATs



7. AUTOMATED TOOLS IN AUDIT

1. Auditor's Approach

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.

2. Scope

Based on management's and auditors' independent risk assessment procedures, 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 FR.

3. Example

Robotic Process Automation (RPA), blockchain, machine learning, Internet of Things (IOT) and Artificial Intelligence (AI) are some prime examples of automation.

7. Automated Tools in Audit

7.1 Internet of Things

Description

- i It refers to the concept of connecting any device to the internet.
- ii **Key components:** Data collection, analytics, connectivity, and people and process.
- iii It affects strategic objectives of the org.
- iv It changes entity's risk profile with exposure to new L&R.

Example

Connected cars, connected manufacturing equipment's, smart home security, etc.

Common Risks

Device hijacking, Data siphoning, Denial of service attacks, Data breaches and Device theft.

Audit Implications

- i Unable to rely on manual controls.
- ii Need to train and upskill auditors.
- iii Consider impact on flow of transactions & new risks introduced by consumer facing tools.
- iv For example, consider payment processing tools that allow users to pay via credit card at a retail location through a mobile device.

7.2 Artificial Intelligence (AI)

Description

- i It refers to a system or a machine that can think and learn.
- ii It utilises data analysis and algorithms to make decisions.
- iii 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.
- iv Siri to help find your Air Pods or told Amazon Alexa to turn off the lights, etc.

Example

Self-driving cars, manufacturing robots, smart assistants, etc.

Common Risks

Security, Inappropriate configuration, Data privacy.

Description

- i Given the invisible nature of algorithms, audits must focus on the logical flow of processes.
- ii Ascertain whether unintended bias has been added to the algorithms.
- iii Assess the effectiveness of algorithms and whether their output is appropriately reviewed and approved.
- iv Consider cybersecurity and search for possible bugs and vulnerabilities.
- iv Confirm understanding of how the use of AI affects the entity's flows of transactions, including the generation of reports or analytics used by MGT.
- iv Consider whether the AI is making decisions - or being utilised by MGT. If MGT shifts its focus on oversight by relying on AI, understand:
 - ▶ What shift occurred,
 - ▶ How new risks might be addressed,
 - ▶ Whether existing risks may not be getting the same level of attention.

7.3 Blockchain

Description

- i It is based on a de-centralized and distributed ledger secured through encryption.
- ii Each transaction is validated by the blockchain participant.
- iii All blocks are sequenced so that any modification or deletion of a block disqualifies the info.

Example

Bitcoin, Crypto currency transfer application, etc.

Common Risks

Inability to reverse transactions, Cyber-attacks and data hacks, Regulatory compliances.

Audit Implications

- i Consider appropriate governance and security around the transactions.
- ii Although blockchain's core security premise rests on cryptography, which is risky.
- iii It does not ignore insecure APIs, data confidentiality & privacy.
- iv Weak blockchain application development protocols are considered.
- v Determine whether data put on blockchain will expose the enterprise for non-compliance with applicable L&R.

7.4 Robotic Process Automation (RPA) 🤖

Description

- i It is the **automation of the repetitive processes** performed by users.
- ii It is a software technology that **emulate humans' actions interacting with digital systems and software**.
- iii **Process efficiency, customer experience and control effectiveness** contributed to RPA.
- iv It can **interact with any application or system**.

Audit Implications

- i Understand RPA processes, which include data extraction, aggregation, sanitisation and cleansing.
- ii To perform substantive testing, understand tools used to develop and maintain RPA.
- iii General IT controls are applicable as always.

Common Risks

Operational and Execution risks, Change management risks, RPA strategy Risk.

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

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.

Scan the QR Code to See RPA workflow chart



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

a 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.

b ↳ 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.
- c ↳ **Unique**: It **cannot be forged or otherwise manipulated**.
- ↳ **Exchange**: NFT exchanges take place with cryptocurrencies such as Bitcoin on specialist sites.

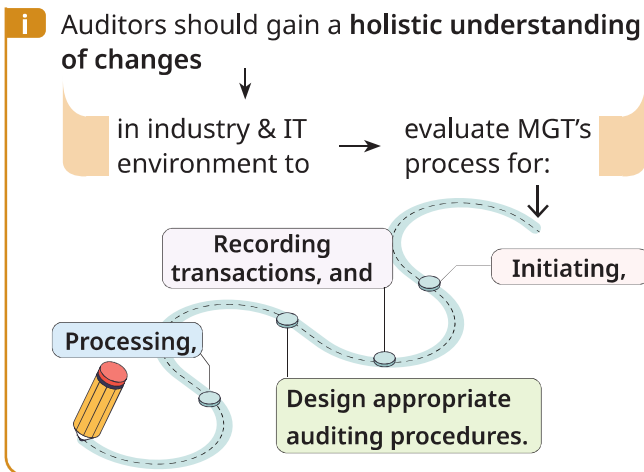
Challenges of NFT

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

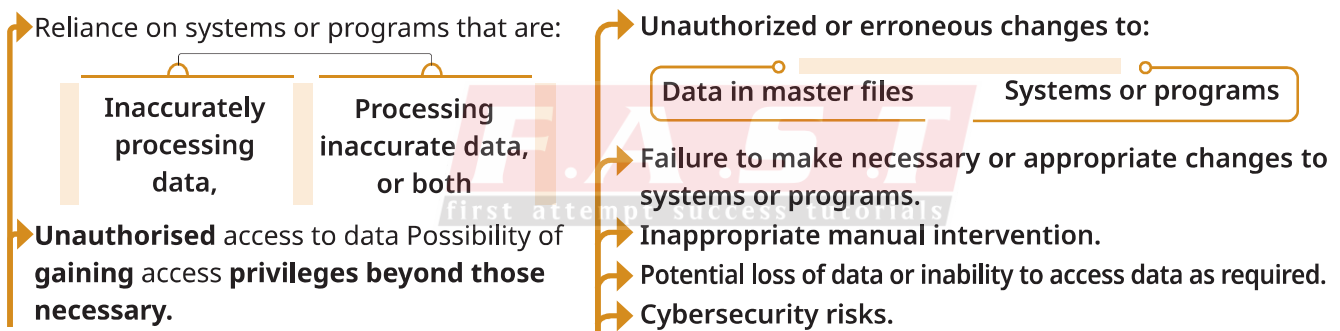
(Holistic approach, New Tech Risk, Upskill)

Auditors should focus on the following control considerations:



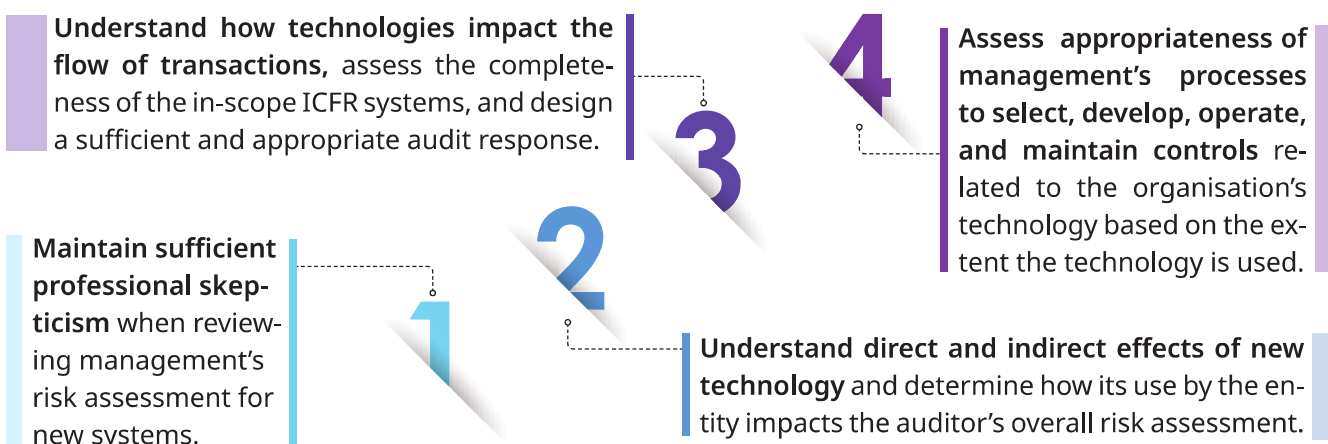
- ii Auditor should consider:**
- Risks resulting from implementation of new technologies **and** how those risks differ from those that arise from more traditional, legacy systems.
 - Whether **digital upskilling or specialists** are necessary to:
 - Determine impact of new technologies,
 - Assist in risk assessment,
 - Understanding design, implementation, and OE of controls.

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



8.1 Key steps for Auditors in a Changing Technology Environment

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



9. NEXT GENERATION AUDIT

The Next Generation Audit is **human-led, tech-powered and data-driven**. It is based on combining emerging technologies to redefine how audits are performed.

Next Generation Audit aims to the following:

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

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.



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, handheld bar scanners, manual counts etc. to optimise quality of deliverables, consolidate audit information and enhance the execution speed while ensuring correctness and completeness of data.



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, hyper-connected networks and digital reflections.**

C.1 Some considerations for future:



1

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.

2

Governance models will become ever more difficult to **balance openness and user contribution with strategic direction and innovation.**



3

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)

4

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.

C.2 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.

✖ 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.

■(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.

■(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.

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 include

- 🚗 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.

